Университетская серия

В. А. Гамза, И. Б. Ткачук

Безопасность банковской деятельности

2-е издание

Учебник

Market DS

Университетская серия

В. А. Гамза, И. Б. Ткачук

Безопасность банковской деятельности

2-е издание,
переработанное и дополненное

Учебник

УДК 336.719+[343.37:343.985.7](470+571)(07)
ББК 65.262.5(2Рос)-98я7+67.523.12(2Рос)я7
Г18

Серия удостоена диплома в номинации «Лучший издательский проект»
на IV Общероссийском конкурсе учебных изданий для высших учебных заведений
«Университетская книга — 2008»

Печатается по решению
Ученого совета Московской финансово-промышленной академии

Ответственный редактор серии
доктор экономических наук, профессор **Ю. Б. Рубин**

Гамза В. А., Ткачук И. Б.

Г18 Безопасность банковской деятельности: учеб. / В. А. Гамза, И. Б. Т
чук. — 2-е изд., перераб. и доп. — М.: Маркет ДС, 2011. — 408 с. (У
верситетская серия).

ISBN 978-5-94416-130-7

Агентство CIP РГБ

Курс «Безопасность банковской деятельности» предназначен для студентов вы
учебных заведений, осуществляющих подготовку по специальности «Финансы и кре
однако может быть полезен и для других экономических специальностей. Его с
хом можно использовать для послевузовской переподготовки экономических кадро
вышения квалификации, а также как практическое пособие для работников служб бе
ности и внутреннего контроля банков, следователей (дознавателей) правоохрани
органов, специализирующихся на расследовании преступлений в сфере экономическо
тельности, прокурорских работников, осуществляющих надзор за расследованием. И
могут извлечь пользу преподаватели, научные работники образовательных учреж
юридического и экономического профиля и другие читатели, интересующиеся проб
ми обеспечения безопасности в кредитно-финансовой сфере.

УДК 336.719+[343.37:343.985.7](470+57
ББК 65.262.5(2Рос)-98я7+67.523.12(2Р

КРАТКОЕ ОГЛАВЛЕНИЕ

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Укрепление устойчивости финансовой и банковской систем современной России по-прежнему остается важным направлением обеспечения экономической и национальной безопасности нашей страны. Проблема повышения уровня защищенности банков от противоправных посягательств касается большинства стран мира, включая государства, имеющие вековые традиции успешного ведения кредитно-финансовой (банковской) деятельности. Особенность положения России заключается в сравнительно недавнем восстановлении института коммерческих банков. В силу исторических причин в стране была утрачена значительная часть опыта обеспечения банковской безопасности досоветского периода. Определенные затруднения отмечаются в становлении современной науки о банковской безопасности, в том числе об особенностях организации и функционирования системы защиты банка, обеспечения безопасности новых направлений банковской деятельности и новых банковских технологий.

Ведущим субъектом обеспечения защиты коммерческих банков от противоправных посягательств является государство. Это обусловлено его конституционными обязательствами, гарантирующими защиту всех форм собственности (ст. 8, 35 и 114 Конституции РФ). По этой причине может показаться, что именно государство должно выступать главным заказчиком исследований в области безопасности банковской деятельности. В действительности это иначе. Своеобразие ситуации заключается в том, что государство взяло на себя в основном функции уголовно-правового и административного пресечения противоправных посягательств в банковской сфере. Основную работу по организации системы выявления и предупреждения криминальных посягательств такого рода законодатель возложил преимущественно на сами банки.

Требования о принятии банками мер защиты их имущества и инфраструктуры содержатся в ряде федеральных законов и нормативных актов Банка России. Именно банк должен обеспечивать своими силами и средствами безопасность банковских операций, охрану имущества, защиту информации (банковской, коммерческой тайны, иных сведений конфиденциального характера, компьютерной информации) и информационной инфраструктуры, защиту системы кадрового обеспечения, личную безопасность руководства и персонала банка. Понятно, что организация столь обширной и разноплановой работы требует соответствующего научного, учебного и методического

обеспечения. По этой причине банковское сообщество России заинтересовано в теоретических разработках и практических рекомендациях банковской безопасности гораздо больше, чем правоохранительные органы государства.

В последние годы отечественные ученые провели немало исследований, касающихся преступлений против коммерческих банков. Однако большинство выполненных работ по-прежнему адресовано правоохранительным органам и не затрагивает вопросов участия в борьбе с преступлениями самих банков и создания ими систем безопасности.

Сложившаяся ситуация отражает противоречие между реальным состоянием дел и объективными потребностями практики. Обширная сфера фактической деятельности банков по обеспечению защиты своего имущества и инфраструктуры от криминальных посягательств не имеет достаточно полного научного и методического отражения. Особенно заметна потребность в практических рекомендациях по построению системы безопасности банков, включая основы ее формирования, правового обеспечения, концептуального и рабочего проектирования, а также управления службой безопасности.

Особенность проблемы заключается в том, что основную работу по организации защиты от криминальных проявлений законодатель возложил на самими банки. К сожалению, надежность предпринятых ими мер безопасности во многих случаях оказалась невысокой. Отсутствие в последние десять лет должной защищенности от экономических рисков и угроз криминального характера стало одной из причин банкротств и прекращения деятельности значительного числа банков и небанковских кредитных организаций[1].

Жертвами посягательств становятся как малые, так и крупные банки. Изучение этой проблемы показывает, что во многих случаях своевременно выявить и предупредить действия злоумышленников не удалось по причине просчетов в организации работы служб, обеспечивающих защиту интересов банка. Как правило, такие просчеты были связаны с ошибками в выборе приоритетов, с отсутствием четкого представления об общей стратегии и вытекающих из нее конкретных мерах обеспечения безопасности банка, с разбалансированностью усилий подразделений, участвующих в обеспечении безопасности.

Обнаружился, в частности, существенный перекос в сторону «силовых» и «технических» методов защиты, а также физической охраны банков при недостаточном учете факторов «беловоротничковой» преступности. В действительности, как показывает практика, наиболее опасными для банка по своим экономическим последствиям являются действия преступников, использующих в противоправных целях не методы «силового воздействия», а приемы

[1] Количество кредитных организаций России, имеющих право на осуществление банковских операций, непрерывно сокращается. В январе 1996 г. их число составляло 2295, в июле 2001 г. — 1331, в июле 2005 г. — 1281, в марте 2008 г. — 1134.

интеллектуального и материального подлога, а также иные виды изощренного обмана, в том числе возможности новых банковских, электронных и полиграфических технологий. Самыми уязвимыми сферами банковской деятельности оказались кредитный бизнес, вексельное обращение, а также соответствующие электронные системы.

Потребовалась организация защиты банков от таких ранее неактуальных угроз, как противоправные посягательства на конфиденциальную и компьютерную информацию банка и его деловую репутацию. Возникла необходимость противодействия проявлениям недобросовестной конкуренции.

Повышение уровня защищенности банка от криминальных посягательств на нынешнем этапе непосредственно связано с методологической проработкой проблемы и проведением на ее основе технологизации защитных мероприятий. Способствовать этой цели призвано настоящее издание.

К несомненным достоинствам этого учебника можно отнести:

- четкое отображение содержания и структуры безопасности банка;
- подробное изложение целей обеспечения безопасности в банковской сфере и вытекающих из них практических задач;
- конкретное определение банковских угроз и их источников;
- детальная разработка системы мер противодействия угрозам различных направлений, видов и уровней;
- тщательное обоснование мер противодействия банковским угрозам с позиций права;
- развернутое описание процесса организации и управления деятельностью службы безопасности банка.

Наполнение учебника и изложенные в нем рекомендации во многом отображают многолетний опыт работы авторов в кредитно-финансовой и правоохранительной сферах. Форма подачи материала позволяет легко воспринимать проблему в целом и в частностях.

Первый заместитель председателя Банка России
А. А. Козлов

ВВЕДЕНИЕ

Курс «Безопасность коммерческого банка» является продолжением цикл
работ теоретического и прикладного характера, в числе которых монографи
и три учебно-практических пособия. Нынешняя работа отображает последни
изменения законодательной и иной нормативной правовой базы обеспечени
безопасности банка, а также особенности современной организации противо
действия угрозам банковскому делу.

Представленные в учебнике материалы содержат системное описание уг
роз безопасности банковской деятельности, правовых и организационных ос
нов противодействия им, а также техники обеспечения безопасности банка
Дается подробное описание особенностей наиболее распространенных видо
преступлений с посягательством на основные элементы безопасности банк
и способов их совершения. Предлагаются рациональные меры и приемы вы
явления, предупреждения и пресечения указанных преступных посягательств

Содержащиеся в книге материалы могут быть использованы для построе
ния оптимальной модели защиты банка от криминальных посягательств, соз
дания типовых программ выявления, предупреждения и пресечения конкрет
ных противоправных деяний ненасильственного характера.

Анализ проблем организации защиты банка и разработка соответствующи
рекомендаций выполнены на основе федеральных конституционных и феде
ральных законов, актов Президента РФ и Правительства РФ, ведомственны
и локальных нормативных актов. Для разработки методических рекомендаци
использовались результаты современных криминалистических исследований.

Курс дает необходимые знания в области защиты банковских инструмен
тов и технологий будущим работникам функциональных и контролирующи
подразделений кредитных организаций. Руководители и работники служ
безопасности банка получат из предлагаемых материалов современные реко
мендации правового, организационно-управленческого, технического, сыск
ного и криминалистического характера, которые будут способствовать повы
шению эффективности их профессиональной деятельности.

Представленные в работе рекомендации будут также полезными при под
готовке материалов для обращения в судебные органы с иском о возмещени
ущерба, причиненного банку противоправными посягательствами.

Работа «Безопасность коммерческого банка» состоит из девяти глав. Пер
вая из них посвящена общим вопросам теории банковской безопасности

писанию потенциально уязвимых мест банка со стороны криминальных уг
оз и иных рисков, системному представлению банковских угроз, а также
бязанностям банка в области разработки и реализации мер предупреждения
ротивоправных посягательств на его собственность и инфраструктуру.

Во второй главе курса рассматриваются вопросы правового обеспечения
анковской безопасности, роль и место в указанной сфере правовых актов ор
анов государственной власти, Банка России и внутренних (локальных) нор
мативных актов банка. Даются рекомендации по эффективному использова
нию правовой базы в конкретных случаях и по созданию системы внутренних
локальных) нормативных актов банка.

Третья глава посвящена вопросам организации системы безопасности бан
а, включающей в себя организацию внутреннего контроля и службы безо
асности.

Содержание четвертой главы охватывает проблемы применения техниче
ких средств для обеспечения безопасности банка. В ней рассматриваются ви
ы технических средств, их назначение, способы и условия применения в це
ях охраны банка, защиты банковских операций и продуктов, а также для ре
шения задач криминалистического и сыскного плана.

Пятая, шестая и седьмая главы содержат подробное описание видов пре
ступных посягательств на имущество и порядок функционирования банка.
В них с использованием данных современной правоохранительной практики
ается описание типичных признаков преступных посягательств на интересы
анка. Излагаются способы выявления, предупреждения и пресечения проти
оправной деятельности.

Глава восьмая посвящена новому направлению деятельности банка — уча
тию кредитной организации в противодействии отмыванию преступных до
одов и финансированию терроризма. Ее содержание охватывает понятие
правовую характеристику легализации (отмывания) доходов, полученных
реступным путем, криминалистическую характеристику указанного преступ
ения и систему мер предупреждения противоправных деяний указанного ви
а. Глава содержит впервые разработанные рекомендации по организации вы
явления признаков легализации преступных доходов.

Девятая глава концентрирует внимание на информационном обеспечении
езопасности банка. Она включает в себя описание видов и правовых основа
ий использования информации в целях обеспечения безопасности, а также
сточников информации. Глава содержит конкретные адреса общедоступных
нформационных ресурсов, имеющих важное значение для поисковой дея
ельности и оценки банковских рисков. В ней дается детальное описание од
ого из названных ресурсов — кредитных историй, а также излагаются дан
ые о возможностях применения специальных аналитических технологий для
ыявления и предупреждения противоправных посягательств на безопасность
анка.

Курс «Безопасность коммерческого банка» предназначен для студенто высших учебных заведений, осуществляющих подготовку по специальност «Финансы и кредит», однако может быть применен и для других экономиче ских специальностей. Его с успехом можно использовать для послевузовско переподготовки экономических кадров, повышения квалификации, а так как практическое пособие для работников служб безопасности и внутренне контроля банков, следователей (дознавателей) правоохранительных органо специализирующихся на расследовании преступлений в сфере экономическо деятельности, прокурорских работников, осуществляющих надзор за рассл дованием. Из него могут извлечь пользу преподаватели, научные работники о разовательных учреждений юридического и экономического профиля и кр читателей, интересующихся проблемами обеспечения безопасности в креди но-финансовой сфере.

Глава 1

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ БЕЗОПАСНОСТИ БАНКА

- Понятие и концепция безопасности банка
- Банк как объект противоправных посягательств
- Система угроз безопасности банка
- Банк как субъект борьбы с противоправными посягательствами

1.1. Понятие и концепция безопасности банка

Деятельность по защите интересов кредитной организации предполагает наличие у осуществляющих ее лиц четких представлений о содержании понятия «безопасность банка». Указанные знания должны представлять собой своего рода программу обеспечения безопасности организации в «свернутом» виде. Основной критерий их истинности — практическая пригодность для использования в процессе построения и функционирования системы безопасности.

Последнее десятилетие в жизни нашей страны характеризуется появлением значительного числа научных работ, методических разработок, различного рода организационных документов (концепций и программ), посвященных проблемам безопасности. Высока и законодательная активность в этой сфере. Знаковым событием здесь, несомненно, является принятие Закона РФ от 5 марта 1992 г. № 2446-1 «О безопасности»[1] (далее — Закон о безопасности). Вслед за ним был принят ряд законов и других нормативных правовых актов, посвященных безопасности различных отраслей, видов и направлений деятельности. В настоящее время насчитывается более чем 3500 ед. документов правового характера, регулирующих порядок обеспечения безопасности в различных сферах жизнедеятельности Российского государства. В их числе федеральные законы, указы Президента РФ, ведомственные нормативные акты, требования, правила, программы и т. п.[2]

Вместе с тем, результаты современных исследований в этой сфере свидетельствуют, что четких представлений о содержании и структуре понятия «безопасность», отражающих действительное положение вещей, наука до настоящего времени не сформулировала.

Аналогичный недостаток присущ и законодательным актам, регулирующим отношения в области безопасности. Например, ст. 1 Закона о безопасности определяет безопасность как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».

---

[1] В ред. Закона РФ от 25 декабря 1992 г. № 4235-1, Указа Президента РФ от 24 декабря 1993 г. № 2288, Федеральных законов от 25 июля 2002 г. № 116-ФЗ, от 7 марта 2005 г. № 15-ФЗ, от 25 июля 2006 г. № 128-ФЗ, от 2 марта 2007 г. № 24-ФЗ // СПС «КонсультантПлюс» (www.consultant.ru).

[2] *Гамза В. А., Ткачук И. Б.* Безопасность коммерческого банка: Организационно-правовые и криминалистические проблемы: монография. М.: Изд-ль Шумилова И. И., 2002. С. 24.

Основной недостаток формулы — нераскрытость содержания и объема самого понятия «защищенность» на уровне, достаточном для того, чтобы служить основой для четкого понимания сути проблем и путей их решения. Не многого нового для раскрытия понятия «безопасность» дают и другие законодательные акты Российской Федерации.

Такие определения безопасности из-за своей расплывчатости малопригодны для решения практических задач правового, организационного, криминалистического, технического и прочих видов защиты конкретных объектов. По существу, они представляют собой описание признаков безопасности как явления и не вскрывают его сущности.

Между тем, определение понятия «безопасность», согласно высказыванию К. Х. Ипполитова, «...не спор о дефинициях, не отвлеченная игра понятий, а сугубо методологический вопрос, так как на основе принятого определения этого понятия, его сущности и внутренней структуры можно будет подойти к определению и классификации угроз, определить систему обеспечения безопасности, место и роль субъектов в этой системе и сформулировать их задачи и функции...»[1].

Особого внимания заслуживают результаты научных исследований и правового регулирования проблем безопасности в кредитно-финансовой сфере. В силу исторических особенностей зашита этой сферы от различного рода опасностей постоянно совершенствовалась на протяжении всего времени существования кредитных организаций. Проблемам ее безопасности посвящались многочисленные научные и методические разработки отечественных и зарубежных исследователей. Не менее активным был процесс правового нормативного регулирования. В частности, правовой сервер профессиональной юридической системы «Кодекс» содержит свыше 1000 документов законодательного, нормативно-технического и методического характера, в которых в большей или меньшей степени затрагиваются вопросы обеспечения безопасности кредитно-финансовой и банковской деятельности. Однако определение понятий безопасности банка и кредитно-финансовой деятельности в них отсутствует.

Показательно, что Федеральные законы от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (в ред. от 26 апреля 2007 г. № 63-ФЗ) (далее — Закон о Банке России) и от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» (в ред. от 3 марта 2008 г. № 20-ФЗ) (далее — Закон о банковской деятельности), содержащие ряд специальных предписаний, фактически посвященных обеспечению безопасности банков, не только игнорируют понятие «безопасность», но и не предполагают обеспечение безопасности в качестве цели законодательного регулирования. До настоящего времени Банк России не издал ни одного нормативного либо

[1] *Ипполитов К. Х.* Экономическая безопасность России в условиях формирования рыночных отношений и система мер ее обеспечения. М.: РСПП, 1996. С. 8.

инструктивно-методического документа, специально посвященного проблеме безопасности коммерческих банков.

Статья 56 Закона о Банке России называет главной целью банковского регулирования и надзора *поддержание стабильности банковской системы* и защиту интересов вкладчиков и кредиторов. Статья 62 Закона о Банке России предоставляет Банку России право устанавливать обязательные нормативы «в целях обеспечения *устойчивости* кредитных организаций». Между тем, понятия «устойчивость» и «надежность» — всего лишь ступенька к полному представлению о безопасности. Согласно современным воззрениям, категория «устойчивость» является составной частью понятий «целостность» и «надежность»[1], которые, в свою очередь, входят в число элементов, характеризующих понятие «безопасность». Что же касается понятия «стабильный», то оно служит в русском языке одним из синонимов слова «устойчивый». Как видим, круг используемых в названных законах терминов замкнулся, не раскрыв сути понятия «безопасность кредитных организаций (банка)».

В качестве объяснения ситуации можно предположить, что в данном случае усилия законодателя были направлены на осмысление и решение проблем прикладного характера. Вопросы же принципиального свойства были оставлены «на потом».

Тем не менее, благодаря выполненным ранее научным наработкам и накопленному практическому опыту решения частных проблем, обобщенному и зафиксированному в нормативных правовых и иных предписаниях, а также в методических рекомендациях (в том числе криминалистического характера), современная наука имеет реальную возможность раскрыть понятие безопасности «вообще» и понятие безопасности банка, в частности, на уровне, отвечающем потребностям сегодняшнего дня.

Следует отметить, что такая попытка предпринята составителями Большого экономического словаря, по мнению которых безопасность банка «...представляет собой состояние защищенности его жизненно важных интересов от недобросовестной конкуренции, противоправной деятельности криминальных формирований и отдельных лиц, способность противостоять внешним и внутренним угрозам, сохранять стабильность функционирования и развития в соответствии с уставными целями»[2]. Однако, несмотря на определенные достоинства (обозначение некоторых источников опасности, попытки классифицировать виды угроз, указание на стабильность функционирования и развития как на объект защиты), это определение страдает рядом недостатков общепринятого подхода к решению проблемы. Нераскрытыми остаются важные в методологическом плане «состояние защищенности» и «жизненно

[1] *Солодкая М. С.* Надежность, эффективность, качество систем управления // Credo. 1999. № 17 (www.credo.osu.ru).

[2] Большой экономический словарь / под ред. А. Н. Азрилияна. 6-е изд., перераб. и доп. М.: Институт новой экономики, 2004. С. 75.

е интересы». Весьма общим является нынешнее представление о видах

ределенную трудность в процессе разработки современного определе-
нятия «безопасность банка» представляет задача упорядочения и ос-
ния на новом уровне значительного по объему и крайне разнородного
ржанию материала практики.
озиций системного подхода «безопасность» представляет собой слож-
ногоуровневую систему. Следовательно, адекватное знание о ней тоже
быть представлено в виде системы (системной характеристики). Пер-
о следует учитывать при построении системной характеристики поня-
зопасность», — это вопрос об основаниях систематизации относящих-
му сведений. Таким основанием должно служить нечто общее, прису-
ем видам накопленных сведений о понятии «безопасность».
чение проблемы с использованием универсального принципа отбора
венных свойств[1] показывает, что для описания явления безопасности
ций банка оптимальным является применение в качестве «единицы
а» понятия «человеческая деятельность».
ласно воззрениям современной социальной философии, человеческая
ность является стержневым элементом общества. «Общество, — по об-
му выражению Г. В. Иващенко, — есть деятельность преследующего
ели человека. Деятельность есть способ существования социального,
соб, которым существует общество»[2]. Вполне очевидно, что понятие
асность» возникает лишь в связи с появлением человека и его деятель-
. Представление о человеческой деятельности, как об условии сущест-
я субъекта в рамках общества, вполне очевидно иллюстрируется
ько на уровне деятельности индивида, но и на уровне функционирова-
зличного рода социальных объединений, в том числе кредитных орга-
й, банков. Банк, например, создается для выполнения определенного
ятельности и существует постольку, поскольку эта деятельность осуще-
ся. Подавляющее большинство опасностей для банка связано именно
еятельностью, с непосредственным выполнением банковских опера-
Прекращение банковских операций (даже при условии сохранности всех
элементов структуры этой организации) ведет к ликвидации банка.
гласно п. 2 ст. 20 Закона о банковской деятельности, задержка начала
ствления банковских операций, предусмотренных лицензией более чем
со дня ее выдачи, является основанием для отзыва у банка лицензии

Суть принципа заключается в том, что «свойства изучаемого объекта перебирают до тех
а набор не начнет вести себя детерминированно. Если исключение какого-то свойства
а не изменяет его детерминированного поведения, то, значит, это свойство не относится
существенных». *Ахлибинский Б. В., Ассеев В. А., Шорохов И. М.* Принцип детерминизма
ных исследованиях. Л.: ЛГУ, 1984. С. 49–50.

Иващенко Г. В. О понятии «безопасность» // Credo. 1999. № 24. (www.credo.osu.ru).

на осуществление банковских операций. В свою очередь, отзыв лицензии представляет собой начало процедуры ликвидации банка как такового.

Место безопасности в системе человеческой деятельности вполне наглядно выявляется в процессе структурирования понятия «деятельность». Последняя, как известно, являясь специфической формой активного поведения человека (коллектива, организации), включает в себя цель, средство, результат и сам процесс. При этом оценка деятельности дается с учетом ее нравственной ориентированности и соответствия нормам права[1].

Иными словами, понятие безопасности включает в себя субъекта (в виде социального индивида или группы лиц), который реализует собственную программу деятельности в соответствии с установленными в обществе нравственными и правовыми предписаниями, использует для этого соответствующие средства и способы и достигает намеченных результатов для удовлетворения своих потребностей.

Субъектом безопасности банковской деятельности является банк (разновидность кредитной организации), основная цель деятельности которого, согласно ст. 1 Закона о банковской деятельности, — извлечение прибыли путем осуществления предусмотренных законом банковских операций. Средствами достижения цели служат имущество банка и его инфраструктура (своего рода инструменты и технологии банковской деятельности, кадровый состав и нематериальные активы, позволяющие извлекать прибыль).

При таком подходе понятие безопасности оказывается непосредственно связанным с условиями деятельности субъекта. Если условия, которые включают в себя, наряду с внешними факторами, используемые субъектом материальные средства, кадровый состав, его теоретические знания и навыки, а также применяемые банком технологии, позволяют достичь намеченных целей, их (условия) следует считать в целом благоприятными (безопасными) для деятельности. Таким образом «...безопасность — не есть состояние защищенности интересов субъекта, безопасность вообще не есть чье бы то ни было состояние. Безопасность есть *условия существования субъекта,* контролируемые им. Безопасность, в общем виде, — есть специфическая совокупность условий *деятельности*»[2]. Это обстоятельство четко подмечено на практике. Именно по названной причине в процессе организации условий того или иного вида деятельности речь идет о безопасности конкретных видов работ (функционирования АЭС, полетов, подводных и строительных работ и т. д.).

Продолжая анализ, необходимо провести различие между объективной безопасностью, которая существует независимо от представлений о ней у субъекта, и собственными представлениями субъекта, оценивающего условия деятельности как безопасные. В последнем случае оценка может не соответствовать действительности. Применяемое ныне описание безопасности как

[1] Новая философская энциклопедия: в 4 т. Т. 1. М.: Мысль, 2001. С. 633–634.

[2] *Иващенко Г. В.* О понятии «безопасность» // Credo. 2000. № 24. (www.credo.osu.ru).

ıние защищенности» от различного рода угроз является прямым поро-
м субъективных представлений о безопасности и лишено конкретного
еского смысла.

не очевидно, что осмысление понятия безопасности, непосредствен-
анного с реальными проблемами, следует начинать с определения тер-
опасность вообще» и «опасность для банка», в частности. Исходя из из-
ых соображений, представляется, что в основе понятия «опасность»
некий источник потенциального ущерба с возможностью причинения
имуществу и (или) инфраструктуре субъекта. Ущерб, нанесенный ука-
элементам структуры субъекта, в свою очередь, препятствует достиже-
амеченных субъектом результатов и может в своих крайних формах
ги к прекращению существования субъекта. На практике «потенциаль-
щерб» реализуется в виде *действий* либо *явлений*. При этом понятие
вие», применяемое для определения специфических форм человече-
ктивности, относится только к деятельности человека. Ущерб, причи-
й различного рода явлениями без непосредственной связи с действия-
кретных лиц (стихийные явления, кризис, техногенные катастрофы
относится к «обстоятельствам»[1].

ответствии с указанным делением, применительно к механизмам реа-
и опасности, нами будут использоваться понятия «угроза действий»
за обстоятельств».

летом принятого положения, что суть понятия безопасности субъекта
ается в безопасности его деятельности, методологической основой
ассификации видов безопасности является классификация видов че-
ской деятельности. По этой причине *проблемы безопасности банка сле-
ассматривать в первую очередь как проблемы безопасности банковской
ьности*. Исходя из сказанного, термин «опасность» применительно
у (банковской деятельности) следует понимать как действия или об-
ьства, способные нанести ущерб установленному порядку функцио-
ния банка (процессу деятельности), его имуществу и инфраструктуре
гвам деятельности), воспрепятствовать достижению банком уставных
и привести в своих крайних формах к прекращению существования

спечение *безопасности банка* (как и любого иного субъекта) представля-
ой процесс создания благоприятных условий деятельности, при которых
уются интересы субъекта и осуществляются поставленные им цели. По-
у понятие «деятельность» складывается из совокупности конкретных
ий, вполне правомерно вести речь о безопасности конкретных банков-
пераций и сделок, о безопасности действий, обеспечивающих банков-
перации, и т. д.

иза В. А. Методологические основы системной классификации банковских рисков // кое дело. 2001. № 6, 7.

С учетом сказанного *безопасность банка* следует рассматривать как *совокупность условий, при которых потенциально опасные для банка действия или обстоятельства предупреждены, либо сведены к такому уровню, при котором они не способны нанести ущерб установленному порядку функционирования банка, сохранению и воспроизводству его имущества и инфраструктуры и воспрепятствовать достижению банком уставных целей.*

Задача создания благоприятных условий банковской деятельности (обеспечение безопасности банка) является законодательно установленной обязанностью государства, представительных и исполнительных органов банка. Усилия названных субъектов (в первую очередь — банка) должны быть направлены на формирование профессионально подготовленного коллектива, овладение соответствующими знаниями и навыками, приобретение необходимого имущества и технологий, на принятие мер организационного и иного характера, позволяющих сохранять и воспроизводить ценности. Иными словами, — *контролировать условия существования и функционирования* банка. Поскольку возможности такого контроля ограничены объективными условиями, в реальной жизни речь может идти только о том или ином *уровне безопасности*, т. е. об относительной безопасности банка или отдельных элементов его деятельности в виде конкретных банковских операций.

Для характеристики уровня защищенности банка и его конкретных операций от источников потенциальной опасности в экономической науке и в банковской практике используется термин «риск», который является составным элементом (продолжением) понятия «опасность». Риск или степень риска представляет собой сочетание вероятности опасного события и тяжести его последствий.

Понятие «риск» в качестве меры допустимо (или недопустимо) опасных условий деятельности (или действий) используется не только в коммерческой и финансовой деятельности, но и в иных видах деятельности, как правило, связанных с источниками повышенной опасности[1].

В настоящее время в этом качестве термин «риск» применяется также и в Уголовном кодексе Российской Федерации (УК РФ) (ст. 41 «Обоснованный риск» и ст. 61 «Обстоятельства, смягчающие наказание»). Однако во всех других случаях Уголовный кодекс РФ использует в качестве меры опасности понятие «угроза». Исследование содержания понятий «риск» и «угроза» свидетельствует об их частичном совпадении. Общим в содержании названных понятий является то, *что оба они используются в качестве меры опасности.*

---

[1] См.: Гражданский кодекс РФ; Федеральные законы от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (в ред. от 26 апреля 2007 г. № 63-ФЗ), от 21 июля 1997 г. № 177-ФЗ «О безопасности гидротехнических сооружений» (в ред. от 18 декабря 2006 г. № 232-ФЗ), от 9 января 1996 г. № 3-ФЗ «О радиационной безопасности населения» (в ред. от 22 августа 2004 г. № 122-ФЗ); Концепцию национальной безопасности Российской Федерации, утв. Указом Президента РФ от 17 декабря 1997 г. № 1300; Методические указания по проведению анализа риска опасных промышленных объектов, утв. постановлением Госгортехнадзора России от 12 июля 1996 г. № 29.

в процессе их структурирования по таким позициям, как источник
новения, отношение к субъекту безопасности и допустимость возник-
ия с точки зрения права, выявляются существенные различия. Анализ
ывает, что отличительными особенностями риска являются:
сфера реализации — предпринимательская (в том числе кредитно-фи-
зая) и производственная деятельность, другие отношения, регулируемые
нским законодательством;
источник возникновения — собственные действия или решения субъ-
езопасности (предпринимателя, банка). Это принципиальное положе-
фиксировано в ст. 2 Гражданского кодекса РФ (ГК РФ), которая опре-
«предпринимательскую деятельность» как «самостоятельную, осущест-
лю *на свой риск*». Дальнейшее негативное развитие событий может быть
о с опасными действиями посторонних лиц (в том числе и противо-
ми) или опасными явлениями, которые субъект безопасности не пред-
или неправильно оценил;
содержание риска с точки зрения права — ошибка субъекта безопасно-
и его сотрудников;
допустимость существования риска. Согласно теории банковских рис-
уществование последних является нормальной составляющей любой
рческой деятельности. Снижение уровня риска прямо связано с умень-
м вероятности получить высокую прибыль[1]. По этой причине защи-
ость банка в сфере извлечения прибыли принято понимать как опти-
ое соотношение между уровнем существующих рисков и прибыльно-
анковской деятельности.
и этом задача субъекта безопасности заключается в так называемом эф-
вном управлении рисками. Цель управления рисками в указанном
е — это достижение посредством имеющихся в распоряжении банка ад-
тративных и экономических механизмов уровня защищенности, позво-
его банку извлекать достаточную прибыль и распределять ее в соответ-
с установленными нормативами и договорами[2].
ходя из указанных выше подходов, в коммерческой и банковской прак-
принято разграничивать риски на приемлемые (допустимые, условно до-
мые) и неприемлемые (недопустимые).
новные источники регулирования отношений, связанных с рисками
дитно-финансовой сфере, — Гражданский кодекс РФ, Законы о Банке
и и о банковской деятельности.
личительные особенности угроз:
сфера реализации — любые виды человеческой деятельности (включая
ринимательскую, производственную и проч.) и отношений между людьми;

Ивасенко А. Г. Банковские риски. М.: Вузовская книга, 1998.

Положение Банка России от 16 декабря 2003 г. № 242-П «Об организации внутреннего
ля в кредитных организациях и банковских группах».

2) источник возникновения угроз — действия или решения лица (лиц), посторонних по отношению к субъекту безопасности (предпринимателю, банку)[1]. Опасные явления, не связанные с человеческой деятельностью, к числу угроз в данном случае не относятся;

3) содержание угрозы с точки зрения права — противоправные, уголовно наказуемые действия.

Основной источник регулирования отношений, связанных с угрозами в кредитно-финансовой сфере, — Уголовный кодекс РФ.

Принципиальная недопустимость угроз с точки зрения уголовного права. «Угроза», в контексте уголовного законодательства связана с умышленными противоправными действиями посторонних лиц в отношении охраняемого субъекта (субъекта безопасности) и характеризуется недопустимо высокой степенью опасности. По этой причине некоторые виды угроз сами по себе являются уголовно наказуемым деянием (угроза убийством или причинением тяжкого вреда здоровью — ст. 119 УК РФ) или отягчающим обстоятельством. Уровень «угрозы», в отличие от уровня «риска», не может быть оценен как «приемлемый» ни при каких обстоятельствах, поскольку с точки зрения уголовного законодательства угроза — явление, принципиально недопустимое.

Следует отметить, однако, что исследования в области экономических дисциплин и нормативные акты, регулирующие отношения в области коммерческих и банковских рисков, в отличие от уголовного права, различий между «риском» и «угрозой» не проводят, ставя в один ряд, например, «риски», вызываемые последствиями некомпетентных решений отдельных работников, и неправомерные действия в виде хищения ценностей банка[2].

Ситуации, когда одно и то же обстоятельство лежит в основе «риска» и в основе «угрозы», вполне вероятны. Однако следует четко представлять, что в таких случаях обстоятельство (речь идет о событии противоправного характера) рассматривается с точки зрения разных субъектов. С одной стороны, возможен «риск» предпринимателя, столкнувшегося в результате принятого им решения с непредвиденными противоправными действиями злоумышленника (мошенника, расхитителя). С другой стороны, действия самого злоумышленника, причастного к указанному событию, следует рассматривать как «угрозу».

Итак, с учетом сказанного, условия безопасного функционирования банка предполагают, что он огражден от угроз (действий преступного характера — преступлений) и снабжен средствами надежного управления рисками (которыми являются опасные для деятельности банка действия и явления, возникающие в связи с принятием сотрудниками банка определенных решений).

[1] Лиц из числа сотрудников организации — субъекта безопасности также следует считать «посторонними» в случае, если совершаемые ими действия (угрозы) расходятся с целями организации и не соответствуют нормам права.

[2] Положение Банка России от 16 декабря 2003 г. № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах».

ее проблема безопасности банка будет рассматриваться в «узком смыс-
через призму обеспечения охраны данного объекта от угроз преступных
гельств. Поскольку ведущая роль в обеспечении безопасности банка
анного вида угроз отведена мерам уголовно-правового характера, суть
ных мер состоит в установлении уголовной ответственности за совер-
преступлений, посягающих на интересы банка.

ичие связей между видами деятельности банка и мерами их уголов-
вовой защиты особенно рельефно проявляется в результате возникно-
новых элементов банковской деятельности. Например, в течение по-
го десятилетия в числе «средств деятельности» банка появились компь-
ре оборудование и компьютерные программы. «Процесс деятельности»
ополнился новыми видами банковских услуг, операций и технологий,
и субъектами деятельности в виде работников коммерческой (а не госу-
енной) организации. Вследствие этого возникла потребность в уго-
-правовой защите указанных элементов деятельности от преступных
ительств (угроз). Названная потребность была реализована введением
вный кодекс РФ ряда новых статей, прямо или косвенно связанных
овской деятельностью[1]. В целях защиты от преступлений в сфере ком-
ной информации, получивших распространение в сфере банковской
х видов деятельности, были приняты ст. 272 «Неправомерный доступ
льютерной информации», ст. 273 «Создание, использование и распро-
ние вредоносных программ для ЭВМ» и ст. 274 «Нарушение правил
атации ЭВМ, системы ЭВМ или их сети».

исле статей Уголовного кодекса РФ, посвященных непосредственно за-
банковской деятельности, появились ст. 172 «Незаконная банковская
ьность», ст. 176 «Незаконное получение кредита», ст. 177 «Злостное ук-
е от погашения кредиторской задолженности» и ст. 183 «Незаконные
ние и разглашение сведений, составляющих коммерческую, налоговую
нковскую тайну».

практике надежность защиты банка мерами уголовно-правового харак-
значительной мере зависит от того, насколько эффективными окажутся
криминалистического характера, которые применяются в целях выявле-
исследования и предупреждения упомянутых преступных посягательств.
ределенным вкладом в повышение результативности методов кримина-
ки в указанном случае могут служить результаты системного анализа по-
«безопасность банка». Они позволяют представить «безопасность бан-
качестве сложной многоуровневой системы, функционирование кото-
беспечивается различными видами и направлениями человеческой
ьности. Выделение понятия «деятельность банка» в качестве системооб-
щего элемента «безопасности» дает возможность ответить на важные
одологическом плане вопросы: какие элементы структуры деятельности

[1] *Гамза В. А.* Защищать инвестора // Содружество. 2001. № 15–16.

банка являются объектами потенциальных угроз: какие именно опасности угрожают этим объектам; каковы возможные отрицательные последствия указанных угроз; какие меры следует принять для их предотвращения или локализации.

Результаты системного анализа служат методологической основой:

- прогнозирования, выявления новых видов угроз безопасности банка по мере изменения содержания его деятельности (появления новых средств деятельности, новых услуг и новых технологий);
- разработки и совершенствования криминалистических характеристик преступлений, посягающих на безопасность банка и методик решения поисково-познавательных задач в уголовном процессе;
- уточнения задач и функций субъектов, участвующих в обеспечении безопасности банка;
- описания с позиций криминалистики всех известных практике видов угроз безопасности банка и создания на их базе алгоритмов деятельности субъектов, участвующих в обеспечении безопасности банка;
- проведения анализа фактического состояния безопасности конкретного объекта (банка) и для разработки адекватных методов криминалистической защиты банковской деятельности в современных условиях.

Основные понятия и определения

Безопасность — специфическая совокупность внутренних и внешних условий деятельности, позволяющих субъекту контролировать процесс собственного существования и достигать намеченных целей указанной деятельности.

Безопасность банка (банковская безопасность) — совокупность внешних и внутренних условий банковской деятельности, при которых потенциально опасные для банковской системы (отдельного банка) действия или обстоятельства предупреждены, пресечены либо сведены к такому уровню, при котором не способны нанести ущерб установленному порядку банковской деятельности (функционированию банка, сохранению и воспроизводству имущества и инфраструктуры банковской системы или отдельного банка) и воспрепятствовать достижению банком уставных целей.

Опасность — источник потенциального ущерба имуществу или инфраструктуре банка, причинение которого может воспрепятствовать достижению банком уставных целей.

Риск (банковский) — мера допустимо (или недопустимо) опасных условий деятельности банка, неблагоприятные последствия которых реализуются в связи с ошибочными действиями (решениями) или бездействием персонала банка. Основной источник правового регулирования отношений, связанных с рисками, — Гражданский кодекс РФ.

Угроза — мера опасности деятельности банка, связанная с противоправными, наказуемыми действиями лиц (как правило, посторонних по отношению

су). Основной источник регулирования правовых отношений, связанных
зами, — Уголовный кодекс РФ.
юза безопасности банка (банковской безопасности) — уголовно наказуе-
иное противоправное деяние (действие либо бездействие), посягающее
ущественные и приравненные к ним права и интересы банка, либо на
ок его функционирования.

1.2. Банк как объект противоправных посягательств

работка системного описания существенных свойств банка как объекта
воправных посягательств является одной из насущных задач теории
ктики банковской безопасности. Практическая деятельность, направ-
я на обеспечение безопасности банка, связана с решением широкого
проблем. Она включает в себя необходимость выполнения большого
ia разноплановой работы, начиная с постановки общих задач выявления,
преждения и расследования преступных посягательств и заканчивая раз-
кой и организацией применения конкретных мер, из которых складыва-
истема защиты банка.
ред субъектами, участвующими в обеспечении безопасности, стоят зада-
лучения, переработки и использования обширной информации о потен-
но уязвимых элементах структуры банка, об угрожающих им опасно-
о видах и способах защиты от них, о рациональном распределении
щихся сил и средств обеспечения безопасности. В связи с необходимо-
упрощения указанных задач возникает потребность в разработке инстру-
, использование которого позволило бы, с одной стороны, охватить еди-
взором всю иерархию указанных выше целей, не тратя усилий на второ-
нные детали.
казанными качествами обладает криминалистическая модель, описываю-
банк в целом как объект преступных посягательств. Оценивая научные
ктические достоинства такой модели применительно к задачам обеспе-
я безопасности банка, следует отметить возможность ее применения в ка-
е логической основы для решения задач познавательного, управленческо-
оискового и иного характера. Полученная с ее использованием информа-
может эффективно применяться в процессе построения и организации
ционирования системы обеспечения безопасности банка, а также в уго-
ом процессе. Кроме того, такая модель может выступать в качестве инст-
нта в научных криминалистических исследованиях, поскольку, в силу
ущих моделям свойств, она может быть использована в качестве аналога
выявления еще непознанных объективно существующих обстоятельств,
тых связей и невыявленных отношений[1].

[1] Новая философская энциклопедия: в 4 т. Т. 1. М.: Мысль, 2004. С. 596.

До настоящего времени попытки специального криминалистического описания банка в качестве объекта (предмета) преступных посягательств отечественными исследователями не предпринимались. Объективно это объясняется сравнительно недавним появлением частных коммерческих кредитных организаций в России и отсутствием достаточного периода времени для научного осознания и реализации назревшей потребности.

Потребность в обеспечении безопасности банка средствами и методами криминалистики, по мнению белорусского профессора Г. А. Зорина, обусловлена объективными факторами, среди которых:

а) возникновение новой самостоятельной отрасли правового регулирования — банковского права и, следовательно, новых видов уголовно-правовых нарушений этого регулирования;

б) появление необходимости адекватного криминалистического противодействия указанным преступным посягательствам;

в) специфика организации, функционирования и структуры банковской системы, требующей определенной организации мер защиты криминалистического характера.

Общеизвестно, что криминалистика, предпринимая системные описания разнообразных общественно опасных деяний, движется в направлении разработки и совершенствования криминалистических характеристик преступлений. Указанные характеристики, без сомнения, являются эффективным инструментом для решения задач борьбы с конкретными видами преступлений.

Однако современная практика свидетельствует о потребности дополнить имеющиеся разработки криминалистическими характеристиками (криминалистическими моделями) *объектов защиты*, к числу которых относится банк. Тенденция к созданию системных характеристик объектов, подвергающихся различного рода угрозам, уже нашла определенное отражение в отечественном законодательстве.

Наиболее цельно она отразилась в сфере обеспечения безопасности объектов реального сектора производства. Речь идет, в частности, о Федеральных законах от 21 июля 1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов» (в ред. 18 декабря 2006 г. № 232-ФЗ), от 21 июля 1997 г. № 117-ФЗ «О безопасности гидротехнических сооружений» (в ред. от 18 декабря 2006 г. № 232-ФЗ) и некоторых других законодательных актах. В них, в числе требований о выполнении соответствующих мер защиты, законодатель установил обязательность разработки специальных документов, получивших наименование «деклараций безопасности опасных производственных объектов». Указанные «декларации» по своей сути представляют не что иное, как системное описание объекта защиты, а изложенные в «декларации» материалы должны служить методической основой для осуществления мер правового, экономического и социального характера, обеспечивающих безопасную эксплуатацию объектов и направленных на предупреждение угроз

видацию их вредных последствий[1]. К сожалению, системное описание в качестве объекта повышенной опасности по отношению к преступ-сягательствам в отечественной научной литературе до настоящего време-сутствует. Следует отметить, что государство предпринимает определенные законодательного (регулирующего), надзорного (административного) го характера, призванные обеспечивать безопасность банковской системы ом и отдельных коммерческих банков в частности.

ультатом государственного регулирования стала система законодатель-других нормативных предписаний государственных органов, представ-их своего рода «требования обеспечения безопасности банка». Отдель-азрозненные элементы, составляющие названные «требования», содержат-аконах о Банке России и о банковской деятельности и иных нормативных вых актах Российской Федерации (в первую очередь, в приказах, инст-иях, положениях и других документах Банка России), а также в норма-их технических документах, соблюдение которых обеспечивает банков-безопасность. По своему содержанию они представляют собой различ-рода условия, запреты, обязательные нормативы, ограничения и другие вания, которые подлежат обязательному исполнению в процессе орга-ции и функционирования банка. Практическая реализация «требований асности» является общей задачей государства и исполнительных органов ерческого банка. При этом подлежащие исполнению требования можно но разграничить на две группы.

ервая — включает в себя положения, относящиеся к организации банка док создания банка) и обеспечению функционирования банка в целом док функционирования банка). Согласно им банк обязан:

- соответствовать условиям достаточности и «правовой чистоты» происхождения уставного капитала;
- создавать резервы (фонды) на покрытие возможных убытков;
- соблюдать обязательные нормативы, устанавливаемые в соответствии с Законом о Банке России;
- иметь лицензию на деятельность банка и выполнение конкретных банковских операций;
- назначать на должности руководителей исполнительных органов и главного бухгалтера банка кандидатов, соответствующих квалификационным требованиям (в содержание которых входит, в частности, отсутствие судимости за совершение преступлений против собственности, хозяйственных и должностных преступлений);
- обеспечивать проведение подготовки и аттестации работников в области банковской безопасности;

[1] Положение о декларации безопасности промышленного объекта, утвержденное постановлением Правительства РФ от 1 июля 1995 г. № 675 «О декларации безопасности промышленного объекта Российской Федерации».

- выполнять требования нормативных правовых актов и нормативных технических документов, устанавливающих правила безопасности при осуществлении основных и вспомогательных банковских операций.

Вторая — относится к обязанности исполнительных структур банка организовывать и выявлять потенциальную опасность, принимать меры по предупреждению угрожающих банку действий и событий и локализации их вредных последствий. При этом исполнительные органы банка обязаны:

- организовывать и осуществлять внутренний контроль за соблюдением порядка управления банком и выполнения отдельных банковских операций;
- принимать меры, позволяющие уменьшать вероятность реализации угроз, а в случаях, когда это оказалось невозможным, снижать тяжесть нежелательных последствий;
- проводить внутренние расследования с целью выяснения причин событий, связанных с нанесением ущерба интересам банка;
- разрабатывать собственные рекомендации по уменьшению угроз интересам банка.

Определенные требования о разработке системы мер защиты банка, в том числе о прогнозировании возможных угроз преступных посягательств, содержатся в Положении Банка России от 16 декабря 2003 г. № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» (в ред. Указаний ЦБ РФ от 30 ноября 2004 г. № 1521-У) (далее — Положение Банка России № 242-П).

Представляется, однако, что система описания банка как объекта угроз и разработанные на основе указанного выше Положения меры защиты не позволяют решить реальных проблем обеспечения безопасности в полном объеме. Это объясняется, во-первых, методологическими недостатками названного нормативного акта. Во-вторых, система мер защиты банка, предусмотренная Положением, создается в качестве инструмента *административного управления безопасностью* (обеспечения безопасности) банка через управление *банковскими рисками*, значительная часть которых не носит криминального характера. По этой причине задача обеспечения безопасности банка от преступных посягательств требует разработки самостоятельной криминалистической модели, включая содержание, структуру и количество составляющих ее элементов. Проблему следует рассматривать через призму высказанных выше представлений о содержании понятий «деятельность банка» и «безопасность банка».

Отправными структурными элементами «деятельности банка» являются уже названные ранее элементы: *средства деятельности* банка и *процесс деятельности* банка.

Именно эти элементы понятия «деятельность банка» являются ведущими объектами преступных посягательств. Дальнейшая детализация понятий «средства деятельности банка» и «процесс деятельности банка» позволяет

ить криминалистическую модель банка, достаточную для решения за-
ретического и практического характера.
ая модель, представляющая в систематизированном виде объекты пре-
их посягательств, позволяет субъектам, участвующим в обеспечении
асности, упорядочить представления о способах и направлениях защи-
ка и более эффективно использовать полученную информацию на
ике.
гласно науке о банковском деле, все *средства банковской деятельности*
ая неимущественные права и нематериальные блага) являются состав-
астью «имущества банка», а все *виды деятельности, обеспечивающей*
ционирование банка и создание соответствующих условий для его функ-
рования, охватываются понятием «инфраструктура банка»[1].
ждый из основных блоков модели, какими являются «имущество»
раструктура» банка, в свою очередь, имеет свою внутреннюю структу-
обенности которой оказывают заметное влияние на виды и динамику
уплений, совершаемых в сфере банковской деятельности.
ким образом, модель банка как объекта противоправных посягательств
ся идеальным отражением реально существующего объекта потенци-
й опасности. Это понятие охватывает банк в целом и отдельные элемен-
структуры, в отношении которых возникает опасность противоправно-
сягательства.
онятие свойств банка как объекта не может быть сведено к сумме
тв его структурных элементов. В юридической практике это подтвержда-
ем, что «банк в целом» и деятельность «банка в целом» рассматриваются
одателем в качестве самостоятельных объектов уголовно-правовой
едовательно, и криминалистической) защиты. Это вытекает из ст. 172
Ф (незаконная банковская деятельность), которая рассматривает банк
деятельность в качестве объектов защиты от субъектов, не имеющих за-
ого права на занятие банковской деятельностью. В то же время состав-
ие банк структурные элементы защищаются системой других норм Уго-
ого кодекса РФ в соответствии с родовыми и видовыми особенностями
нных элементов.
ждый из двух основных блоков криминалистической характеристики
а («имущество» и «инфраструктура») по мере «развертывания» обнаружи-
свою внутреннюю структуру, которая формируется с учетом влияния гра-
ского и уголовного права. При более подробном рассмотрении элементы
теристики выявляют следующие особенности.

ущество банка. Понятие имущества банка тесно связано с понятием со-
ания права собственности на объекты имущества. Имущество банка
чает в себя наличные и безналичные деньги (национальная валюта),

Банковское дело: учеб. / под ред. О. И. Лаврушина. М.: Финансы и статистика, 1999.
-23.

валютные ценности и ценные бумаги (как его собственные, так и привлеченные средства), имущественные права на объекты банковской деятельности (предметы залога и т. п.), а также здания, оборудование и инвентарь.

Содержание права собственности в соответствии со ст. 209 ГК РФ заключается в признании и защите установленными законом способами права собственника владеть, пользоваться и распоряжаться своим имуществом. В том числе в установлении права защиты от преступных посягательств.

Преступные посягательства на имущество банка относятся к преступлениям против собственности, включенным в главу 21 УК РФ. Непосредственным объектом выступает одна из форм собственности (частная собственность акционеров банка). *Предмет* преступлений — вещи, составляющие движимое и недвижимое имущество банка.

С позиций уголовного права (и криминалистики) имущество банка может рассматриваться в качестве предмета (объекта) хищений (кража — ст. 158 УК РФ; мошенничество — ст. 159 УК РФ; присвоение или растрата — ст. 160 УК РФ; грабеж — ст. 161 УК РФ; разбой — ст. 162 УК РФ; вымогательство — ст. 163 УК РФ; хищение предметов, имеющих особую ценность, — ст. 164 УК РФ; причинение имущественного ущерба путем обмана или злоупотребления доверием — ст. 165 УК РФ; умышленные уничтожение или повреждение имущества — ст. 167 УК РФ; уничтожение или повреждение имущества по неосторожности — ст. 168 УК РФ.

Ввиду весьма широкого перечня объектов имущества банка в настоящей работе будут рассмотрены лишь те из них, которые имеют отношение к специфике банковской деятельности и совершаются ненасильственным путем. Прежде всего, это средства обеспечения активных банковских операций. Согласно науке о банковском деле, эти средства имеют наименование «активы банка». К ним относятся: кассовая наличность и приравненные к ней средства; инвестиции в ценные бумаги; ссуды; оборудование[1].

Криминалистически значимой, например, оказывается принадлежность активов банка к тому или иному виду доходной деятельности банка, а следовательно, и к обособленным суммам, предназначенным для обеспечения конкретных видов банковской деятельности.

От того, в каком виде банковской деятельности используются денежные средства (и в каких элементах структуры банковских активов они обособлены), зависят характер (способы совершения) и распространенность преступлений, конечной целью которых является завладение наличными деньгами.

Особую привлекательность для преступников, посягающих на собственность банка, имеют его активы в виде кассовой наличности и приравненных к ней средств (далее — денежные средства). С точки зрения решения задач криминалистики целесообразным является выделение таких видов денежных средств банка, как: *наличные деньги* (находящиеся в обращении банковские

[1] Банковское дело: учеб. / под ред. О. И. Лаврушина. М.: Финансы и статистика, 1999. С. 90.

ы, металлическая монета и иностранная валюта); *эквиваленты денежных пв* — ценные бумаги (чек, вексель, облигация), золотой сертификат Ми- рства финансов РФ и проч. Следует выделить также в качестве само- льного предмета преступных посягательств *платежные средства, не яв- иеся ценными бумагами, но служащие средством получения наличных денег*: тные либо расчетные пластиковые карты, платежные документы (пла- е поручения), депозитный сертификат и т. д.[1]

нфраструктура банка. Под инфраструктурой банка принято понимать со- ность элементов имущественного, правового, организационного харак- и устойчивых связей между ними, обеспечивающих порядок создания бильного функционирования банка. В теории банковского дела принято аничивать элементы внутренней и внешней инфраструктуры.

числа элементов *внутренней инфраструктуры*, представляющих интерес иминалистическом плане и служащих основанием для классификации риминалистически значимым признакам, можно выделить следующие:

внутренние правила совершения банковских операций и защиты инте- ресов банка, технология банковских операций;

порядок управления деятельностью банка (построение учета, отчетно- сти, аналитической базы, компьютерная обработка данных на основе современных коммуникационных систем);

кадровое обеспечение банка (система поиска, отбора сотрудников, мо- тивации сотрудников и т. д.);

информационное обеспечение банка.

орядок функционирования банка подвергается угрозам противоправного ктера во всех случаях посягательств на другие элементы структуры банка. объясняется тем, что любое из преступлений, направленное против инте- в банка, совершается путем грубого нарушения банковских правил, при- ных обеспечивать защиту интересов банка, его клиентов и корреспонден- з ходе совершения операций в сфере кредитования, расчетных, кассовых аций и т. п. С другой стороны, укрепление безопасности любого из эле- ов структуры банка непосредственно связано с совершенствованием по- а функционирования банка в целом и порядка осуществления отдельных ковских операций.

При более подробном рассмотрении понятие «порядок функционирования а» принято разграничивать на такие составляющие, как порядок совер- ия операций, установленный законодательными актами и внутренними илами с целью защиты интересов банка и его клиентов; порядок ведения а и отчетности; порядок управления деятельностью банка (в том числе азе современных коммуникационных систем); порядок информационного

[1] Подробнее криминалистические характеристики преступных посягательств на имущество а даны в книге: *Гамза В. А., Ткачук И. Б.* Безопасность коммерческого банка: учеб.-практ. по- е. М.: Изд-ль Шумилова И. И., 2000. С. 22–87.

обеспечения, призванный обеспечивать банк сведениями о надежности потенциальных и реальных клиентов, о возникновении конкретных угроз безопасности банка и т. д.

Преступные посягательства на порядок функционирования банка законодатель включил в гл. 23 УК РФ «Преступления против службы в коммерческих и иных организациях». Речь идет о деяниях, предусмотренных ст. 201 УК РФ «Злоупотребление полномочиями» и ст. 204 УК РФ «Коммерческий подкуп». Непосредственным объектом названных видов преступлений является нормальное функционирование управленческого аппарата коммерческой или иной организации (в том числе — банка).

Предметом преступлений является нарушение правил нормативного характера, определяющих направленность, регулирующих порядок и условия осуществления банковской деятельности, регламентирующих права и обязанности ее участников (законов, нормативных актов Банка России и других ведомств, внутренних нормативных актов коммерческого банка и т. д.).

Информация (информационные ресурсы) банка. Статья 128 ГК РФ относит информацию к одному из видов объектов гражданских прав, наряду с вещами, деньгами и ценными бумагами, иным имуществом, имущественными правами, работами и услугами, охраняемыми результатами интеллектуальной деятельности и нематериальными благами. На этом основании право собственности на информацию охраняется законом. В тех случаях, когда информация выступает в качестве товара, она является объектом договорных отношений, которые защищаются в порядке, предусмотренном Гражданским кодексом РФ.

С точки зрения криминалистики объектами защиты информации банка являются:

- система формирования, распространения и использования информационных ресурсов банка, включающая в себя информационные системы различного уровня и назначения, базы и банки данных, информационные технологии, в том числе регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический персонал разработчиков информационной системы банка, пользователей информационной системы банка и обслуживающий их персонал;
- информационная инфраструктура, включающая центры обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены компоненты информационных банковских систем, а также ведутся переговоры, содержащие информацию с ограниченным доступом;
- информационные ресурсы, содержащие сведения, отнесенные к защищаемой информации и представленной в виде носителей на магнитной

и оптической основе, информативных физических полей, информацион-
онных массивов и баз данных;
основные технические средства и системы, вспомогательные техниче-
ские средства, системы и сети связи;
вспомогательные технические средства и системы зданий, размещенные
в помещениях, где обрабатывается (циркулирует) информация, содер-
жащая сведения, отнесенные к защищаемым, а также сами помещения,
предназначенные для ведения конфиденциальных переговоров.
ветственность за неправомерные деяния в отношении объектов инфор-
ации в целом и банка, в частности, установлена соответствующими нор-
Гражданского кодекса РФ (ГК РФ), Уголовного кодекса РФ (УК РФ),
сса Российской Федерации об административных правонарушениях (да-
КоАП РФ), Трудового кодекса РФ (ТК РФ) и другими актами россий-
законодательства, а также внутренними документами организа-
собственников информации. Информация банка, защищаемая законом
роз преступного характера, в целом может быть разделена на два вида.
вому из них относятся сведения конфиденциального характера, состав-
ие коммерческую и банковскую тайну. Ответственность за преступные
ательства на них предусмотрена ст. 183 УК РФ «Незаконное получе-
разглашение сведений, составляющих коммерческую или банковскую
».
второму виду относится компьютерная информация. Уголовный ко-
РФ содержит три состава преступления, устанавливающих уголовное на-
е за преступные посягательства на информацию этого вида. Это ст. 272
равомерный доступ к компьютерной информации»; ст. 273 «Создание,
ьзование и распространение вредоносных программ для ЭВМ» и ст. 274
ушение правил эксплуатации ЭВМ, системы ЭВМ или их сети». Обяза-
ым признаком названных преступлений является наступление вредных
дствий.
рактическое значение для криминалистического обеспечения безопасно-
анка является систематизация его защищаемой информации по следую-
признакам:

по виду носителя, в котором она содержится (информация на матери-
альном носителе — бумажном, магнитном, в физическом поле и их раз-
новидностях или информация в устной форме);

по месту нахождения (информация, заключенная в документе, циркули-
рует в помещениях, в средствах вычислительной техники и связи);

по форме изложения (в формах текста, компьютерных программ).

адры банка. По оценке отечественных и зарубежных исследователей они
тся важнейшим внутренним источником риска. При этом в первую оче-
имеются в виду риски, связанные с принятием персоналом ошибочных ре-
й. Однако не исключаются и угрозы, связанные с противоправным поведе-
персонала. Последние, с точки зрения их выявления и предупреждения,

имеют существенные различия по своей внутренней структуре. Интенсивность, виды и цели возможных преступных посягательств на личный состав банка зависят от функциональных обязанностей и полномочий каждого конкретного сотрудника.

Самостоятельным направлением изучения является такой вид угроз безопасности кадрам банка, как принуждение сотрудников к совершению действий, противоречащих интересам банка (либо вовлечение их в преступную деятельность), а также внедрение в кадровый состав представителей криминальных и иных враждебных банку организаций.

Изучение проблемы «кадров банка» с точки зрения обеспечения безопасности выявляет прямую зависимость этого элемента (как и других элементов системы безопасности) от порядка функционирования банка и его частного направления — порядка кадрового обеспечения.

Объектами преступных посягательств на кадры банка являются конкретные сотрудники банка и установленный внутренними нормативными документами порядок приема сотрудников на работу и выполнения ими трудовых обязанностей.

Нематериальные блага банка. В соответствии с гражданским законодательством нематериальные блага относятся к одному из видов объектов гражданских прав (ст. 128 ГК РФ). Гражданский кодекс РФ не дает исчерпывающего перечисления видов нематериальных благ. Их наиболее полный систематизированный перечень содержится в ст. 150 ГК РФ, посвященной порядку осуществления и защиты нематериальных прав личности. Право на такую защиту законодательство России признает и за юридическими лицами. В соответствии с п. 7 ст. 152 ГК РФ правила о защите деловой репутации гражданина соответственно применяются и к защите деловой репутации юридического лица.

Наиболее полный систематизированный перечень нематериальных благ юридического лица содержится в Положении по ведению бухгалтерского учета и бухгалтерской отчетности в Российской Федерации, утвержденном приказом Министерства финансов РФ от 29 июля 1998 г. № 34 н.

Чаще всего объектом противоправных посягательств на нематериальные блага банка являются его деловая репутация и деловые связи. Как и другие виды объектов гражданских прав нематериальные блага защищаются законодательством России в первую очередь нормами Гражданского кодекса РФ. Кроме того, противоправные посягательства на деловую репутацию и деловые связи банка в соответствующих случаях квалифицируются как преступления, предусмотренные ст. 129 УК РФ «Клевета» и ст. 130 УК РФ «Оскорбление».

Предметом преступного посягательства на деловую репутацию с точки зрения криминалистики являются: сведения о банке, искажение которых может причинить вред уставным целям его деятельности (о финансовой надежности банка, профессиональных и личных качествах руководителей банка, уровне профессиональной подготовки и организации профессиональной

ьности персонала, соответствии деятельности банка законодательству
ормам деловой этики, соблюдении принятых банком обязательств, об от-
нии банка к интересам клиента и т. д.).
едметом преступного посягательства на деловые связи банка являются
и отношения, установившиеся между банком и его контрагентами
ессе банковской деятельности и способствующие получению банком
ных (либо потенциальных) доходов.

Основные понятия и определения

ебования обеспечения безопасности банка — система условий, запретов,
ичений и других обязательных требований, содержащихся в федераль-
аконах и иных нормативных правовых актах, а также в нормативно-тех-
ских документах, внутренних (локальных) нормативных актах банка, со-
ение которых призвано обеспечить безопасность банковской деятельно-

ъект противоправного посягательства — имущество банка и приравнен-
нему объекты гражданского права вне зависимости от вида и назначе-
обеспечения, нематериальные активы, руководство и персонал банка,
же система создания и функционирования банка, банковские технологии
дства их технического обеспечения.
одель банка как объекта противоправных посягательств — идеальное от-
ие реально существующего объекта потенциальной опасности.
мущество банка — наличные и безналичные деньги (национальная валю-
алютные ценности и ценные бумаги (собственные и привлеченные сред-
, имущественные права на объекты банковской деятельности (предметы
а и т. п.), а также здания, оборудование и инвентарь.
нфраструктура банка — совокупность элементов имущественного, пра-
го, организационного характера и устойчивых связей между ними, обес-
вающих порядок создания и стабильного функционирования банка.
анковская технология — упорядоченная совокупность функционально
формационно взаимосвязанных операций, действий, работ и процедур,
леченных необходимыми ресурсами (финансовыми, материальными, тех-
скими, временными, информационными, программно-математически-
адровыми и т. п.), реализуемых техническими и человеко-машинными
емами и направленных на достижение эффективности банковских опера-
.
анковская операция — составная часть банковской технологии; регулярд
действия, выполняемые банком согласно его статусу для извлечения при-
ı.

ГОСТ Р 8.561–95 Государственная система обеспечения единства измерений. Метрологи-
е обеспечение банковских технологий. Общие положения, принятые и введенные в дейст-
остановлением Госстандарта России от 29 августа 1995 г. № 451.

Банковские сделки — операции банка, осуществляемые в соответствии с лицензией Банка России, а также другие действия банка, выполняемые им в рамках законодательства для извлечения прибыли, для проведения которых лицензия не требуется.

1.3. Система угроз безопасности банка

Изучение содержания и видов преступных посягательств на безопасность банка является составной частью разработки мер защитного характера. Наличие четких представлений о характере и видах указанных посягательств позволяет выстроить адекватную систему мер их выявления, предупреждения и расследования.

Системное описание угроз преступных посягательств (далее — угроз), которым подвергается банк, призвано выявлять индивидуальные особенности каждой угрозы и давать полное описание возможных связей и отношений между угрозой и элементами структуры банка, подлежащими защите.

Основным результатом разработки системной характеристики банковских угроз является построение обобщенной модели, отображающей присущие угрозам специфические обстоятельства и взаимосвязи, которые могут проявиться в реальной ситуации[1].

Определение основных видов банковских угроз непосредственно связано с представлением о банке как объекте потенциальной опасности. По этой причине описание угроз следует начинать применительно к их связи с элементами структуры банка, в отношении которых возникает угроза. Вполне очевидно, что основная опасность для банка заключается в угрозе потери (либо неполучения) имущества. *Угрозу потери имущества* следует рассматривать в качестве основной, которая в своей крайней форме может привести к прекращению существования банка. Однако описание реальной ситуации будет неполным без указания на механизм, посредством которого эта угроза реализуется. Изучение показывает, что в подавляющем большинстве случаев потеря имущества происходит в процессе осуществления банком своей уставной деятельности и непосредственно связана с нарушениями порядка функционирования банка. Такие нарушения следует рассматривать как *угрозы порядку функционирования* банка, которые являются промежуточными между потенциальной угрозой потери имущества и реализацией этой угрозы. С позиций описания причинной связи между «основной опасностью» и угрозой ее реализации они выступают в качестве «сопутствующих» либо «дополняющих» угроз.

Перечисленные выше элементы системной характеристики банковских угроз являются исходными и могут включать в себя по мере их «развертывания»

[1] *Гамза В. А.* Методологические основы системной классификации банковских рисков // Банковское дело. 2001. № 6, 7.

ически все виды связей и отношений между потенциальными угрозами льными ситуациями, с которыми встречается банк.

ассификация угроз по отношению к объекту посягательств (банку и со-ющим его структурным элементам) позволяет выделить следующие су-зенные с точки зрения криминалистики разновидности угроз (в наиболее виде): *угрозы имуществу* и *угрозы инфраструктуре* (названные блоки туры банка и составляющие элементы их подробно описаны в предыду-араграфе). Особенности блоков и составляющих их элементов форми-специфические черты у других элементов характеристики безопасности (таких как «способ реализации угроз», «лица, причастные к реализации », «последствия реализации угроз» и проч.). Вполне очевидны, напри-азличия между механизмом реализации угроз, подвергающих опасности кные средства банка, и механизмом реализации угроз в отношении дело-епутации либо порядка управления деятельностью банка. Специфиче-особенности механизма реализации угроз закономерно связаны с осо-стями личностных и социальных характеристик субъектов, причастных лизации угроз. Так, лица, причастные к угрозам в отношении порядка льности банка, порядка совершения банковских операций, как правило, ются сотрудниками банка (закономерная связь между спецификой объек-сягательства и особенностями лица, причастного к реализации угрозы). ъекты, причастные к реализации, например, угроз в сфере ссудной (кре-ой) деятельности банка, в большинстве случаев в штате банка не состоят, о нередко обладают преступным опытом. Специфические особенности турных элементов банковских угроз оказывают существенное влияние рактер мер, призванных обеспечивать защиту интересов банка. Иными ми, свойства структурных элементов банка являются определяющими ля способа реализации угроз, так и для разработки мер защиты банка.

ассификация угроз по отношению к видам деятельности банка. Представ-е об «угрозах деятельности банка» относится преимущественно к органи-деятельности банка в целом, включая отдельные ее направления. С точ-ения организации защиты банка от угроз в виде преступных посяга-тв имеет значение разграничение его деятельности на «операционную», чающую совершение банковских операций, и «внеоперационную» — язанную непосредственно с банковскими операциями.

епосредственным предметом преступных посягательств *на операционную ельность* является установленный специальными нормативными актами док совершения банковских операций и входящих в них направлений льности банка. Практика правоохранительной деятельности свидетельст-о том, что угрозам преступных посягательств в сфере операционной дея-ности банка в большей или меньшей степени подвергается порядок осу-вления практически всех выполняющихся банком операций.

ледует отметить, что конечной целью нарушений порядка совершения операций в подавляющем большинстве случаев является преступное

завладение денежными средствами, которые используются в этих банковских операциях. От того, в каком виде банковской деятельности используются денежные средства (и в каких элементах структуры банковских активов они обособлены), зависят характер (способы совершения) и распространенность преступных посягательств на них.

Дальнейшая систематизация угроз операционной деятельности банка по степени распространения позволяет выявить группы посягательств на безопасность банка, объединенные в специфические подвиды, например: «угрозы в сфере кредитной деятельности банка», «угрозы в сфере расчетно-кассового обслуживания».

К числу подвидов операционной деятельности банка следует отнести не только сами банковские операции, но и деятельность по их непосредственному обеспечению (информационному, правовому, техническому, технологическому и т. д.). Угрозы, которым подвергается процесс обеспечения банковских операций, признаются отечественной и зарубежной наукой о банковском деле в качестве самостоятельных видов угроз и имеют собственные наименования. В их числе: «угроза преступных посягательств в сфере правового обеспечения конкретных сделок»[1], «угроза преступных посягательств в сфере информационного обеспечения сделок», «угроза преступных посягательств в сфере технологического обеспечения банковских операций» и т. д. Каждый из них имеет свою внутреннюю структуру, которая по мере необходимости может быть детализирована.

С точки зрения криминалистики указанные подвиды операционной деятельности нередко становятся предметом преступных посягательств, имеющих целью прямое либо опосредованное завладение собственностью банка.

Непосредственным предметом преступных посягательств *на внеоперационную деятельность* банка может служить порядок деятельности банка, выполняемой вне банковских операций, а также имущество и приравненные к нему объекты гражданского права, которые используются в этой деятельности. Преступные посягательства в указанных случаях могут быть направлены против собственности банка (носить характер разбойных нападений, краж или уничтожения имущества банка, вымогательства) либо посягать на инфраструктуру банка: на порядок деятельности банка, его информационное и кадровое обеспечение, нематериальные блага, деловую репутацию и деловые

[1] Изучение судебной и следственной практики свидетельствует о широком распространении умышленных нарушений мошенниками порядка правового оформления некоторых видов банковских операций (в частности, при приобретении банком векселей, оформлении залога, выдаче гарантии). При этом обман потерпевших совершается под видом «ошибок», влекущих недействительность сделки либо существенно уменьшающих размеры обязательств векселедателя. Такой прием позволяет преступникам отказываться от исполнения обязательств и маскировать мошеннические действия путем придания им видимости гражданско-правового деликта. Подробнее об этом: *Гамза В. А., Ткачук И. Б.* Безопасность коммерческого банка: учеб.-практ. пособие. М.: Изд-ль Шумилова И. И, 2000. С. 33.

і банка с партнерами. *Действия*, связанные с реализацией внеоперацион-
угроз, в большинстве случаев совершаются посторонними по отношению
ку лицами. Однако участие сотрудников банка в подобного рода посяга-
твах на интересы банка полностью не исключается. Лица из числа персо-
банка могут действовать в указанных случаях как самостоятельно, так
участии с посторонними.

о мере детализации угроз до уровня правового описания появляются но-
специфические основания для их классификации. При этом в зависимо-
т объекта посягательства и регулирующей отрасли права они приобрета-
чество преступлений, административных правонарушений и служебных
гупков, посягающих на имущество и инфраструктуру (порядок функцио-
вания) банка.

соответствии с отраслями права, охраняющими объект посягательства,
могут быть представлены как:

преступления, предусмотренные Уголовным кодексом РФ, посягаю-

- на *имущество* банка (преступления против собственности): кража (ст. 158), мошенничество (ст. 159), присвоение или растрата (ст. 160), грабеж (ст. 161), разбой (ст. 162), вымогательство (ст. 163), хищение предметов, имеющих особую ценность, (ст. 164), причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165), причинение имущественного ущерба путем умышленного уничтожения или повреждения (ст. 167), причинение имущественного ущерба путем уничтожения или повреждения по неосторожности (ст. 168);
- на *инфраструктуру* (порядок функционирования) банка: клевета и оскорбление (ст. 129 или 130), незаконное получение кредита (ст. 176), злостное уклонение от погашения кредиторской задолженности (ст. 177), незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183), неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273), нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274), изготовление или сбыт поддельных денег или ценных бумаг (ст. 186), злоупотребление полномочиями (ст. 201), коммерческий подкуп (ст. 204);

) правонарушения, предусмотренные КоАП РФ, в том числе посягаю-
:

- на *имущество* банка: уничтожение или повреждение чужого имущества, если эти действия не повлекли значительного ущерба (ст. 7.17), мелкое хищение (ст. 7.27);
- на *инфраструктуру* (порядок функционирования) банка: нарушение правил защиты информации (ст. 13.12), разглашение информации с ограниченным доступом (ст. 13.14), нарушение порядка представления статистической информации (ст. 13.19), незаконное получение кредита (ст. 14.11), воспрепятствование должностными лицами кредитной организации осуществлению функций временной администрации (ст. 14.14), ненадлежащее управление юридическим лицом (ст. 14.21), совершение сделок и иных действий, выходящих за пределы установленных полномочий (ст. 14.22), осуществление дисквалифицированным лицом деятельности по управлению юридическим лицом (ст. 14.23), нарушение порядка работы с денежной наличностью и порядка ведения кассовых операций (ст. 15.1), невыполнение обязанностей по контролю за соблюдением правил ведения кассовых операций (ст. 15.2), нарушение порядка открытия счета налогоплательщику (ст. 15.7), нарушение срока исполнения поручения о перечислении налога или сбора (взноса) (ст. 15.8), неисполнение банком решения о приостановлении операций по счетам налогоплательщика, плательщика сбора или налогового агента (ст. 15.9), неисполнение банком поручения государственного внебюджетного фонда (ст. 15.10), грубое нарушение правил ведения бухгалтерского учета и представления бухгалтерской отчетности (ст. 15.11), недобросовестная эмиссия ценных бумаг (ст. 15.17), использование служебной информации на рынке ценных бумаг (ст. 15.21), нарушение законодательства о банках и банковской деятельности (ст. 15.26);

в) дисциплинарные проступки, предусмотренные Трудовым кодексом РФ, в том числе посягающие:

- на *имущество* банка: совершение по месту работы хищения (включая мелкое) чужого имущества, растраты, умышленного его уничтожения или повреждения, установленных вступившим в законную силу приговором суда или постановлением органа, уполномоченного на применение административных взысканий (подп. «г» п. 6 ст. 81);
- на *инфраструктуру* (порядок функционирования) банка: прогул (отсутствие на рабочем месте без уважительных причин более 4 ч подряд в течение рабочего дня) (подп. «а» п. 6 ст. 81), появление на работе в состоянии алкогольного, наркотического или иного токсического опьянения (подп. «б» п. 6 ст. 81), разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей (подп. «в» п. 6 ст. 81), совершение виновных действий работником, непосредственно обслуживающим денежные или товарные ценности, если эти действия дают основание для утраты доверия к нему со стороны работодателя (п. 7 ст. 81), принятие необоснованного решения руководителем организации (филиала, представительства), его заместителями и главным бухгалтером, повлекшего нарушение сохранности имущества, неправомерное его использование

или иной ущерб имуществу организации (п. 9 ст. 81), однократное грубое нарушение руководителем организации (филиала, представительства), его заместителями своих трудовых обязанностей (п. 10 ст. 81), предоставление работником работодателю подложных документов или заведомо ложных сведений при заключении трудового договора (п. 11 ст. 81).

целях разработки и реализации мер правовой, организационной и экоческой защиты банка названные противоправные посягательства подются дальнейшему структурированию в рамках криминалистических харистик видов преступлений.

лассификация угроз по лицам, причастным к их реализации. На практике уг- анковской деятельности реализуется с участием конкретных лиц, имею- го или иное отношение к банковской деятельности. Указание на наличие і связи и описание ее особенностей служит важным элементом классиции угроз, имеющим существенное теоретическое и практическое значе- Использование сведений о свойствах личности субъектов, причастных лизации банковских угроз, представляется наиболее перспективным наением повышения эффективности выявления, предотвращения пре- ых посягательств на интересы банка, а также локализации их вредных едствий.

точки зрения системного подхода категория «лица, причастные к реали- л угроз» является самостоятельным элементом характеристики банков- угроз. Об этом свидетельствуют присущие данной категории лиц инди- альные особенности, а также специфические связи и отношения с други- лементами названной характеристики.

сходя из общих положений уголовного права и криминалистики «лицо, астное к реализации угроз» является одним из ведущих элементов опи- я события преступного посягательства. Его содержание оказывает ре- ее влияние на правовую оценку события и характер мер по предупре- ию потенциального или возмещению причиненного ущерба. Таким зом, сведения об элементе характеристики банковских угроз, условно на- ном «субъект угрозы», имеют существенное научное и практическое зна- е.

самом общем виде информация о личности должна включать в себя све- я об отношении лица к банку (сотрудник или посторонний — «производ- нный признак»). Дальнейшее структурирование сведений об участниках овских операций по «производственному признаку» выявляет практиче- целесообразность разграничения на тех, кто входит в персонал банка, тех, кто не входит в число сотрудников банка, однако участвует в его опе- ях, связан с ним договорными отношениями (клиенты, контрагенты, еспонденты), а также на тех, кто не имеет к банку никакого отношения горонние).

В свою очередь, исследование элемента «персонал банка» свидетельствует о практической значимости выделения в самостоятельные элементы структуры таких категорий персонала, как руководство банка (лица, принимающие управленческие решения); лица, участвующие в выполнении банковских операций (средний персонал); лица, участвующие в технологическом обеспечении банковских операций: деятельности технических и программных средств обработки и передачи информации (технический персонал).

Из числа «субъектов угроз», не входящих в число сотрудников банка и не связанных с банком какими-либо отношениями, целесообразно выделить три основные категории. Это юридические лица (недобросовестные конкуренты; организации, собирающие конфиденциальную информацию и совершающие другие действия, противоречащие интересам банка); физические лица (криминальные элементы) и неформальные группы (организованные преступные группы).

Классификация преступных посягательств по отношению субъекта к собственным действиям, создающим угрозу интересам банка. Практические потребности в защите порождают необходимость изучения особенностей отношения субъектов к собственным действиям, создающим угрозу банку. Описание отношения субъекта к собственным действиям, создающим угрозу деятельности банка, присутствует в науке о банковском деле, а также в методических и нормативных документах, посвященных банковской деятельности. Например, применяемый в методических и нормативных документах термин «ошибка» свидетельствует об отсутствии преступного умысла, а термин «мошенничество» — наоборот, об умышленном характере действий[1]. Однако в качестве самостоятельного элемента описания банковских угроз (рисков) субъективное отношение причастных к ним лиц в науке о банковском деле не исследуется.

В то же время указанный элемент является весьма важным для решения задач уголовного судопроизводства и обеспечения потребностей криминалистики. Изучение свидетельствует об уголовно-правовой и криминалистической значимости выявления таких видов субъективного отношения лица к собственным действиям, как преступный умысел, неосторожность (легкомыслие или небрежность), невиновность.

Определенный практический интерес представляют мотивы и цель, которыми руководствовался субъект при совершении указанных выше действий. В наиболее общем виде мотивы могут быть сведены в три группы:

а) субъект действовал исходя из собственных интересов или интересов третьих лиц, не считаясь с интересами банка;

б) субъект руководствовался враждебными по отношению к банку мотивами;

в) субъект действовал в интересах банка (в том числе ложно понятых).

[1] Приложение 2 к Положению об организации внутреннего контроля в банках от 28 августа 1997 г. № 509, утв. Приказом Банка России от 28 августа 1997 г. № 02-372.

ль, которой руководствовался субъект при совершении посягательств на ресы банка, с определенной долей точности находит свое отражение в по-ствиях реализованных угроз. Результатом посягательств на интересы бан-ще всего является причиненный ему имущественный ущерб. Результатом считать также и удовлетворение преступником каких-то своих потребно-желаний, страстей, стремлений. Информация об этом указывает на путь, ий к преступнику, очерчивает круг подозреваемых.

обобщенном виде цели преступных посягательств на интересы банка но свести в две основные группы.

ервая — завладение имуществом (правом на имущество) банка с целью ения его в свою собственность. Вторая — ограничение деятельности а-конкурента либо его устранение с рынка финансовых услуг. Обе назван-цели, как правило, достигаются поэтапно. Наиболее распространенной межуточной целью является снижение финансовых возможностей банка и разрушения клиентских связей, срыва переговоров и сделок, распростра-ия дезинформационных материалов порочащего характера, умышленного чения в заведомо убыточные проекты. В более жестком варианте для нения банка-конкурента с рынка финансовых услуг могут иметь место тожение его имущества, разрушение элементов инфраструктуры (в том е путем противоправных посягательств на кадровый состав — угрозы, вы-тельство, вербовка, внедрение, похищение; на оборудование, компьютер-сети, программы и т. п.).

лассификация преступных посягательств по степени тяжести последствий ляет выявить следующие виды ущерба, причиненного безопасности банка:

восполнимый ущерб — потери имущества и элементов инфраструктуры, которые банк может восполнить за счет собственных средств без угрозы своему существованию и без перевода банка на внештатный режим работы (финансовые потери, снижение доходности, обесценение активов или увеличение обязательств, недостижение установленных целевых ориентиров деятельности, ухудшение деловой репутации и разрушение деловых связей);

условно восполнимый ущерб — потери имущества и управления, создающие угрозу существованию банка, которые он не может устранить без привлечения внешних средств. Эти последствия выражаются в неспособности банка исполнить требования федеральных законов, регулирующих банковскую деятельность, а также нормативных актов Банка России или удовлетворить требования кредиторов по денежным обязательствам и (или) исполнить обязанность по уплате обязательных платежей. Внешними инструментами восполнения потерь в данных случаях могут служить заемные финансовые средства, привлеченный для восстановления управления новый персонал (вплоть до введения внешнего управления), приобретение новых технических средств обеспечения банковских операций и т. д. Размеры внешнего заимствования

не должны выходить за пределы, установленные законодательством и нормативными актами Банка России. В противном случае появляются основания для отзыва у заемщика лицензии на осуществление банковских операций. Для возмещения условно восполнимых потерь банк вынужден переходить на внештатный режим работы;

- невосполнимый (катастрофический) ущерб — потери имущества и инфраструктуры банка, возместить которые не представляется возможным, а его причинение влечет ликвидацию или реорганизацию банка.

Основные виды угроз безопасности банка. Обстоятельства, способы и субъекты их реализации

Угроза потери имущества — посягательство на собственные и привлеченные средства банка; имущественные права на объекты банковской деятельности, а также здания, оборудование и инвентарь.

Угроза порядку функционирования — посягательство на установленные законодательными и иными нормативными правовыми актами требования, условия и запреты, связанные с созданием банка, организацией и целями его деятельности.

Угроза операционной деятельности — посягательство на порядок совершения банковских операций и деятельности по их информационному, правовому, организационному, техническому и технологическому обеспечению.

Угроза внеоперационной деятельности — посягательство на порядок деятельности банка, выполняемой вне банковских операций, а также имущество и приравненные к нему объекты гражданского права, которые используются в этой деятельности.

Виды деятельности банка, в процессе которых реализуются угрозы:

а) *операционная деятельность* — процесс выполнения банком одной из следующих банковских операций (сделок):

- привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок);
- размещение привлеченных средств от своего имени и за свой счет;
- открытие и ведение банковских счетов физических и юридических лиц;
- осуществление расчетов по поручению физических и юридических лиц, в том числе банков-корреспондентов по их банковским счетам;
- инкассация денежных средств, векселей, платежных и расчетных документов и кассовое обслуживание физических и юридических лиц;
- купля-продажа иностранной валюты в наличной и безналичной формах;
- привлечение во вклады и размещение драгоценных металлов;
- выдача банковских гарантий;
- осуществление переводов денежных средств по поручению физических лиц без открытия банковских счетов (за исключением почтовых переводов);

- выдача поручительств за третьих лиц, предусматривающих исполнение обязательств в денежной форме;
- приобретение права требования от третьих лиц исполнения обязательств в денежной форме;
- доверительное управление денежными средствами и иным имуществом по договору с физическими и юридическими лицами;
- осуществление операций с драгоценными металлами и драгоценными камнями;
- предоставление в аренду физическим и юридическим лицам специальных помещений или находящихся в них сейфов для хранения документов и ценностей;
- лизинговые операции;
- оказание консультационных и информационных услуг;

) *неоперационная деятельность* — деятельность, не связанная непосредно с процессом выполнения банковских операций (посягательства совертся путем кражи, грабежа, разбоя, вымогательства, умышленного уничтожия или повреждения имущества, незаконного получения и разглашения ений, составляющих коммерческую, налоговую или банковскую тайну, оч.).

пособы реализации угроз безопасности банка:

посягательства, совершенные с применением насилия и угроз (противоправные деяния насильственного характера);

посягательства, совершенные тайно либо с применением обмана (противоправные деяния ненасильственного характера).

убъекты угроз:

) персонал банка:

- руководство (лица, принимающие управленческие решения);
- лица, участвующие в выполнении банковских операций (средний персонал);
- лица, участвующие в технологическом обеспечении банковских операций, в деятельности технических и программных средств обработки и передачи информации (технический персонал);

) лица, не входящие в число сотрудников банка, однако участвующие о операциях на основе договорных отношений (клиенты, контрагенты, еспонденты);

) лица, не имеющие с банком трудовых и иных договорных отношений сторонние):

- юридические лица (недобросовестные конкуренты, организации, собирающие конфиденциальную информацию и совершающие другие действия, противоречащие интересам банка);
- физические лица (криминальные элементы);
- неформальные группы (организованные преступные группы).

1.4. Банк как субъект борьбы с противоправными посягательствами

Ведущим субъектом борьбы с противоправными посягательствами на безопасность банка является государство. Выполняя указанную функцию через органы законодательной, исполнительной и судебной власти, государство устанавливает уголовную и иную ответственность за противоправные посягательства на интересы банка. На государственные органы власти возложена обязанность выявления, предупреждения и расследования правонарушений в указанной сфере, наказание виновных в их совершении и возмещение причиненного ущерба. В рамках мер по предупреждению противоправных посягательств государство осуществляет контроль и надзор за выполнением банком установленных законодательством требований безопасности.

Другим важным участником борьбы с преступлениями и правонарушениями в банковской сфере является сам банк, на который законодательно возложены обязанности разработки и реализации мер предупреждения противоправных посягательств на его собственность и инфраструктуру (обеспечение защиты мест хранения денег и других ценностей, кассовых операций, объектов информации и информатизации, банковских технологий, выявление недобросовестных партнеров, защита персонала и т. д.).

Следует отметить, что наряду с деятельностью по обеспечению собственной безопасности законодатель возложил на банк и его службы определенные обязанности в борьбе с преступлениями и правонарушениями, не посягающими непосредственно на его интересы. Речь идет об участии банка в противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также в реализации контроля за соблюдением валютного законодательства.

Банк как субъект противодействия преступлениям и правонарушениям, посягающим непосредственно на его интересы

Показательно, что реальная ситуация, сложившаяся в сфере обеспечения банковской безопасности, потребовала от банков, несмотря на отсутствие прямых законодательных предписаний, выйти за пределы мер предупреждения и принять более широкое участие в борьбе с противоправными посягательствами на интересы кредитных организаций. Это было вызвано недостаточной активностью правоохранительных органов в выявлении преступлений в банковской сфере и розыске преступников[1], а также необоснованными отказами от уголовного преследования по заявлениям банков в случаях, когда для маскировки банковских преступлений преступники использовали заключение

[1] *Гамза В. А.* Проблемы выявления, пресечения и раскрытия ненасильственных преступных посягательств на безопасность коммерческого банка // Российская юридическая доктрина в XXI веке: Проблемы и пути их решения: научно-практическая конференция / под ред. А. И. Демидова. Саратов: СГАП, 2001. С. 256–258.

ивных договоров. Такие отказы мотивировались наличием мнимых граж-
о-правовых отношений, якобы подлежащих разрешению в граждан-
процессуальном порядке.

нижению активности органов исполнительной власти в обеспечении
асности банков в определенной мере способствовал отказ законодателя
инципа публичности при осуществлении уголовного преследования за со-
ение отдельных видов преступлений в банковской сфере (примечание 2
201 УК РФ, ст. 23 Угловно-процессуального кодекса РФ (УПК РФ)). Пре-
вление банку права давать согласие на возбуждение уголовного дела (или
ывать в нем) было воспринято правоохранительными органами как воз-
ние основной ответственности за выявление указанных преступных по-
ельств на сам банк.

ким образом, банк (в лице службы безопасности и других структурных
азделений) стал фактическим участником не только предупредительной,
скной деятельности в сфере обеспечения собственной безопасности.

Правовой основой предупредительно-профилактической и сыскной дея-
ости службы безопасности банка, осуществляемой в интересах собствен-
безопасности, служит Закон РФ от 11 марта 1992 г. № 2487-1 «О частной
тивной и охранной деятельности в Российской Федерации» (в ред.
4 июля 2007 г. № 214-ФЗ) (далее — Закон о частной детективной деятель-
и), который разрешает (при наличии соответствующей лицензии) осуще-
ение сыска в целях предоставления услуг по изучению рынка, сбору инфор-
ии для деловых переговоров, выявлению некредитоспособных или ненадеж-
деловых партнеров (п. 2 ст. 3). Практика свидетельствует, что признаки
тупных посягательств выявляются в большинстве случаев именно в про-
е целенаправленного изучения «некредитоспособных» и «ненадежных»
неров.

Детальное нормативное регулирование целей и задач деятельности службы
пасности, а также порядка и форм ее проведения осуществляется самим
ом путем принятия основанных на действующем законодательстве внут-
них нормативных документов (локальных нормативных актов): Устава
ложения) службы безопасности, Положения о внутреннем контроле, По-
ения о защите банковской тайны, Инструкции о внутреннем расследова-
и др.

Как правило, банк возлагает на службу безопасности следующие норма-
но закрепленные обязанности:

- выявлять признаки готовящихся и совершенных преступных посяга-
  тельств на интересы банка и принимать меры по их предупреждению
  и пресечению;
- готовить материалы к направлению в правоохранительные органы для
  решения вопроса о возбуждении уголовного дела в соответствии со
  ст. 141 УПК РФ;

- участвовать в расследовании по возбужденным уголовным делам на основании п. 7 ст. 3 Закона о частной детективной деятельности;
- участвовать в уголовном преследовании обвиняемого в соответствии со ст. 22 УПК РФ;
- собирать и представлять следственным органам в соответствии со ст. 86 УПК РФ письменные документы (в том числе — согласно ст. 84 УПК РФ — материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации) и предметы для приобщения их к уголовному делу в качестве доказательств;
- осуществлять розыск лиц, совершивших посягательства на интересы банка или подозреваемых в их совершении, а также принимать в пределах своей компетенции меры по возмещению нанесенного банку ущерба.

В этих целях службе безопасности вменяется в обязанность:

- вести сыскную деятельность на основании Закона о частной детективной деятельности;
- участвовать в плановых и внеплановых внутренних проверках деятельности подразделений банка, проводящихся методами административного и финансового контроля;
- проводить внутреннее (служебное) расследование по фактам причинения ущерба собственности и порядку функционирования банка;
- организовывать и осуществлять в указанных выше целях взаимодействие с правоохранительными органами, оказывать им содействие в проведении предусмотренных законом мероприятий следственного, розыскного и организационного характера;
- разрабатывать и осуществлять меры по предупреждению преступных посягательств на интересы банка;
- использовать средства и методы криминалистики.

Банк как субъект противодействия преступлениям и правонарушениям, связанным с легализацией (отмыванием) доходов, полученных преступным путем

Лишение преступника возможности владеть, пользоваться, распоряжаться денежными средствами или иным имуществом, полученным в результате совершения преступлений, является одним из наиболее эффективных методов борьбы с опасными формами организованной преступности.

Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [1] (в ред. от 28 ноября 2007 г. № 275-ФЗ) (далее — Закон о противодействии легализации преступных доходов) предоставил государству

[1] Собрание законодательства РФ. 2001. № 33 (ч. 1). Ст. 3418.

ювые и организационные возможности для предупреждения операций
ежными средствами или иным имуществом, добытым в результате пре-
ной деятельности, а также для идентификации и розыска материальных
ностей, подлежащих изъятию. Одновременно Закон расширил число орга-
ий, обязанных участвовать в реализации мер противодействия «отмыва-
» преступных доходов.

Субъектами указанной деятельности стали *уполномоченный орган* — Феде-
ная служба по финансовому мониторингу (далее — ФСФМ России), об-
ванная Указом Президента РФ от 1 ноября 2001 г. № 1263 «Об уполно-
енном органе по противодействию легализации (отмыванию) доходов,
ченных преступным путем, и финансированию терроризма», а также *ор-
зации, осуществляющие операции с денежными средствами и иным имуще-
м*, в первую очередь кредитные организации (банки)[1].

ФСФМ России является федеральным органом исполнительной власти,
овные задачи которой: сбор, обработка и анализ информации об операци-
сделках) с денежными средствами или иным имуществом, подлежащим
ролю в соответствии с законодательством о противодействии «отмыва-
» преступных доходов; создание единой информационной системы и ве-
ие федеральной базы данных в сфере противодействия «отмыванию» пре-
ных доходов; направление информации о признаках выявленных престу-
ий в правоохранительные органы.

На банк Закон возложил обязанность сбора и передачи ФСФМ России
ичной информации о сделках, вызывающих подозрение в их использова-
в целях «отмывания» преступных доходов.

В рамках участия в противодействии «отмыванию» преступных доходов
к обязан осуществить следующие меры:

- самостоятельно организовать систему внутреннего контроля с учетом Закона и рекомендаций Банка России;
- отслеживать попытки «отмывания» преступных доходов в процессе банковских операций;
- идентифицировать лиц, совершающих подозрительные операции с денежными средствами или иным имуществом;
- документально фиксировать и представлять в уполномоченный орган в порядке, установленном Банком России[2], сведения об операциях, вызывающих подозрение в «отмывании» преступных доходов, и о причастных к ним лицах;

Далее в соответствии с целями настоящего издания противодействие «отмыванию» пре-
ных доходов рассматривается только с позиций коммерческого банка. Участие в ней других
ударственных организаций не исследуется.

Положение Центрального Банка РФ от 20 декабря 2002 г. № 207-П «О порядке представле-
кредитными организациями в уполномоченный орган сведений, предусмотренных Федераль-
законом "О противодействии легализации (отмыванию) доходов, полученных преступным
м, и финансированию терроризма"».

- обеспечивать конфиденциальность функционирования системы внутреннего контроля, а также защиту собранной информации от несанкционированного доступа посторонних в процессе ее хранения и передачи в уполномоченный орган.

Собранные банком материалы предназначены для возможной реализации в уголовно-судебной сфере. Они могут служить основанием для возбуждения уголовного дела, представляться в орган дознания, следователю или в суд, в производстве которого находится уголовное дело, а также использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства Российской Федерации.

Невыполнение банком требований законодательства в области противодействия «отмыванию» преступных доходов может повлечь отзыв (аннулирование) лицензии на совершение банковских операций. Лица из числа персонала банка, виновные в нарушении Закона, несут административную, гражданскую и уголовную ответственность в соответствия с законодательством Российской Федерации.

Банк, как субъект противодействия преступлениям и правонарушениям в области валютного регулирования

В соответствии с Федеральным законом от 10 декабря 2003 г. № 173-ФЗ «О валютном регулировании и валютном контроле» (в ред. от 30 октября 2007 г. № 242-ФЗ) (далее — Закон о валютном регулировании) валютное регулирование и валютный контроль осуществляются в интересах экономической безопасности России путем обеспечения устойчивости отечественной валюты и стабильности внутреннего валютного рынка Российской Федерации.

Субъектами валютного регулирования в соответствии с Законом о валютном регулировании являются *органы валютного регулирования* — Центральный банк РФ и Правительство РФ. Для реализации функций, предусмотренных Законом, они издают в пределах своей компетенции акты органов валютного регулирования, обязательные для резидентов и нерезидентов. Ограничивают круг субъектов валютных операций, устанавливают ограничения на перемещение валюты через государственную границу, принимают меры к возврату в Россию валютной выручки и продаже обязательной части выручки государству, а также к возмещению возможного ущерба в случае невозврата валютной выручки.

Названные субъекты являются одновременно и органами валютного контроля в Российской Федерации. Кроме них, в реализации контрольных функций участвуют *агенты валютного контроля*.

В качестве агентов валютного контроля выступают уполномоченные банки — кредитные организации, имеющие право на основании лицензий осуществлять банковские операции со средствами в иностранной валюте, а также действующие на территории Российской Федерации в соответствии с лицензиями

рального банка РФ филиалы кредитных организаций, созданных в соот-
вии с законодательством иностранных государств, имеющие право осу-
влять банковские операции со средствами в иностранной валюте, а также
енные органы.

Iерами предупреждения незаконных валютных операций со стороны
омоченного банка являются контроль за соответствием совершаемых
ж действующему законодательству, отказ банка от совершения операции
ткрытия счета, направление информации о выявленных правонаруше-
органам валютного регулирования.

онтрольные функции банка осуществляются путем сбора сведений о со-
аемых валютных операциях и проверки их соответствия валютному зако-
ельству. В этих целях Закон возложил на банк обязанность запрашивать
лучать от резидентов и нерезидентов следующие документы (копии доку-
ов), связанные с проведением валютных операций, открытием и ведени-
етов:

) документы, удостоверяющие личность физического лица;

) документ о государственной регистрации физического лица в качестве
ивидуального предпринимателя;

) документы, удостоверяющие статус юридического лица, — для нерези-
в; документ о государственной регистрации юридического лица — для
дентов;

) свидетельство о постановке на учет в налоговом органе;

) документы, удостоверяющие права лиц на недвижимое имущество;

) документы, удостоверяющие права нерезидентов на осуществление ва-
ых операций, открытие счетов (вкладов), оформляемые и выдаваемые
ами страны места жительства (места регистрации) нерезидента, если по-
ие нерезидентом такого документа предусмотрено законодательством
странного государства;

уведомление налогового органа по месту учета резидента об открытии
(вклада) в банке за пределами территории Российской Федерации;

регистрационные документы в случаях, когда предварительная регист-
я предусмотрена в соответствии с настоящим Федеральным законом;

документы (проекты документов), являющиеся основанием для прове-
я валютных операций, включая договоры (соглашения, контракты), дове-
сти, выписки из протокола общего собрания или иного органа управле-
юридического лица; документы, содержащие сведения о результатах тор-
в случае их проведения);

0) документы, подтверждающие факт передачи товаров (выполнения ра-
оказания услуг), информации и результатов интеллектуальной деятельно-
в том числе исключительных прав на них, акты государственных органов;

1) документы, оформляемые и выдаваемые кредитными организациями,
чая банковские выписки; документы, подтверждающие совершение ва-
ых операций;

12) таможенные декларации — документы, подтверждающие ввоз в Российскую Федерацию валюты Российской Федерации, иностранной валюты и внешних и внутренних ценных бумаг в документарной форме;

13) паспорт сделки.

В качестве агента валютного контроля уполномоченный банк проводит проверку полноты и достоверности учета по валютным операциям резидентов и нерезидентов, проверяет соблюдение резидентами и нерезидентами актов валютного законодательства Российской Федерации и актов органов валютного регулирования.

В необходимых случаях указанную деятельность он осуществляет во взаимодействии с таможенными органами, передавая им для выполнения функций агентов валютного контроля информацию в объеме и порядке, установленном Центральным банком РФ.

Собранная банком информация о валютных операциях, проведенных с его участием, должна быть представлена органам валютного контроля.

Органы и агенты валютного контроля и их должностные лица обязаны сохранять в соответствии с законодательством Российской Федерации коммерческую, банковскую и служебную тайну, ставшую им известной при осуществлении их полномочий.

При наличии сведений о нарушении актов валютного законодательства Российской Федерации и актов органов валютного регулирования банк обязан передать органу валютного контроля, имеющему право применять санкции к данному лицу, информацию, позволяющую идентифицировать субъекта нарушения; раскрыть содержание нарушения с указанием нарушенного нормативного правового акта, дату совершения и сумму незаконной валютной операции или нарушения.

Материалы о нарушениях валютного законодательства могут быть реализованы в уголовно-судебной сфере. Они могут служить основанием для возбуждения уголовного дела, а также использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства Российской Федерации.

За неисполнение функций агента валютного контроля в отношении банка могут быть применены санкции вплоть до отзыва (аннулирования) лицензии на совершение банковских операций. Лица из числа персонала банка, виновные в нарушении Закона о валютном регулировании, несут административную, гражданскую и уголовную ответственность в соответствия с законодательством Российской Федерации.

Основные формы и методы участия банка в обеспечении собственной безопасности:

- выполнение требований безопасности, связанных с созданием и функционированием банка;
- выполнение мер предупреждения и выявления противоправных посягательств на интересы банка, осуществляемых в рамках нормативно-правовой, организационной, сыскной и криминалистической деятельности;

участие в преследовании лиц, посягающих на интересы банка, и возмещении причиненного ими ущерба.

Основные формы и методы участия банка в противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма:

выполнение функций организации, осуществляющей операции с денежными средствами или иным имуществом;

создание и организация деятельности системы внутреннего контроля банка;

осуществление деятельности по выявлению операций, подлежащих обязательному контролю, и иных операций, связанных с денежными средствами или иным имуществом, связанных с легализацией (отмыванием) доходов, полученных преступным путем и финансированием терроризма;

направление сведений, выявленных системой внутреннего контроля, в уполномоченный орган;

выполнение запросов уполномоченного органа о получении дополнительной информации относительно сведений, выявленных системой внутреннего контроля.

Основные формы и методы участия банка в противодействии правонарушениям в области валютного регулирования:

выполнение функций агента валютного контроля организации, осуществляющей операции с денежными средствами или иным имуществом;

осуществление контроля за соответствием совершающихся в банке валютных операций валютному законодательству;

передача органу валютного контроля информации о выявленных фактах нарушения валютного законодательства (операциях и причастных к ним лицам);

отказ от совершения операции или открытия счета в целях предупреждения нарушения валютного законодательства.

ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. В чем заключаются безопасность банка и деятельность по ее обеспечению?
2. Раскройте содержание понятия «опасность».
3. Каковы различия между такими мерами опасности, как «риск» и «угроза»?
4. Что собой представляют требования безопасности банка, какие группы норм их составляют?
5. Назовите основные элементы структуры банка, которые служат обьектом преступных посягательств.
6. Каковы основные виды угроз безопасности банка?
7. Каким трем основным направлениям преступной деятельности банк обязан противодействовать в соответствии с требованиями законодательства?
8. Назовите основные формы и методы участия банка в обеспечении собственной безопасности, в противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, в противодействии правонарушениям в области валютного регулирования.

Глава 2

ПРАВОВЫЕ ОСНОВЫ БЕЗОПАСНОСТИ БАНКА

Система правового обеспечения безопасности банка
Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания
Банковское законодательство
Нормативные акты Банка России
Внутренние нормативные акты банков

2.1. Система правового обеспечения безопасности банка

Общая характеристика законодательства о банковской безопасности

: точки зрения права осуществление защиты банка представляет собой есс реализации законодательства о банковской безопасности. Речь идет ализации правовых норм, регламентирующих полномочия, обязанности, тственность органов государственной власти, представительных и испол-ельных органов банка, связанных с процессами его создания и безопасно-ункционирования.

аконодательство о банковской безопасности состоит из совокупности овых актов различной юридической силы, регулирующих отношения ере охраны и защиты банковского дела. По степени юридической силы и них выделяются федеральные конституционные и федеральные законы, Президента РФ и Правительства РФ, нормативные правовые акты субъ-в Федерации, а также ведомственные нормативные акты.

По направленности правового воздействия в число этих актов входят нор-ивные правовые акты общего действия, регулирующие отношения в сфере спечения безопасности банков наряду с другими объектами защиты, а так-нормативные правовые акты специального действия, имеющие целью спечить безопасность исключительно в банковской сфере.

Правовые акты *общего действия*, регулирующие отношения в сфере обес-ения безопасности банков, наряду с другими объектами защиты содержат-отраслях законодательства[1], решающих вопросы:

- конституционного строя;
- государственной службы;
- гражданского права;
- труда и занятости населения;
- информации и информатизации;
- безопасности и охраны правопорядка;

[1] Здесь и далее перечень отраслей законодательства приводится в очередности, установлен-Классификатором правовых актов, одобренным Указом Президента РФ от 15 марта 2000 г. 11.

- уголовного права;
- уголовного процесса;
- административных правонарушений и административной ответственности.

Нормативные правовые акты *специального действия*, регламентирующие правоотношения в сфере обеспечения безопасности исключительно банковской деятельности, содержат законодательство о банковском деле и о банковской системе.

Значительный массив правовых актов специального действия, направленных на обеспечение безопасности акционерных коммерческих банков, содержится в ведомственных нормативных актах Банка России, обязательных для федеральных органов государственной власти, органов власти субъектов Федерации и местного самоуправления, всех юридических и физических лиц. Такие акты издаются в формах указания, положения или инструкции Банка России[1].

Законодательство о конституционном строе

Ведущим законодательным актом названной отрасли права является Конституция РФ, которая:

- определяет правовое положение Банка России в качестве федеральной экономической службы (п. «ж» ст. 71), наделенной функциями по разработке и регулированию единой государственной денежно-кредитной политики, контролю и надзору за кредитными организациями (банками) в целях поддержания стабильности банковской системы;
- устанавливает общие принципы владения, пользования и распоряжения объектами частной собственности, которыми являются коммерческие банки (ч. 2 ст. 8), признает законные права и интересы юридических лиц, к числу которых относятся акционерные коммерческие банки, и гарантирует их защиту органами государственной власти (ч. 1 ст. 35).

Законодательство о государственной службе в Российской Федерации

Федеральный закон от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» (в ред. от 29 марта 2008 г. № 30-ФЗ) (далее — Закон о государственной службе):

- обязывает государственных служащих в процессе профессиональной деятельности по обеспечению исполнения полномочий государственных органов строго соблюдать Конституцию РФ, федеральные конституционные законы, федеральные законы, иные нормативные правовые акты Российской Федерации, конституции (уставы), законы и иные

[1] Положение «О порядке подготовки и вступления в силу нормативных актов Банка России», объявленное приказом Банка России от 15 сентября 1997 г. № 02–395.

нормативные правовые акты субъектов Российской Федерации и обеспечивать принцип верховенства Конституции РФ над иными нормативными актами и должностными инструкциями (п. 1. ч. 1. ст. 15), соблюдать при исполнении должностных обязанностей права и законные интересы граждан и организаций (п. 4 ч. 1 ст. 15);

обеспечивает защиту законных интересов банка от неправомерных действий государственных служащих путем установления их ответственности за подготавливаемые и принимаемые решения, неисполнение либо ненадлежащее исполнение своих должностных обязанностей (п. 1. ч. 1 ст. 18);

устраняет условия, способствующие принятию неправомерных решений в пользу одних лиц вопреки интересам других, путем установления запрета государственным служащим участвовать на платной основе в деятельности органа управления коммерческой организацией, за исключением случаев, установленных федеральным законом (п. 1. ч. 1. ст. 17); осуществлять предпринимательскую деятельность (п. 1 ч. 1. ст. 17); быть поверенными или представителями по делам третьих лиц в государственном органе, в котором он замещает должность гражданской службы, если иное не предусмотрено настоящим Федеральным законом и другими федеральными законами (п. 5. ч. 1. ст. 17); получать в связи с исполнением должностных обязанностей вознаграждения от физических и юридических лиц (подарки, денежное вознаграждение, ссуды, услуги, оплату развлечений, отдыха, транспортных расходов и иные вознаграждения) (подп. 6 п. 1. ч. 1 ст. 17);

регламентирует основания и условия доступа государственных служащих к конфиденциальной информации хозяйствующих субъектов (в том числе банков);

содержит положения, направленные на обеспечение защиты охраняемой законом тайны (в том числе банковской);

устанавливает ответственность государственных служащих за нарушение порядка обращения с конфиденциальными сведениями, поступившими от указанных субъектов;

наделяет конфиденциальные сведения, полученные государственными органами (и их сотрудниками) от банков в связи с исполнением должностных обязанностей, статусом служебной тайны, порождающей правовые последствия как для государственных структур, так и для отдельных их сотрудников, допущенных к этой информации;

устанавливает обязанность государственных служащих хранить государственную и иную охраняемую законом (в том числе банковскую) тайну (подп. 7 п. 1 ч. 1. ст. 15);

признает разглашение государственным служащим сведений, составляющих государственную и иную охраняемую законом тайну (в том числе банковскую), основанием для расторжения служебного контракта по инициативе представителя нанимателя (подп. «в» п. 3. ч. 1 ст. 37).

Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» (далее — постановление Правительства РФ № 1233):

- устанавливает порядок обращения государственных органов и их сотрудников со сведениями конфиденциального характера, полученными от организаций любой формы собственности (банков в том числе);
- служит типовой основой для разработки соответствующих ведомственных инструкций.

Гражданское законодательство

Гражданский кодекс РФ:

- устанавливает систему условий, соблюдение которых обязательно для осуществления защиты банковской деятельности способами, предусмотренными Гражданским кодексом РФ и другими законами, перечисляет объекты гражданских прав банка, подлежащие защите, дает определение этих объектов[1];
- регламентирует основания возникновения гражданских прав (ст. 8) юридических лиц и способы их правовой защиты (ст. 12);
- устанавливает понятие юридического лица, каковым является банк (ст. 48);
- определяет момент возникновения правоспособности юридического лица (банка) и его права осуществлять банковские операции, на занятие которыми необходимо получение лицензии (ст. 49, п. 2 ст. 51);
- дает исчерпывающий перечень объектов гражданских прав, подлежащих защите, в числе которых наряду с вещами и имущественными правами находится информация и нематериальные блага (ст. 128). Устанавливает обязательные признаки, которыми должны обладать эти объекты (гл. 6–8);
- определяет виды и форму сделок (ст. 153–165);
- устанавливает порядок регулирования отдельных вопросов банковской деятельности, соблюдение которого является обязательным условием правовой охраны совершенных операций (сделок) и приобретенных банком объектов гражданских прав: банковская гарантия (ст. 368–379), заем и кредит, финансирование под уступку денежного требования, банковский вклад (ст. 834–844), банковский счет, расчеты (ст. 845–860);
- обязывает банк хранить банковскую тайну (ст. 857);
- устанавливает обязанность банка соблюдать вышеуказанные предписания, регламентирующие порядок установления и изменения граждан-

[1] Гражданский кодекс РФ занимает ведущее положение относительно других актов законодательства, содержащих нормы гражданского права (п. 2 ст. 3 ГК РФ). Поэтому специальные акты банковского законодательства (законы, указы Президента РФ, постановления Правительства РФ, ведомственные акты), содержащие эти нормы, принимаются в строгом соответствии с Гражданским кодексом РФ.

ско-правовых отношений в качестве обязательного условия защиты принадлежащих ему объектов гражданского права средствами гражданского, уголовного и иных видов законодательства.

Законодательство о труде и занятости населения

удовой кодекс РФ:

регулирует трудовые и иные непосредственно с ними связанные отношения (в том числе в сфере обеспечения безопасности банка);

регламентирует вопросы обеспечения безопасности банков, возникающие в процессе установления, реализации и прекращения трудовых отношений между работниками банка и работодателем;

служит законодательной основой для иных федеральных законов, законодательных и нормативных актов, в том числе локальных нормативных актов банка, содержащих нормы трудового права (ст. 5);

регламентирует защиту кадрового состава банка от проникновения лиц, не соответствующих требованиям безопасности, на стадии отбора кандидатов на работу путем отказа от заключения с ними трудового договора;

предусматривает принятие специальных стандартов поведения, направленных на защиту интересов банка, и дополнительных обязательств по их соблюдению;

устанавливает основания и порядок прекращения трудовых отношений с лицами, которые причинили (могут причинить) вред интересам банка, путем расторжения трудового договора (увольнение).

Нормы Трудового кодекса РФ, иных федеральных законов, нормативных правых актов, устанавливающих основание для отказа от заключения трудового вора с лицом, не отвечающим требованиям безопасности:

предоставление работником работодателю подложных документов или заведомо ложных сведений при заключении трудового договора (п. 11 ст. 81 ТК РФ)[1];

отсутствие согласия на заключение трудового договора с кандидатом на должность руководителя и (или) главного бухгалтера банка со стороны органа, не являющегося работодателем по этому договору (в данном случае — Банка России — ст. 67 ТК РФ, ст. 16 Закона о банковской деятельности), в отношении лица:

а) которое имеет судимость за совершение преступления против собственности, хозяйственного и должностного преступления;

б) совершившего в течение года административное правонарушение в области торговли и финансов, установленное вступившим в законную силу постановлением органа, уполномоченного рассматривать дела об административных правонарушениях;

[1] Трудовой кодекс РФ не содержит прямого запрета на заключение трудового договора с ли-, представившими подложные документы или заведомо ложные сведения, однако в соответи с п. 11 ст. 81, будучи заключенным, он подлежит прекращению.

в) с которым в течение последних двух лет по инициативе администрации расторгнут трудовой договор по основаниям, предусмотренным п. 7 ст. 81 ТК РФ (совершение виновных действий работником, непосредственно обслуживающим денежные или товарные ценности, если эти действия дают основание для утраты доверия к нему со стороны работодателя);

г) которое лишено права занимать определенные должности или заниматься определенной профессиональной деятельностью в банковской сфере в связи с назначением наказания, предусмотренного ст. 47 УК РФ;

д) которое лишено права занимать руководящую должность в исполнительном органе или в совете директоров (наблюдательном совете) банка в связи с дисквалификацией, предусмотренной ст. 3.11 КоАП РФ;

е) которое не соответствует квалификационным требованиям кандидата на должность руководителя банка, его исполнительных органов и (или) главного бухгалтера (п. 6.17. Инструкции Банка России от 23 июля 1998 г. № 75-И «О порядке применения федеральных законов, регламентирующих процедуру регистрации кредитных организаций и лицензирования банковской деятельности» (с изм. от 31 июля 1998 г, 28 июня, 5 и 8 июля 1999 г., 19 июня и 7 августа 2001 г.), объявленной указанием Банка России от 24 ноября 1998 г. № 421-У.

Нормативные акты Банка России, предписывающие создание системы защиты персонала банка от лиц, не отвечающих требованиям безопасности.

Положение Банка России № 242-П устанавливает обязанность банка:

а) разработать систему контроля за подбором и расстановкой кадров с целью защиты финансового состояния банка, ограждения персонала от лиц с сомнительной деловой и общественной репутацией;

б) иметь четкие критерии квалификационных (образование, стаж) и личностных характеристик сотрудника применительно к содержанию работы и объему ответственности (п. 4.9 Положения)[1].

Нормы Трудового кодекса РФ, иные законодательные и нормативные требования, предписывающие принятие работником стандартов поведения, направленных на защиту интересов банка, и обязательств по их соблюдению.

1. Трудовой кодекс РФ:
   - предписывает работникам соблюдать дисциплину труда — обязательное для всех работников подчинение правилам поведения, определенным в соответствии с Кодексом, иными законами, трудовым договором, локальными нормативными актами организации (ст. 189).

[1] Требования к соблюдению поверочных стандартов при приеме служащих на работу, а также контроля за подбором и расстановкой кадров, критерии квалификационных и личностных характеристик служащих детализированы в Письме Банка России от 30 июня 2005 г. № 92-Т «Об организации управления правовым риском и риском потери деловой репутации в кредитных организациях и банковских группах».

Грубые нарушения дисциплины труда, связанные с невыполнением установленных в банке правил безопасного поведения, правил защиты объектов гражданских прав банка и порядка его функционирования, могут создавать условия для совершения преступных посягательств на интересы банка, представлять непосредственную подготовку к совершению таких посягательств либо свидетельствовать об определенной деформации нравственно-психологических качеств личности работника и о вероятности совершения им более тяжких правонарушений в будущем;

- обязывает работника банка предоставить работодателю свои персональные данные в объеме, предусмотренном Кодексом и иными федеральными законами (п. 1 и 2 ст. 86);
- незамедлительно сообщить работодателю либо непосредственному руководителю о возникновении ситуации, представляющей угрозу жизни и здоровью людей, сохранности имущества работодателя (ст. 21);
- соблюдать правила внутреннего трудового распорядка (локальные нормативные акты), в том числе направленные на обеспечение безопасности банка (ст. 189);
- не разглашать сведения, составляющие коммерческую (банковскую) и налоговую тайну, ставшие известными в связи с исполнением трудовых обязанностей (подп. «в» п. 6 ст. 81);
- нести в особо оговоренных случаях полную материальную ответственность за ущерб, причиненный банку (ст. 242 и 243).

. Закон о банковской деятельности обязывает всех служащих кредитной низации хранить тайну об операциях, счетах и вкладах ее клиентов и корюндентов (банковскую тайну), а также об иных сведениях, свободный уп к которым закрыт кредитной организацией (ст. 26).

. Положение Банка России № 242-П устанавливает для работников креной организации обязанности:

- доводить до сведения органов управления и руководителей структурных подразделений кредитной организации (филиала) информацию обо всех нарушениях законодательства Российской Федерации, учредительных и внутренних документов, случаях злоупотреблений, несоблюдения норм профессиональной этики (п. 3 Приложения № 1 к Положению);
- соблюдать требования законодательства о финансовых рынках, стандартов профессиональной деятельности на финансовых рынках, в кредитных организациях с целью обеспечения надлежащего уровня надежности и минимизации рисков банковской деятельности.

. Указание Банка России от 7 июля 1999 г. № 603-У «О порядке осуществления внутреннего контроля за соответствием деятельности на финансовых

рынках законодательству о финансовых рынках в кредитных организациях» (далее — Указание Банка России № 603-У):

а) вменяет в обязанность работнику, участвующему в осуществлении операций (сделок) кредитной организации, доводить до сведения своего непосредственного руководителя и представителя службы внутреннего контроля банка информацию:

- о юридических лицах, в которых он и (или) его родственники (супруг, супруга, родители, дети, братья, сестры) владеют самостоятельно или в группе лиц 20% или более голосующих акций (долей, паев) (п. 3.4);
- о юридических лицах, в органах управления которых он и (или) его родственники занимают должности (п. 3.4);
- об операциях (сделках), в совершении которых он может быть признан заинтересованным лицом, либо совершаемых сотрудником кредитной организации в своих интересах и за свой счет (п. 11.4);
- о совершаемых клиентами банка сделках, имеющих признаки незаконной легализации (отмывания) преступных доходов (п. 6.3, 6.4);

б) запрещает работнику, участвующему в осуществлении операций (сделок) кредитной организации на финансовых рынках, использовать служебную информацию в собственных интересах и передавать ее третьим лицам, проводить операции (сделки) в своих интересах (п. 5.4);

в) предписывает работнику, участвующему в осуществлении операций (сделок) кредитной организации на финансовых рынках:

- соблюдать приоритет интересов клиентов над интересами банка и своими собственными интересами в случае возникновения конфликта интересов (п. 3.3);
- ставить интересы банка выше собственных при совершении сделок на финансовых рынках (п. 3.4).

5. Положение Банка России от 9 октября 2002 г. № 199-П «О порядке ведения кассовых операций в кредитных организациях на территории Российской Федерации» (далее — Положение Банка № 199-П) обязывает работника, осуществляющего кассовые операции:

- строго соблюдать правила совершения операций с ценностями и их хранения;
- своевременно сообщать руководству банка обо всех обстоятельствах, угрожающих обеспечению сохранности вверенных ему ценностей;
- возмещать суммы допущенных по его вине недостач и не выявленных им неплатежных и поддельных денежных знаков;
- не разглашать сведения об операциях по хранению ценностей, их отправке, перевозке, охране, сигнализации, а также служебных поручениях по кассе.

5. Внутренние (локальные) нормативные акты банка, предписывающие нятие работником стандартов поведения, направленных на защиту инте-ов банка, и обязательств по их соблюдению.

Банк должен разработать для определенных категорий работников внут-ние (локальные) нормативные акты, устанавливающие специальные пра-а и стандарты поведения, связанные с обеспечением безопасности банка.

ила и стандарты разрабатываются в строгом соответствии с положениями онодательства, с учетом особенностей организации деятельности конкрет-о банка.

Общие правила поведения работников банка устанавливаются правилами реннего трудового распорядка. Специальные обязательства работника кретизируются (с учетом специфики выполняемых им трудовых обязанно-й) в инструкции по конфиденциальному делопроизводству, в правилах об-ения с материальными ценностями, стандартах профессиональной дея-ности в кредитных организациях и некоторых других, с которыми работ-знакомится под расписку.

Допускается перечислять обязанности работника, связанные с обеспечени-сохранности доверенных ему информации и ценностей, непосредственно рудовом договоре, который также заключается в письменной форме. При-ие работником специальных обязательств предполагает его согласие со-дать ряд дополнительных условий, установленных локальными докумен-и банка.

Работник, получающий допуск к сведениям, составляющим служебную коммерческую (банковскую) тайну, кроме обязанностей, непосредственно занных с обеспечением сохранности информации, представляет кадровому парату сведения о возникновении оснований для отказа к допуску (суди-сть за совершение преступлений против собственности, хозяйственных олжностных преступлений, совершение административного правонаруше-в области финансов и т. п.).

Поскольку выполнение отдельных правил и стандартов временно ограни-вает гражданские права работников, факт их принятия специально огова-вается в трудовом договоре. Принятие специальных обязательств является временным условием заключения договора, и наоборот, отказ от них слу-т основанием для прекращения трудового договора.

Основания для расторжения трудового договора с лицами, не отвечающими ебованиям безопасности, установленные нормами Трудового кодекса РФ и иных деральных законов:

1) Кодекс устанавливает возможность расторжения трудового договора инициативе работодателя в целях обеспечения безопасности банка по сле-ющим основаниям, связанным с наличием виновных действий (бездейст-я) работника, перечисленных в ст. 81. Такими действиями являются:

- разглашение охраняемой законом тайны, ставшей ему известной в связи с исполнением им трудовых обязанностей (подп. «в» п. 6);

- совершение по месту работы хищения (в том числе мелкое) чужого имущества, растраты, умышленного его уничтожения или повреждения, установленных вступившим в законную силу приговором суда или постановлением органа, уполномоченного на применение административных взысканий (подп. «г» п. 6)[1];
- совершение виновных действий непосредственно обслуживающим денежные или товарные ценности, если эти действия дают основание для утраты доверия к нему со стороны работодателя (п. 7);
- принятие необоснованного решения руководителем организации (филиала, представительства), его заместителями и главным бухгалтером, повлекшего нарушение сохранности имущества, неправомерное его использование или иной ущерб имуществу организации (п. 9);
- однократное грубое нарушение руководителем организации (филиала, представительства), его заместителями своих трудовых обязанностей (п. 10);
- предоставление работодателю подложных документов или заведомо ложных сведений при заключении трудового договора (п. 11);
- прекращение допуска к государственной тайне, если выполняемая работа требует допуска к ней (п. 12);
- совершение виновных действий, предусмотренных трудовым договором с руководителем организации, членами коллегиального исполнительного органа организации (п. 13);
- другие случаи, установленные Кодексом и иными федеральными законами (п. 14).

К числу других случаев относятся:

- осуждение работника за совершение преступления, не связанного с работой в банке, к лишению свободы, исправительным работам не по месту работы, либо к иному наказанию, исключающему возможность продолжения данной работы (в частности, к лишению права занимать определенные должности или заниматься определенной деятельностью в соответствии с наказанием, установленным ст. 47 УК РФ);
- дисквалификация (лишение физического лица права занимать руководящие должности в исполнительном органе управления юридического лица), назначенная в соответствии со ст. 3.11 на основании соответствующей статьи Особенной части КоАП РФ).

Законодательство по вопросам информации и информатизации

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации):

[1] До вступления в законную силу приговора суда работник может быть временно отстранен от занимаемой должности по требованию органа и должностных лиц, уполномоченных федеральными законами и иными нормативными правовыми актами (ст. 76 ТК РФ, ст. 29 и 114 УПК РФ).

- определяет принципы защиты конфиденциальной информации банка, права и обязанности банка в сфере обеспечения безопасности информационных процессов при применении информационных систем, технологий и средств их обеспечения (ст. 1);
- служит принципиальной основой для разработки законодательных норм, иных нормативных, в том числе локальных актов банка, регулирующих отношения, связанные с созданием, использованием и защитой информации (ст. 4);
- вводит понятие конфиденциальной информации, разновидностью которой является банковская тайна, и устанавливает основания для правомерного ограничения доступа к ее составляющим от посторонних (ст. 2);
- устанавливает в качестве основания защиты документированной информации возможность нанесения ущерба ее собственнику (банку) в случае неправомерного обращения с нею (ч. 1 ст. 16);
- обязывает собственника информационных ресурсов осуществлять контроль за выполнением требований по защите информации (п. 6 ч. 4 ст. 16);
- возлагает на собственника конфиденциальной информации обязанность обеспечивать уровень ее защиты в соответствии с законодательством (пп. 1–5 ч. 4 ст. 16).

каз Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня дений конфиденциального характера»[1] (в ред. Указа Президента РФ от ентября 2005 г. № 1111).

число сведений конфиденциального характера включены сведения, свяные с коммерческой деятельностью, доступ к которым ограничен в соотвии с Гражданским кодексом РФ и федеральными законами (коммерчея тайна) (п. 5 Перечня).

Сведения, составляющие банковскую тайну, относятся одновременно ведениям конфиденциального характера. Они связаны с коммерческой ельностью, доступ к ним ограничен в соответствии со ст. 857 ГК РФ (банская тайна) и ст. 26 Закона о банковской деятельности (банковская тайна).

Законодательство о безопасности

Закон о безопасности:

- закрепляет правовые основы обеспечения безопасности граждан и организаций (в том числе банков), дает понятие системы безопасности и ее функций;
- определяет понятие безопасности и перечисляет ее объекты (ст. 1);
- устанавливает ведущую роль государства в обеспечении безопасности названных объектов, признавая государство основным субъектом обеспечения безопасности, осуществляющим названные функции через органы законодательной, исполнительной и судебной власти;
- включает в число субъектов безопасности иные организации (к числу которых относится банк);
- наделяет субъектов безопасности (под определение которых попадает банк) правами и обязанностями по участию в обеспечении безопасности в соответствии с законодательством (ст. 2);
- предписывает государству обязанность проведения единой государственной политики в области обеспечения безопасности системой мер экономического, политического, организационного и иного характера (ст. 4);
- устанавливает законодательные основы обеспечения безопасности (ст. 6);
- определяет понятие системы безопасности, которую образуют органы законодательной, исполнительной и судебной власти, государственные, общественные, иные организации (под определение которых подпадают банки) и объединения, граждане, принимающие участие в обеспечении безопасности в соответствии с законом, а также законодательство, регламентирующее отношения в сфере безопасности (ст. 8);
- устанавливает основные функции системы безопасности, в числе которых выявление и прогнозирование угроз, осуществление комплекса оперативных и долговременных мер по их предупреждению и нейтрализации и проч. (ст. 9);
- разграничивает полномочия органов власти в системе безопасности (ст. 10).

Указ Президента РФ от 10 января 2000 г. № 24 «О Концепции национальной безопасности Российской Федерации».

В ней банковская система отнесена к важнейшим составляющим единого экономического пространства России, а ее ослабление включено в число угроз национальной безопасности страны.

Государственная стратегия экономической безопасности РФ (Основные положения), одобренная Указом Президента РФ от 29 апреля 1996 г. № 608.

Стратегия экономической безопасности Российской Федерации:

- определяет экономическую безопасность как составную часть национальной безопасности России;
- признает устойчивость финансовой и банковской систем одним из основных критериев, определяющих состояние экономической безопасности страны.

Постановление Правительства РФ от 27 декабря 1996 г. № 1569 «О первоочередных мерах по реализации Государственной стратегии экономической безопасности Российской Федерации (Основных положений), одобренной Указом Президента РФ от 29 апреля 1996 г. № 608»:

а) возлагает на федеральные органы исполнительной власти обязанность разработать с участием Банка России мер:

[1] Собрание законодательства РФ. 1997. № 10. Ст. 1127.

- по предотвращению угроз экономической безопасности страны;
- по организации мониторинга и прогнозирования факторов, определяющих возникновение угроз экономической безопасности;
- по проведению исследований для выявления тенденций и возможностей развития угроз (как существующих, так и вероятных) и поиску оптимальных путей их преодоления (п. 3);
- по созданию системы обеспечения экономической безопасности страны, включающей: выявление ситуаций, при которых фактические или прогнозируемые параметры экономического развития выходят за пределы пороговых значений, разработку мер по их преодолению (п. 5);

5) устанавливает Перечень критериев экономической безопасности РФ иложение № 2), в число которых включена устойчивость финансовой сисы. Обязанность разработки количественных (пороговых) и качественных аметров этого критерия возложена на федеральные органы исполнительвласти с участием Банка России (п. 6 Приложения № 2).

. Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания

Правовые акты общего действия, обеспечивающие безопасность банков имущественно методами охранительного содержания, представлены двумя аслями материального права — уголовного и административного, и соотствующими им процессуальными отраслями (уголовно-процессуальным дминистративно-процессуальным правом). Участие в реализации указан отраслей права государственных органов и должностных лиц регламентиано законодательством о субъектах правоохранительной деятельности, истности, Законом РФ от 18 апреля 1991 г. № 1026-1 «О милиции» (в ред. от тября 2007 г. № 225-ФЗ) (далее — Закон о милиции).

Особенности функционирования регулятивных правовых механизмов уканых отраслей права в сфере банковской безопасности заключаются в слещем.

Уголовное законодательство. Все нормы уголовного законодательства Росской Федерации представлены Уголовным кодексом РФ. В случае приняновых законов, предусматривающих уголовную ответственность, они подат включению в Кодекс. Уголовный кодекс РФ регулирует отношения по оду обеспечения безопасности банка путем установления уголовно-правоохраны от преступлений:

а) посягающих непосредственно на интересы (безопасность) легитимных ков (кредитной организации) *в сфере экономической деятельности* — незная банковская деятельность (ст. 172), способствующая незаконной коненции; незаконное получение кредита (ст. 176), злостное уклонение от пения кредиторской задолженности (ст. 177);

б) посягающих на интересы коммерческих и других организаций, к числу которых относится банк:

- *в сфере интересов службы в коммерческих и иных организациях* — злоупотребление полномочиями (ст. 201), коммерческий подкуп (ст. 204)[1];
- *в сфере экономической деятельности* — легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174), легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления (ст. 174.1), принуждение к совершению сделки или к отказу от ее совершения (ст. 179), незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183);
- *в сфере защиты собственности* — кража (ст. 158), мошенничество (ст. 159), присвоение или растрата (ст. 160), грабеж (ст. 161), разбой (ст. 162), вымогательство (ст. 163), умышленные уничтожение или повреждение имущества (ст. 167);
- *в сфере защиты компьютерной информации* — неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273), нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274);
- *в сфере защиты сотрудников банка от преступлений против жизни и здоровья, свободы, чести и достоинства личности, связанных с их профессиональной деятельностью,* — убийство (ст. 105), умышленное причинение тяжкого вреда здоровью (ст. 111), умышленное причинение средней тяжести вреда здоровью (ст. 112), умышленное причинение легкого вреда здоровью (ст. 115), побои (ст. 116), истязание (ст. 117), угроза убийством или причинением тяжкого вреда здоровью (ст. 119), похищение человека (ст. 126), незаконное лишение свободы (ст. 127), клевета (ст. 129), оскорбление (ст. 130).

Уголовно-процессуальное законодательство. Нормы уголовно-процессуального законодательства Российской Федерации представлены Уголовно-процессуальным кодексом РФ. В отличие от уголовного законодательства, в соответствии с ч. 3 ст. 1 УПК РФ допускает возможность применения в качестве источника процессуального права норм, не включенных в Кодекс, однако признанных международным договором Российской Федерации.

Уголовно-процессуальный кодекс РФ устанавливает порядок судопроизводства по фактам преступлений (в том числе посягающих на безопасность банка), обязательный для судов, органов прокуратуры, предварительного

[1] Уголовное преследование за эти деяния, если они причинили вред интересам исключительно коммерческой организации (банка), осуществляется по заявлению этой организации или с ее согласия.

ıствия и дознания, а также иных участников процесса (в число которых ıят банк и его служба безопасности).

Согласно ст. 21 УПК РФ уголовное преследование от имени государства уголовным делам осуществляет прокурор, а также следователь и дознава-. Эти должностные лица обязаны в каждом случае обнаружения призна- преступления принимать предусмотренные Уголовно-процессуальным ко-сом РФ меры по установлению события общественно опасного деяния, бличению лица (лиц), виновного в его совершении.

Применительно к сфере банковской безопасности исключение составляют ния (предусмотренные ст. 201 и 204 УК РФ, в случаях, если причинили ı интересам банка), уголовные дела по которым возбуждаются по заявле-руководителя банка или с его согласия (ст. 23 УПК РФ). Это заявление кит поводом для возбуждения уголовного дела (ст. 140 УПК РФ).

В случае совершения преступления, посягающего на безопасность банка, ледний приобретает права участника уголовного судопроизводства со сто-ы обвинения и может выступать в качестве потерпевшего (ст. 42), граж-ского истца (ст. 44), через своих представителей (ст. 45).

Выступая в качестве *потерпевшего*, банк в лице своего представителя имеет во:

- знать о предъявленном обвинении;
- давать показания;
- представлять доказательства;
- заявлять ходатайства и отводы;
- участвовать с разрешения следователя или дознавателя в следственных действиях, производимых по его ходатайству;
- знакомиться с протоколами следственных действий, произведенных с его участием, и подавать на них замечания;
- знакомиться с постановлением о назначении судебной экспертизы и заключением эксперта в случаях, предусмотренных ч. 2 ст. 198;
- знакомиться по окончании предварительного расследования со всеми материалами уголовного дела, выписывать из него любые сведения и в любом объеме, снимать копии с материалов уголовного дела, в том числе с помощью технических средств;
- получать копии постановлений о возбуждении уголовного дела, признании его потерпевшим или об отказе в этом, о прекращении уголовного дела, приостановлении производства по нему, а также копии приговора суда первой инстанции, решений судов апелляционной и кассационной инстанций;
- участвовать в судебном разбирательстве уголовного дела в судах первой, второй и надзорной инстанций;
- выступать в судебных прениях;
- поддерживать обвинение;

- знакомиться с протоколом судебного заседания и подавать на него замечания;
- приносить жалобы на действия (бездействие) и решения дознавателя, следователя, прокурора и суда;
- обжаловать приговор, определение, постановление суда;
- знать о принесенных по уголовному делу жалобах и представлениях и подавать на них возражения;
- ходатайствовать о применении мер безопасности в соответствии с ч. 3 ст. 11;
- осуществлять иные полномочия, предусмотренные Уголовно-процессуальным кодексом РФ.

Кроме того, потерпевший имеет право на возмещение имущественного и морального вреда, причиненного преступлением, а также расходов, понесенных в связи с его участием в ходе предварительного расследования и в суде, включая расходы на представителя, согласно требованиям ст. 131 УПК РФ.

В качестве *гражданского истца* банк наделяется правами:

- предъявлять (после возбуждения уголовного дела, но до окончания предварительного расследования) имущественный иск и иск для имущественной компенсации морального вреда без уплаты государственной пошлины;
- поддерживать гражданский иск;
- представлять доказательства;
- давать объяснения по предъявленному иску;
- заявлять ходатайства и отводы;
- знакомиться с протоколами следственных действий, произведенных с его участием;
- участвовать с разрешения следователя или дознавателя в следственных действиях, производимых по его ходатайству либо ходатайству его представителя;
- отказаться от предъявленного им гражданского иска на любой стадии уголовного судопроизводства (до удаления суда на совещание в совещательную комнату для вынесения приговора);
- знакомиться по окончании расследования с материалами уголовного дела, относящимися к предъявленному им гражданскому иску, и выписывать из уголовного дела любые сведения и в любом объеме;
- знать о принятых решениях, затрагивающих его интересы, и получать копии процессуальных решений, относящихся к предъявленному им гражданскому иску;
- участвовать в судебном разбирательстве уголовного дела в судах первой и апелляционной инстанций;
- выступать в судебных прениях для обоснования гражданского иска;
- знакомиться с протоколом судебного заседания и подавать на него замечания;

приносить жалобы на действия (бездействие) и решения дознавателя, следователя, прокурора и суда;
обжаловать приговор, определение и постановление суда в части, касающейся гражданского иска;
знать о принесенных по уголовному делу жалобах и представлениях и подавать на них возражения;
участвовать в судебном рассмотрении принесенных жалоб и представлений в порядке, установленном Уголовно-процессуальным кодексом РФ.

Доказательствами по уголовному делу, которые может представлять банк, ответствии со ст. 74 УПК РФ могут быть показания представителя потерпего (банка), а также документы и вещественные доказательства, относяся к расследуемому событию.

Право представителей банка собирать и представлять письменные докуты и предметы для приобщения их к уголовному делу в качестве доказств от имени потерпевшего и гражданского истца установлено ст. 86 К РФ.

Защитник, выступающий представителем банка (потерпевшего или гражского истца), кроме того, вправе собирать доказательства путем:
получения предметов, документов и иных сведений;
опроса лиц с их согласия;
истребования справок, характеристик, иных документов от органов государственной власти, местного самоуправления, общественных объединений и организаций, которые обязаны предоставлять запрашиваемые документы или их копии.

В качестве участника уголовного судопроизводства банк, признанный пострадевшим или гражданским истцом, имеет *право* обжаловать действия (бездействие) и решения органа дознания, дознавателя, следователя, прокурора, также иных лиц в той части, в которой производимые процессуальные действия и принимаемые процессуальные решения затрагивают его интересы (ст. 123 УПК РФ).

Законодательство об административных правонарушениях. Законодательство об административных правонарушениях состоит из КоАП РФ и принятых в соответствии с ним законов субъектов Российской Федерации об административных правонарушениях. Кроме того, в соответствии с ч. 2 ст. 1 КоАП РФ допускается возможность применения в качестве источника процессуального права норм, не включенных в Кодекс, однако признанных международным договором Российской Федерации.

КоАП РФ регулирует отношения по поводу обеспечения безопасности бизнеса путем установления защиты законных экономических интересов юридических лиц (к числу которых относится банк) от следующих видов административных правонарушений:

- осуществление предпринимательской деятельности без государственной регистрации или без специального разрешения (лицензии) (ст. 14.1);
- незаконное получение кредита (ст. 14.11);
- совершение сделок и иных действий, выходящих за пределы установленных полномочий (ст. 14.22);
- осуществление дисквалифицированным лицом деятельности по управлению юридическим лицом (ст. 14.23);
- нарушение законодательства о государственной регистрации (ст. 14.25);
- неисполнение банком поручения государственного внебюджетного фонда (ст. 15.10);
- грубое нарушение правил ведения бухгалтерского учета и представления бухгалтерской отчетности (ст. 15.11);
- недобросовестная эмиссия ценных бумаг (ст. 15.17);
- незаконные сделки с ценными бумагами (ст. 15.18);
- использование служебной информации на рынке ценных бумаг (ст. 15.21);
- нарушение правил ведения реестра владельцев ценных бумаг (ст. 15.22);
- уклонение от передачи регистратору ведения реестра владельцев ценных бумаг (ст. 15.23);
- нарушение валютного законодательства (ст. 15.25);
- нарушение законодательства о банках и банковской деятельности (ст. 15.26);
- нарушение законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ст. 15.27).

Административно-процессуальное законодательство. Нормы административно-процессуального законодательства представлены разделами III, IV и V КоАП РФ.

Раздел III содержит положения о субъектах (судьях, органах, должностных лицах), уполномоченных рассматривать дела об административных правонарушениях, и их компетенции. Раздел IV регламентирует порядок производства по делам об административных правонарушениях. Раздел V устанавливает порядок исполнения постановлений по делам об административных правонарушениях.

В соответствии с КоАП РФ перечисленные ниже органы и должностные лица наделены следующими административными полномочиями в сфере обеспечения банковской безопасности:

1. Суд — рассматривать дела об административных правонарушениях, предусмотренных ст. 14.1, 14.11, 14.21–14.23, 15.12 и 15.26).

2. Прокурор — возбуждать дела о любом другом административном правонарушении, ответственность за которое предусмотрена КоАП РФ или законом субъекта Российской Федерации.

). Органы милиции — возбуждать дела об административных правонару-
ениях, предусмотренных ст. 14.1, 14.11.
. Должностные лица органов, уполномоченных в области банкротства
инансового оздоровления, — возбуждать дела об административных пра-
арушениях, предусмотренных ст. 14.21–14.23.
. Органы, уполномоченные в области рынка ценных бумаг — возбуждать
ссматривать дела об административных правонарушениях, предусмотрен-
ст. 15.17–15.24.
. Органы валютного контроля — рассматривать дела об административ-
правонарушениях, предусмотренных ст. 15.25.
. Должностные лица Банка России — составлять протоколы об админи-
тивных правонарушениях, предусмотренных ст. 15.26.
. Федеральный орган исполнительной власти, уполномоченный прини-
меры по противодействию легализации (отмыванию) доходов, получен-
преступным путем, и финансированию терроризма, — рассматривать де-
б административных правонарушениях, предусмотренных ст. 15.27.

***аконодательство о милиции и негосударственных предприятиях, участвую-
в обеспечении банковской безопасности методами охранительного содер-
ия.***

акон о милиции определяет милицию в Российской Федерации как
тему государственных органов исполнительной власти, призванных за-
щать жизнь, здоровье, права и свободы граждан, собственность, интере-
бщества и государства от преступных и иных противоправных посяга-
ств, и наделенных правом применения мер принуждения в установлен-
пределах.

огласно ст. 10 Закону о милиции, на милицию возлагаются следующие
анности, имеющие отношение к обеспечению безопасности в банковской
е:

) предотвращать, выявлять, пресекать и расследовать, в соответствии
оловно-процессуальным кодексом РФ преступления:
- посягающие исключительно на безопасность банка;
- посягающие на безопасность банка наряду с другими объектами защиты;

) предотвращать и пресекать, в соответствии с КоАП РФ, администра-
ые правонарушения, посягающие на безопасность банка;
) выявлять обстоятельства, способствующие совершению указанных пре-
лений и административных правонарушений, и в пределах своих прав
нимать меры к устранению данных обстоятельств;
) принимать и регистрировать заявления, сообщения и иную поступаю-
информацию о преступлениях, административных правонарушениях
бытиях, угрожающих безопасности банка, своевременно принимать меры,
усмотренные законодательством;

д) разыскивать лиц, совершивших преступление, скрывающихся от органов дознания, следствия и суда, уклоняющихся от исполнения уголовного наказания, а также разыскивать похищенное имущество;

е) охранять на основе договоров с юридическими лицами (в том числе с банками) принадлежащее им имущество;

ж) лицензировать деятельность частных детективных и охранных предприятий, согласовывать уставы служб безопасности в организациях (в том числе кредитных), контролировать соблюдение установленных федеральным законом правил частной детективной и охранной деятельности (в том числе служб безопасности банков);

з) осуществлять взаимодействие с охранными структурами банков и межбанковских объединений в сфере обеспечения банковской безопасности (в соответствии с принципами деятельности, установленными в ст. 4 Закона).

Принятое в развитие Закона Положение о Министерстве внутренних дел РФ (утв. Указом Президента РФ от 19 июля 2004 г. № 927) конкретизирует изложенные Законом о милиции основные задачи и функции МВД России, в том числе имеющие непосредственное отношение к обеспечению безопасности в банковской сфере.

Разработанное на основе Закона Соглашение между МВД России и Ассоциацией российских банков о взаимодействии в области обеспечения банковской безопасности от 29 декабря 1995 г. (объявлено приказом МВД России от 4 января 1996 г. № 4 «О реализации Соглашения между МВД России и Ассоциацией российских банков») устанавливает следующие основные направления такого взаимодействия:

- защита коммерческих банков от проникновения организованных преступных групп в их среду;
- защита банковских организаций и их сотрудников от преступных посягательств;
- разработка и внедрение специальных технологий по технической укрепленности и защите банковских объектов, средств связи и т. д.;
- совершенствование систем обеспечения безопасности инкассации и транспортировки денежных средств, а также банковских объектов пунктов обмена валют, хранилищ, офисов и т. п.;
- оказание помощи в обучении, переподготовке и повышении квалификации кадров для служб безопасности банков;
- разработка совместных предложений по совершенствованию правовой основы обеспечения банковской безопасности.
- осуществление системы мер, направленных на предупреждение и раскрытие преступлений (ст. 3), на совершенствование информационного обмена между сторонами Соглашения (ст. 4) и расширение законодательной базы взаимодействия (ст. 5).

Закон о частной детективной деятельности определяет частную детективную и охранную деятельность как оказание на возмездной договорной основе

уг физическим и юридическим лицам предприятиями, имеющими специ-
ое разрешение (лицензию) органов внутренних дел, в целях защиты за-
ных прав и интересов своих клиентов.
акон о частной детективной деятельности предоставляет банку возмож-
ть пользоваться для обеспечения безопасности кредитной организации ус-
ми детективного и охранного характера (ст. 1), в том числе:
а) заключить договор с частным детективом, объединением частных де-
ивных предприятий (ст. 9) и (или) охранным предприятием (ст. 11);
) учредить охранно-сыскное предприятие банка в виде обособленного
разделения (службы безопасности) с правом открытия текущих и расчет-
счетов для осуществления охранно-сыскной деятельности в интересах
ственной безопасности учредителя (ст. 14);
з) осуществлять в целях обеспечения безопасности банка в рамках полно-
ий службы безопасности:

- сбор сведений по гражданским делам;
- изучение рынка, сбор информации для деловых переговоров, выяв-
ление некредитоспособных или ненадежных деловых партнеров;
- установление обстоятельств неправомерного использования в предпри-
нимательской деятельности фирменных знаков и наименований, не-
добросовестной конкуренции, а также разглашения сведений, состав-
ляющих коммерческую (и ее разновидность — банковскую) тайну;
- выяснение биографических и других характеризующих личность
данных об отдельных гражданах (с их письменного согласия) при за-
ключении ими трудовых и иных контрактов;
- поиск утраченного банком имущества;
- сбор сведений по уголовным делам;
- защиту жизни и здоровья персонала банка;
- охрану имущества банка;
- проектирование, монтаж и эксплуатационное обслуживание средств
охранно-пожарной сигнализации;
- консультирование и подготовку рекомендаций по вопросам право-
мерной защиты от противоправных посягательств (ст. 3).

*Эрганизационные, правовые и иные нормативные вопросы учреждения и функ-
нирования охранно-сыскных предприятий регламентируют:*

1. Инструкция «Об организации работы по лицензированию и осуществ-
ию органами внутренних дел контроля за частной детективной и охранной
гельностью на территории Российской Федерации», утвержденная прика-
МВД России от 19 июня 2006 г. № 4471 — порядок лицензирования служ-
безопасности (частной детективной и охранной деятельности).
2. Перечень видов вооружения охранников, утвержденный постановлени-
Правительства РФ от 14 августа 1992 г. № 587 — виды вооружения охран-
организаций (в том числе охранно-сыскных), порядок его приобретения,
га, хранения и ношения.

2.3. Банковское законодательство

Обеспечение безопасности банков, стабильности банковской системы и защиты интересов вкладчиков является важнейшим направлением законодательных установлений, посвященных банковскому делу и банковской системе. В целях реализации указанных задач банковское законодательство детально регламентирует порядок создания и функционирования кредитных организаций и устанавливает квалификационные требования к их руководителям, создает систему банковского контроля и надзора за соблюдением банками законодательных и иных нормативных предписаний в сфере безопасности, наделяет Центральный банк Российской Федерации (Банк России) правами и обязанностями органа банковского регулирования и надзора.

Законом о Банке России на Банк России, выступающий в качестве органа банковского регулирования и надзора, возложена обязанность осуществлять надзорные, контрольные и специальные разрешительные функции за деятельностью кредитных организаций в целях поддержания стабильности банковской системы, защиты интересов вкладчиков и кредиторов (ст. 56). Регулирующие и надзорные функции Банка Росси нацелены прежде всего на решение вопросов безопасности путем создания имущественно полноценной кредитной организации, формирование у банка ресурсов, позволяющих обеспечить адекватную защиту от угроз и их последствий. Понятие ресурсов банка, наряду с имуществом, включает в себя, как известно, квалифицированное руководство и управленческий персонал.

В соответствии со ст. 59 Банку России предоставлено право регистрировать кредитные организации в Книге государственной регистрации кредитных организаций, выдавать кредитным организациям лицензии на осуществление банковских операций и отзывать их.

В процессе регистрации и выдачи лицензии Банк России, руководствуясь интересами безопасности кредитной организации, предъявляет квалификационные требования в области безопасности банковского дела к руководителям исполнительных органов, а также к главному бухгалтеру кредитной организации (ст. 60).

Другое основное направление участия Банка России в обеспечении финансовой стабильности кредитных организаций состоит в установлении и поддержании надлежащего порядка его функционирования. В этих целях Банк России разрабатывает нормативные предписания, относящиеся к порядку проведения банковских операций, к организации управления банковскими рисками и к организации внутреннего контроля в банке.

Банк России имеет право устанавливать обязательные для кредитных организаций правила проведения банковских операций, ведения бухгалтерского учета, составления и представления бухгалтерской и статистической отчетности (ст. 57). При этом Банк России может запрашивать и получать у кредитных

анизаций необходимую информацию об их деятельности, требовать разъ-ений по полученной информации.

В соответствии со ст. 62 в целях обеспечения устойчивости кредитных ор-изаций Банку России предоставлено право устанавливать обязательные ормативы экономического характера, в том числе максимальный размер пных кредитных рисков и максимальный размер риска на одного кредито-вкладчика) и т. д.

Банк России вправе проверять кредитные организации и их филиалы для ествления своих функций в области банковского надзора и регулирова-(ст. 73).

Для выявления ситуаций, угрожающих законным интересам кредиторов падчиков), стабильности банковской системы в целом, Банк России анали-ует деятельность кредитных организаций (ст. 75). Наличие таких ситуаций жит основанием для принятия Банком России мер надзорного характера есение обязательных для исполнения предписаний и наложение санкций, дусмотренных ст. 75.

В случае невыполнения в установленный Банком России срок предписа-об устранении выявленного нарушения, а также в случае, если это нару-ие или совершаемые кредитной организацией операции создали реальную розу интересам кредиторов (вкладчиков), Банк России вправе:

а) взыскать с кредитной организации штраф до 1% размера оплаченного ус-ного капитала, но не более 1% минимального размера уставного капитала;

б) потребовать от кредитной организации:

- проведения мероприятий по ее финансовому оздоровлению, в том числе изменения структуры активов;
- замены ее руководителей;
- реорганизации;

в) изменить для кредитной организации обязательные нормативы на срок шести месяцев;

г) ввести запрет на осуществление кредитной организацией отдельных ковских операций, предусмотренных выданной лицензией, на срок до од-о года, а также на открытие филиалов на тот же срок;

д) назначить временную администрацию по управлению кредитной орга-ацией на срок до шести месяцев. Порядок назначения и деятельности вре-ной администрации устанавливается федеральными законами и издавае-ми в соответствии с ними нормативными актами Банка России;

е) отозвать у кредитной организации лицензию на осуществление банков-х операций по основаниям, предусмотренным Законом о банковской дея-ьности. Порядок отзыва лицензии на осуществление банковских операций навливается нормативными актами Банка России.

Нарушение кредитной организацией установленных Банком России норма-ов и иных обязательных требований признается административным право-ушением и влечет предупреждение или наложение административного

штрафа (п. 2 ст. 15.26 КоАП РФ). Составление административных протоколов о таких правонарушениях отнесено к компетенции должностных лиц Банка России (ст. 28.3 КоАП РФ).

Закон о банковской деятельности установил систему положений, имеющих целью обеспечить стабильность банковской системы, финансовую надежность банков, защиту прав, интересов вкладчиков и кредиторов кредитных организаций:

а) дал определение понятия банка (ст. 1), которое позволило выделить банк из числа других объектов с целью защиты (в том числе путем применения ст. 172 УК РФ) его исключительного права заниматься банковской деятельностью;

б) установил исчерпывающий перечень банковских операций (ст. 5 Закона) и порядок их лицензирования (ст. 13), обеспечив исключительное право банка на их осуществление;

в) закрепил возможность обеспечения безопасности банковской системы путем:

- отказа в регистрации;
- отзыва лицензий у кредитных организаций, не отвечающих требованиям безопасности.

Организация, претендующая на регистрацию и получение лицензии на осуществление банковских операций, обязана предоставить:

- декларации о доходах учредителей — физических лиц, подтверждающие источники происхождения средств, вносимых в уставный капитал кредитной организации (содержание которых позволяет сделать вывод о чистоте капитала и налоговой правопослушности учредителей — п. 7 ст. 14);
- анкеты кандидатов на должности руководителей исполнительных органов и главного бухгалтера кредитной организации, заполняемые ими и содержащие сведения, подтверждающие их профессиональную компетентность и положительную деловую репутацию (п. 8 ст. 14).

Решение об отказе в государственной регистрации кредитной организации и выдаче лицензии на осуществление банковских операций может быть принято только на основаниях несоответствия квалификационным требованиям вышеназванных уполномоченных лиц банка и неудовлетворительного финансового положения учредителей кредитной организации или невыполнения ими своих обязательств перед бюджетами различного уровня за последние три года (ст. 16).

Обеспечение безопасности банковской системы путем отзыва лицензии на осуществление банковских операций осуществляется Банком России в следующих названных в ст. 20 Закона случаях:

- установление недостоверности сведений, на основании которых выдана лицензия;
- задержка начала осуществления банковских операций, предусмотренных лицензией, более чем на год со дня ее выдачи;

- установление факта недостоверности отчетных данных, задержка более чем на 15 дней представления ежемесячной отчетности (отчетной документации);
- осуществление, в том числе однократного, банковских операций, не предусмотренных лицензией Банка России;
- неисполнение требований федеральных законов, регулирующих банковскую деятельность, а также нормативных актов Банка России, если в течение года к кредитной организации неоднократно применялись меры, предусмотренные Законом о Банке России;
- неспособность кредитной организации удовлетворить требования кредиторов по денежным обязательствам и (или) исполнить обязанность по уплате обязательных платежей в течение одного месяца с наступления даты их исполнения, если требования к кредитной организации в совокупности составляют не менее 1 тыс. минимальных размеров оплаты труда;
- неоднократное в течение года виновное неисполнение содержащихся в исполнительных документах арбитражных судов требований о взыскании денежных средств со счетов (вкладов) клиентов кредитной организации при наличии денежных средств на счете (во вкладе) этих лиц.

В целях обеспечения финансовой надежности (в том числе локализации иных последствий угроз) кредитная организация обязана:

- создавать соответствующие резервы (фонды), минимальные размеры которых устанавливаются Банком России;
- осуществлять классификацию активов, выделяя сомнительные и безнадежные долги, и создавать резервы (фонды) на покрытие возможных убытков в порядке, устанавливаемом Банком России;
- организовывать внутренний контроль, обеспечивающий надлежащий уровень надежности, соответствующий характеру и масштабам проводимых операций (ст. 24).

Значимым элементом обеспечения безопасности банка является установленная ст. 26 обязанность кредитной организации и ее служащих хранить банковскую тайну, содержанием которой является информация об операциях, счетах и вкладах своих клиентов и корреспондентов. Ответственность за разглашение банковской тайны, наряду с сотрудниками банка, возлагается на должностных лиц других организаций, которым эти сведения стали известны в связи с исполнением служебных обязанностей.

2.4. Нормативные акты Банка России

Нормативные акты Банка России, регулирующие отношения в сфере обеспечения безопасности банков, издаются в соответствии со ст. 7 Закона о Банке России в форме *указаний*, *положений и инструкций*.

Правила подготовки нормативных актов Банка России устанавливаются Банком России самостоятельно. Согласно Положению ЦБ РФ от 15 сентября 1997 г. № 519 «О порядке подготовки и вступления в силу нормативных актов Банка России» нормативные акты издаются в виде:

- *указаний*, если их содержанием является установление отдельных правил по вопросам, отнесенным к компетенции Банка России;
- *положений*, если их основным содержанием является установление системно связанных между собой правил по вопросам, отнесенным к компетенции Банка России;
- *инструкций*, если их основным содержанием является определение порядка применения положений федеральных законов, иных нормативных правовых актов по вопросам компетенции Банка России (в том числе указаний и положений Банка России).

Кроме того, в соответствии с Положением ЦБ РФ от 18 июля 2000 г. № 115-П Банк России издает также официальные разъяснения по вопросам применения федеральных законов и иных нормативных правовых актов. Эти разъяснения нормативными актами не являются, однако обязательны для применения субъектами, на которых распространяет свою силу нормативный правовой акт, по вопросам применения которого издано официальное разъяснение Банка России.

Нормативные акты Банка России, регулирующие правоотношения в сфере обеспечения безопасности кредитных организаций (коммерческих банков), разграничены на две основные группы.

В *первую* входят нормативные предписания, устанавливающие *обязательные для банков правила и условия безопасности банковской деятельности*, в том числе:

- нормативные предписания, призванные обеспечить требования безопасности банковской деятельности в процессе создания и регистрации банков;
- обязательные нормативы экономической безопасности (минимального размера собственных средств, максимальных размеров рисков различного вида и т. д.);
- нормативные предписания, устанавливающие меры защиты банковских операций и видов банковской деятельности от противоправных посягательств;
- нормативные предписания, устанавливающие систему внутреннего контроля банков в целях выявления и предупреждения рисков и угроз их деятельности.

Вторая группа нормативных актов устанавливает *механизм реализации Банком России полномочий в области контроля и надзора за соблюдением кредитными организациями банковского законодательства* (включая вышеуказанные правила). Акты второй группы регламентируют право Банка России:

- запрашивать и получать у банков необходимую информацию об их деятельности и требовать по ней разъяснений;
- применять меры надзорного и административного характера в случае нарушения кредитными организациями банковского законодательства и ведомственных нормативных актов[1];
- проверять кредитные организации и их филиалы.

Ведомственные нормативные предписания, имеющие целью обеспечить выполнение требований безопасности в процессе создания и регистрации банков.

Инструкция Банка России от 14 января 2004 г. № 109-И «О порядке принятия Банком России решения о государственной регистрации кредитных организаций и выдаче лицензий на осуществление банковских операций» устанавливает следующие обязательные показатели безопасности, которым должно соответствовать регистрируемая кредитная организация (банк):

- устойчивое финансовое положение учредителя;
- временной ценз деятельности учредителя не менее трех лет;
- отсутствие задолженности учредителя перед федеральным, региональным и местным бюджетом за последние три года;
- способность банка сохранять финансовую стабильность и выполнять пруденциальные нормы деятельности;
- право собственности одного из учредителей на здание (помещение), в котором будет располагаться банк, или обязательство о предоставлении его в аренду (субаренду) лицом, не являющимся учредителем;
- наличие подразделения внутреннего контроля;
- достаточный уровень компетентности кандидатов на должности руководителей исполнительных органов и главного бухгалтера кредитной организации, отсутствие у них судимости и положительная деловая репутация;
- наличие в банковском здании охранно-пожарной и тревожной сигнализации и технически укрепленного кассового узла для осуществления кассовых операций.

Несоответствие этим условиям (требованиям безопасности) служит основанием для отказа в государственной регистрации кредитной организации (банка).

Инструкция Банка России от 16 января 2004 г. № 110-И «Об обязательных нормативах банков» в целях обеспечения экономических условий устойчивого функционирования банковской системы России, защиты интересов вкладчиков и кредиторов устанавливает обязательные нормативы:

- достаточности собственных средств (капитала) банка;
- ликвидности банков;
- максимального размера риска на одного заемщика или группу связанных заемщиков;

[1] Разграничение нормативных актов на эти группы в определенной мере условно, поскольку ведомственные указания, положения и инструкции Банка России в ряде случаев включают нормативные предписания обоих видов.

- максимального размера крупных кредитных рисков;
- максимального размера кредитов, банковских гарантий и поручительств, предоставленных банком своим участникам (акционерам);
- совокупной величины риска по инсайдерам банка;
- использования собственных средств (капитала) банков для приобретения акций (долей) других юридических лиц.

Долговременные нормативные акты, устанавливающие правила обеспечения безопасности безналичных и наличных расчетов.

Положение Банка России от 3 октября 2002 г. № 2-П «О безналичных расчетах в Российской Федерации» (далее — Положение Банка России № 2-П)[1] устанавливает технологию безопасного проведения операций по безналичным расчетам между юридическими лицами в валюте России и на ее территории с использованием предусмотренных российским законодательством расчетных документов (платежные поручения, аккредитивы, чеки, платежные требования, инкассовые поручения), а также правила проведения расчетных операций по корреспондентским счетам (субсчетам) кредитных организаций (филиалов), в том числе открытых в Банке России, и счетам межфилиальных расчетов.

Положение, разработанное с учетом криминалистических рекомендаций технического и методического характера, вводит строго определенные формы безналичных расчетов, условия их применения и обработки, предписывает порядок проверки подлинности расчетных документов и изложенных в них сведений при приеме банком.

Положение Банка России № 199-П устанавливает порядок безопасного совершения кассовых операций с участием физических и юридических лиц, а также инкассации денежных средств и других ценностей для кредитных организаций и их филиалов, действующих на территории России.

Регламентированные Положением требования безопасности работы с наличными денежными средствами и ценными бумагами, предусматривают:

- применение кассовых технологий, исключающих внедрение поддельных денежных чеков в процессе их операционной обработки;
- реализацию мер правового и организационного характера, направленных на установление специальных обязательств работников касс (инкассации) и ответственности за их нарушения;
- оснащение работников кассы техническими средствами и методиками для выявления неплатежных и поддельных денежных знаков;
- оборудование кассового узла банка согласно требованиям к его устройству и технической укрепленности в целях обеспечения сохранности денег и других ценностей;
- соблюдение установленных требований к техническому состоянию инкассаторского спецавтотранспорта и его специальному оборудованию,

[1] Указанное Положение не распространяется на порядок безналичных расчетов физических лиц. Относительно последних см. Положение ЦБ РФ от 1 апреля 2003 г. № 222-П «О порядке осуществления безналичных расчетов физическими лицами в Российской Федерации».

к средствам защиты и вооружения, необходимых для обеспечения безопасности сотрудников инкассации и сохранности перевозимых ценностей.

Распоряжение Банка России от 26 января 2006 г. № Р-27 о введении в дейие стандарта Банка России СТО БР ИББС-1.0–2006 «Обеспечение информационной безопасности организаций банковской системы Российской Феации» устанавливает требования по обеспечению информационной безности в организациях банковской системы Российской Федерации.

Введение в действие этого стандарта повысило надежность применяемых ками мер защиты от противоправных посягательств на охраняемую банскую информацию.

Инструкции оперативного характера, содержащие требования безопасности осуществления отдельных видов банковской деятельности. Инструкция порядке осуществления операций доверительного управления и бухгалтерм учете этих операций кредитными организациями Российской Федера», утвержденная Приказом Банка России от 2 июля 1997 г. № 02–287, сожит положения, направленные на предотвращение конфликтов интересов юн (п. 5.3), на предотвращение незаконного использования служебной юрмации (п. 5.4), на анализ и предупреждение рисков криминального хагера.

Банк — доверительный управляющий, обязан:

- установить запреты и ограничения на участие сотрудников в сделках, противоречащих интересам клиента;
- осуществить разработку правил обмена служебной и конфиденциальной информацией и обеспечить контроль за ее соблюдением служащими;
- вести анализ рисков (в том числе рисков преступных посягательств), возникающих в процессе доверительного управления, и принимать необходимые меры для предотвращения финансовых потерь вследствие ошибок, мошенничества сотрудников, а также превышения дилерами или другими работниками своих полномочий или исполнения своих обязанностей с нарушением принятых стандартов деятельности, этических норм либо разумных пределов риска (подп. «г» п. 1 приложения 6).

Методические рекомендации Банка России, посвященные вопросам разработки осуществления мер защиты банков от противоправных посягательств. Рендации по разработке кредитными организациями правил внутреннего троля в целях противодействия легализации (отмыванию) доходов, полых преступным путем, и финансированию терроризма даны в приложек письму Банка России от 13 июля 2005 г. № 99-Т.

Методические рекомендации по проверке кассовой работы, утвержденные мом Банка России от 4 июня 1996 г. № 25–1–601, информируют банки тодах проверки защищенности наличных денег и других ценностей от тивоправных посягательств.

Нормативные акты, регламентирующие вопросы организации и функционирования системы внутреннего контроля банка. Положение Банка России № 242-П предписывает банку обязанность создать систему внутреннего контроля, основными задачами которой является своевременное выявление действий и обстоятельств, угрожающих порядку функционирования и имуществу банка, принятие решений, направленных на их устранение.

Нормативные акты, устанавливающие право Банка России получать от банков необходимую информацию об их деятельности и требовать по ней разъяснений. Указание Банка России от 16 января 2004 г. № 1375-У «О правилах составления и представления отчетности кредитными организациями в Центральный банк Российской Федерации» устанавливает обязанность кредитных организаций систематически (с предписанной периодичностью по разработанной Банком России форме) представлять информацию, необходимую для целей банковского надзора и регулирования, в том числе для анализа состояния безопасности кредитной организации.

В соответствии с этим указанием наряду с отчетностью по установленным формам Банк России вправе запрашивать от кредитных организаций отдельные сведения и разъяснения в разовом порядке, а также проводить единовременные обследования деятельности кредитных организаций. Кроме сведений, представляемых в виде периодических отчетов, Банк России наделен правом получать информацию, представляемую в особом порядке. К этим сведениям относится информация, которая представляется для получения предварительного согласия Банка России по вопросам, возникающим в процессе создания и функционирования банка.

Специально выделенным видом информации, предоставляемой Банку России кредитной организацией, являются сведения о состоянии внутреннего контроля банка. Согласно п. 5.1. Положения Банка России № 242-П кредитные организации предоставляют в территориальные учреждения Банка России Справку о внутреннем контроле в кредитной организации по установленной Положением форме один раз в год по специально установленной форме, предусматривающей ответы на вопросы о наличии и особенностях организации службы внутреннего контроля, о количестве выявленных службой нарушений и других результатах ее деятельности.

При необходимости Банк России может запрашивать у банка отчет о состоянии внутреннего контроля за определенный период его деятельности, а также любую иную информацию по вопросам компетенции службы внутреннего контроля банка.

Обо всех существенных изменениях системы внутреннего контроля (в частности, о назначении и освобождении от должности руководителя службы внутреннего контроля) банк обязан уведомить в трехдневный срок территориальное учреждение Банка России.

Нормативные акты, регламентирующие порядок проверок коммерческих банков и их филиалов. Инструкция Банка России от 25 августа 2003 г. № 105-И

порядке проведения проверок кредитных организаций (и их филиалов
лномоченными представителями Центрального банка Российской Федера
и (Банка России)» устанавливает порядок проверки кредитных организа
и и их филиалов с целью выявить ситуацию, угрожающую интересам кре
оров и вкладчиков, проверить соблюдение кредитными организациями
филиалами банковского, валютного законодательства и нормативных ак
Банка России.

В необходимых случаях проверки кредитных организаций и их филиало
ествляются в координации с правоохранительными и финансовыми ор
ами.

Установленные Инструкцией способы проверки включают изучение доку
итов банка, информации, содержащейся в базах данных, собеседовани
отрудниками, проведение контрольных расчетов, а также тестирование ап
атно-программных средств, используемых банком для выполнения бан
ских операций, их учета и составления документов.

Периодичность проверок банков устанавливается Банком России, как пра
о, не реже одного раза в два года. Кредитные организации (их филиалы
ериод проверки должны содействовать ее проведению.

Оценка работы банка по результатам материалов проверки может сопрово
иться необходимыми рекомендациями, а в установленных случаях — пред
аниями по устранению выявленных недостатков. Контроль за выполнени
редписаний и рекомендаций, направленных кредитной организации (фи
лу), осуществляется подразделениями банковского надзора.

*Содержание и порядок применения мер надзорного и административного ха
тера* в случае нарушения кредитной организацией банковского законода
ьства и ведомственных нормативных актов регламентировано следующим
ументами.

Инструкция «О применении к кредитным организациям мер воздействия
нарушения пруденциальных норм деятельности», введенная в действие при
ом Банка России от 1 марта 1997 г. № 02–139, устанавливает порядок приме
ия к кредитным организациям предупредительных и принудительных мер
действия за нарушение пруденциальных норм деятельности (п. 3).

Согласно п. 1.9 меры предупредительного характера могут осуществляться
орме:

- доведения до органов управления кредитной организации информации
о недостатках в ее деятельности;
- изложения рекомендаций надзорного органа по исправлению создав
шейся в кредитной организации ситуации;
- предложения представить в надзорный орган программу мероприятий,
направленных на устранение недостатков, включая при необходимости
обязательства, принимаемые на себя кредитной организацией, ее учре
дителями (участниками);

- установления дополнительного контроля за деятельностью кредитной организации и за выполнением ею мероприятий по нормализации деятельности.

Основные принудительные меры воздействия (п. 1.15):

- штраф;
- требование об осуществлении кредитной организацией мероприятий по ее финансовому оздоровлению, в том числе требование о предоставлении и выполнении плана финансового оздоровления (плана санации);
- ограничение проведения кредитными организациями отдельных операций на срок до шести месяцев;
- запрет на осуществление кредитными организациями банковских операций, предусмотренных выданной лицензией, на срок до одного года;
- запрет на открытие филиалов на срок до одного года;
- требование о замене руководителей кредитной организации;
- введение временной администрации по управлению кредитной организацией;
- отзыв лицензии на осуществление банковских операций.

В соответствии со ст. 20 Закона о банковской деятельности объявляется процедура отзыва банковской лицензии.

2.5. Внутренние нормативные акты банков

Современная система правового регулирования деятельности банка посредством норм, установленных государством и его уполномоченными органами, не может регламентировать всех особенностей возникающих при этом отношений. Более того, государство и не преследует такой цели. Признавая за хозяйствующими субъектами (банками) право самим восполнить неполноту нормативной регламентации, законодатель предоставил им возможность принимать внутренние (локальные) нормативные акты, исходя из своей структуры и специфики осуществляемой деятельности.

Локальные нормативные акты представляют собой одну из разновидностей правовых норм. Они разрабатываются в рамках банка на основе законодательства Российской Федерации и адресуются, в первую очередь, акционерам и персоналу. Однако в ряде случаев их содержание имеет правовое значение и для лиц, посторонних для кредитной организации. Например, подписание договора от имени банка (или другой организации) сотрудником, не имеющим на это полномочий, установленных внутренним нормативным актом, может повлечь нежелательные правовые последствия для контрагента.

Обязанность банка принять нормативные акты локального регулирования, в одних случаях, прямо предусмотрена законодательством и нормативными

ами ведомств. В других — не будучи предписанной непосредственно — вы-
ает из смысла конкретных законодательных актов.
Главный локальный нормативный акт банка — его устав. Принятие банком
ава в соответствии со ст. 14 Закона о банковской деятельности и является
зательным условием регистрации кредитной организации и получения ли-
зии на осуществление банковских операций.
Федеральный закон от 21 ноября 1996 г. № 129-ФЗ «О бухгалтерском уче-
(в ред. от 3 ноября 2006 г. № 183-ФЗ) (далее — Закон о бухгалтерском уче-
в ст. 6 требует от руководителей банка принять и утвердить внутренни
рмативные акты, регламентирующие учетную политику коммерческой ор-
изации, в том числе порядок проведения инвентаризации и методы оценк
ов имущества и обязательств; порядок контроля за хозяйственными опера-
ми и т. д.
Прямое предписание банку о принятии внутренних нормативных доку-
нтов, регулирующих деятельность службы внутреннего контроля, содер-
тся в п. 2 ст. 7 Закона о противодействии легализации преступных доходов.
Локальные нормативные акты, регламентирующие порядок обеспечения
ковской тайны (которая охватывается понятием коммерческой тайны)
текают из содержания Закона о банковской деятельности, обязывающего
к хранить тайну (ст. 26. Банковская тайна).
Конкретные меры по организации охраны конфиденциальности информа-
и предусмотрены ст. 10 Федерального закона «О коммерческой тайне
29 июля 2004 г. № 98-ФЗ (в ред. от 24 июля 2007 г. № 214-ФЗ) (далее — За-
о коммерческой тайне). В их число входит принятие банком локальных
рмативных актов:
а) определяющих перечень информации, составляющей коммерческую
ну;
б) ограничивающих доступ к информации, составляющей коммерческую
ну, путем установления порядка обращения с этой информацией и контро-
за соблюдением такого порядка;
в) регулирующих отношения по использованию информации, составляю-
й коммерческую тайну, работниками на основании трудовых договоров
онтрагентами на основании гражданско-правовых договоров.
Локальные нормативные акты, содержащие нормы трудового права, регу-
рующие отношения между банком (работодателем) и его сотрудниками
фере защиты конфиденциальной информации, а также в других сферах
к обязан принять в пределах своей компетенции в соответствии со ст. 8
РФ.
Государство не ограничивает количества и видов внутренних нормативных
ов банка. Однако в соответствии с п. 5.1. Положения Банка России № 242-П
кегодном отчете Банку России о состоянии внутреннего контроля кредит-
организация должна сообщить о наличии предусмотренного названным

Положением перечня локальных нормативных актов, регулирующих ее деятельность в сфере обеспечения безопасности банковской деятельности[1].

Процедура принятия локальных нормативных актов установлена Федеральным законом от 26 декабря 1995 г. № 208-ФЗ «Об акционерных обществах» (далее — Закон об акционерных обществах). Утверждение внутренних документов, регулирующих деятельность органов управления и контроля организации, Закон отнес к компетенции общего собрания акционеров (подп. 19 п. 1 ст. 48, п. 2 ст. 85 Закона об акционерных обществах). Совет директоров наделен правом утверждения внутренних документов, за исключением тех, утверждение которых отнесено Законом об акционерных обществах к компетенции общего собрания акционеров, а также иных внутренних документов общества, утверждение которых отнесено уставом общества к компетенции исполнительных органов (подп. 13 п. 1 ст. 65 Закона об акционерных обществах).

Важнейшим требованием к локальному нормотворчеству является безусловное соответствие принимаемых в его рамках внутренних нормативных документов общим принципам и конкретным предписаниям действующего законодательства.

По этой причине формирование системы локальных нормативных актов банка следует начинать с разработки и принятия Положения о локальных нормативных актах. Указанный документ должен служить инструментом реализации указанных выше требований путем установления основанного на принципах российского законодательства единого порядка создания, основных требований к форме и содержанию локальных актов и процедуре их принятия в акционерном обществе (банке). Положение утверждается советом директоров банка.

Типовая структура Положения включает в себя:

1. Общие положения.
2. Виды локальных нормативных актов, принимаемых банком.
3. Порядок разработки локальных нормативных актов.
4. Порядок принятия локальных нормативных актов.
5. Порядок изменения и отмены локальных нормативных актов.
6. Ввод в действие локальных нормативных актов.

В настоящее время банки сформировали собственную внутреннюю систему норм, обеспечивающих механизм исполнения общих принципов и положений правовых актов государства на уровне хозяйствующего субъекта. Наличие такой системы является важным элементом защиты безопасности банка.

---

[1] Приложение 2 к Положению Банка России от 16 декабря 2003 г. № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» — «Перечень основных вопросов, связанных с осуществлением внутреннего контроля, по которым кредитная организация должна принять внутренние документы».

ормативные требования локальных актов, направленные на защиту ег
опасности, обеспечиваются не только «внутренними» мерами воздействия
тдельных случаях их нарушение является основой для применения санк
со стороны государства в рамках Гражданского кодекса РФ и Уголовног
екса РФ. В частности, целям уголовно-правовой охраны порядка внутрен
отношений между банком и его служащим, установленного локальным
мативными актами, соответствует ст. 201 УК РФ (Злоупотребление полно
иями). Нарушение внутреннего порядка обращения со сведениями, со
зляющими коммерческую или банковскую тайну, может повлечь наказа
, предусмотренное ст. 139 ГК РФ (Служебная и коммерческая тайна) ил
83 УК РФ (Незаконные получение и разглашение сведений, составляю
к коммерческую, налоговую или банковскую тайну). С другой стороны, от
ствие внутренних нормативных актов, устанавливающих режим защит
фиденциальной информации, делает невозможной ее правовую защит
собственником, так и государством.

Предписания, имеющие опосредствованное отношение к обеспечени
опасности банка, содержатся в большинстве его локальных нормативны
ов, в первую очередь в тех, которые направлены на обеспечение порядк
функционирования:

- регламентирующих политику банка и технологию осуществления бан
  ковских операций;
- распределяющих функции и полномочия между подразделениями и со
  трудниками банка;
- определяющих процедуру принятия решений;
- регулирующих деятельность службы внутреннего контроля и т. д.

К числу локальных нормативных актов, регламентирующих деятельность
равленную исключительно на обеспечение безопасности банка, относятс
тренние документы, устанавливающие:

- внутриобъектовый режим кредитной организации;
- режим обеспечения зашиты сведений конфиденциального характер
  и компьютерной информации (перечень сведений, составляющих ком
  мерческую (банковскую) тайну, положение об организации защит
  конфиденциальной и компьютерной информации, инструкция о рас
  пределении доступа пользователей к конфиденциальной информации
  к осуществлению операций в программном обеспечении, а также к ба
  зам данных в компьютерных системах и т. д.);
- порядок организации и функционирования службы безопасности (уста
  службы безопасности либо положение о службе безопасности, инструк
  ция о проведении внутренних расследований по фактам нарушений по
  рядка обеспечения безопасности банка).

ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. Какие виды нормативных правовых актов (по степени юридической силы) регулируют отношения в сфере охраны и защиты банковского дела?
2. В чем заключается различие между нормативными правовыми актами общего действия и нормативными правовыми актами специального действия, регулирующими отношения в сфере обеспечения безопасности банков?
3. Какие отрасли законодательства содержат нормативные правовые акты общего действия, регулирующие отношения в сфере обеспечения безопасности банков?
4. Какие отрасли материального права содержат нормы, обеспечивающие безопасность банков методами охранительного содержания?
5. Какой законодательный акт предоставляет банку возможность пользоваться для обеспечения собственной безопасности услугами негосударственной организации?
6. Какие способы и формы обеспечения безопасности банка предусматривает банковское законодательство?
7. Назовите основные виды нормативных правовых актов Банка России.
8. Какие две основные группы нормативных актов Банка России регулируют отношения в сфере обеспечения безопасности банков?
9. Что собой представляет внутренний нормативный акт банка, каково его место в правовом регулировании?
10. Какие внутренние нормативные акты банк обязан принять в соответствии с требованиями законодательства?
11. Какими мерами принуждения обеспечиваются предписания внутренних нормативных актов банка?

Глава 3

ОРГАНИЗАЦИОННЫЕ ОСНОВЫ БЕЗОПАСНОСТИ БАНКА

- Организация системы безопасности банка
- Субъекты обеспечения безопасности банка
- Средства и методы обеспечения безопасности банка
- Организация внутреннего контроля банка
- Организация службы безопасности банка

3.1. Организация системы безопасности банка

Система безопасности банка представляет собой динамическую организа
о уполномоченных структур, реализующих своими силами и средствам
ы правового (нормативного), организационного, технического, сыскного
минералистического, криминологического характера, в целях защиты иму
ства, инфраструктуры и порядка функционирования кредитной организа
т от противоправных посягательств.

Такая система создается с учетом необходимости защиты банка от всех из
тных видов негативных воздействий и их отрицательных последствий. Глав
ми требованиями к системе безопасности являются ее надежность и эффек
ность, которые обеспечиваются соблюдением в процессе ее организаци
функционирования основополагающих принципов: законности; подкон
льности и подотчетности руководству банка; сочетания гласности и конфи
циальности; системности; полноты и всесторонности обеспечения защиты
имодействия; приоритета мер предупредительного характера; экономиче
й целесообразности; разграничения полномочий; развития и совершенст
ания.

На практике это означает следующее.

Процесс создания и функционирования системы осуществляется в строго
тветствии с положениями Конституции РФ, федеральных законов, акто
езидента РФ и Правительства РФ, нормативных правовых актов субъекто
дерации, а также нормативных актов ведомств и внутренних (локальных
рмативных актов банка.

Создание и функционирование системы финансируется банком. Руково
тели и сотрудники подразделений, входящих в состав системы безопасно
банка, полностью подотчетны руководству банка. Они принимаются н
боту, назначаются на должность, освобождаются от должности и увольня
ся с работы приказом руководителя банка. Основные задачи служб (а в не
ходимых случаях — текущие поручения) утверждаются руководителе
нка. О результатах своей деятельности структурные подразделения систе
безопасности отчитываются перед руководителем банка. Полученны
териал о фактах посягательства на инте есы банка используются

по усмотрению руководителя банка (за исключением случаев обязательного информирования правоохранительных органов, предусмотренных законодательством). Руководитель банка контролирует расходование денежных средств и материальных ресурсов, выделенных структурным подразделениям системы безопасности.

Ведущими структурными элементами системы безопасности банка являются его службы внутреннего контроля и собственной безопасности. Однако эффективность функционирования названных служб в значительной мере зависит от правильной организации их взаимодействия с иными структурными подразделениями банка, с подразделениями безопасности других хозяйствующих субъектов, с частными детективными и охранными структурами, а также с государственными органами, выполняющими контрольные, надзорные и правоохранительные функции.

Обязанности осуществления взаимодействия в интересах обеспечения безопасности банка возлагаются на руководителей служб внутреннего контроля, безопасности и других структурных подразделений, а также на отдельных сотрудников банка. Эти обязанности устанавливаются актами законодательства, ведомственными и локальными нормативными актами, формулируются в виде пунктов соответствующих договоров и соглашений между банком и другими организациями (государственными и негосударственными).

Так, Положение Банка России № 242-П содержит специальные предписания, посвященные обязанностям сотрудников подразделений банка по взаимодействию со службой внутреннего контроля. Так, в соответствии с п. 3 Приложения 1 кредитная организация должна установить порядок, при котором служащие доводят до сведения органов управления и руководителей структурных подразделений кредитной организации (филиала) информацию обо всех нарушениях законодательства Российской Федерации, учредительных и внутренних документов, случаях злоупотреблений, несоблюдения норм профессиональной этики.

Аналогичные требования о взаимодействии сотрудников банка со службой внутреннего контроля содержатся в пп. 2.10.9, 2.10.10 и 2.10.12 Приложения 1 к Письму Банка России от 13 июля 2005 г. № 99-Т «О методических рекомендациях по разработке кредитными организациями правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Деятельность службы внутреннего контроля банка осуществляется гласно. Служба безопасности, наряду с гласными методами, применяет в необходимых случаях методы и средства негласного характера, не нарушающие конституционные права граждан и не требующие для их осуществления специальных полномочий (использует скрытые камеры наблюдения, скрытые методы защиты имущества и информации и т. д.).

Надежность обеспечения безопасности банка оценивается по степени уязвимости наиболее слабо защищенного элемента его имущества и инфраструктуры

щита банка осуществляется с использованием всего арсенала предусмотрен
х законодательством сил и средств, находящихся в его распоряжении.
Исходя из целей функционирования банка, основной задачей системы
юпасности является предотвращение угроз его деятельности. По этой при
не система безопасности ориентируется на приоритет мер предупредитель
го характера, на преимущественное применение таких средств и методов
горые позволяют воспрепятствовать преступным намерениям субъектов по
ательства или пресечь их на начальной стадии.
Функционирование системы безопасности связано с определенными рас
ами, границы которых определяются рядом факторов, в числе которы
ервую очередь учитывается экономическая целесообразность. Речь иде
ом, что затраты на обеспечение безопасности банка должны оцениватьс
очки зрения их сопоставимости с возможным ущербом от реализации по
циальных угроз. Расходы на создание и функционирование системы безо
ности в целом не должны превышать размер возможного ущерба. При
п экономической целесообразности следует учитывать и в частных случаях
пример, при выборе средств и методов противодействия определенным ви
и угроз.
Общее руководство построением системы безопасности банка и ответствен
сть за ее функционирование возлагаются на руководителей банка и назван
х выше служб. Разработанная система мер безопасности реализуется сотруд
ками служб внутреннего контроля и безопасности в рамках их функционал
их обязанностей. Однако для выполнения некоторых видов лицензируемы
бот в области защиты имущества и информации банка привлекаются на до
зорной основе организации, имеющие соответствующие лицензии.
Система безопасности банка создается, развивается и совершенствуетс
основе использования средств и методов, разработанных современной нау
й, рекомендаций по их наиболее эффективному применению, с учето
ыта борьбы с преступностью в банковской сфере отечественных и зарубеж
их правоохранительных структур и негосударственных служб, а также обоб
ения и анализа собственного опыта.
Созданию системы предшествует разработка документально оформленно
оекта, составными частями которого является концепция безопасност
нка и пакет внутренних документов банка нормативного, организационно
етодического характера.
Концепция безопасности банка содержит подробное и обоснованное опи
ние подлежащих защите объектов; описание всех видов потенциальных уг
з и их отрицательных последствий; программу разработки адекватных ме
щиты (выявления, предупреждения, пресечения угроз). Наличие концепци
легчает процесс анализа, оценки полноты и всесторонности принятых ме
щиты, способствует целенаправленному установлению слабых мест систем
зопасности, выявлению и классификации причин и условий, способство
вших совершению посягательств на интересы банка.

Пакет внутренних документов банка содержит нормативные предписания, организационные распоряжения и методические рекомендации, имеющие целью обеспечение надежного и эффективного функционирования структурных элементов системы защиты.

3.2. Субъекты обеспечения безопасности банка

Субъектами обеспечения банковской безопасности являются: государство, Банк России, правоохранительные органы (милиция и др.), прокуратура, органы судебной власти, акционерный коммерческий банк (в целом), отдельные структурные подразделения банка (служба внутреннего контроля, служба безопасности), юридические и физические лица, вступающие с банком в договорные отношения.

В процессе обеспечения безопасности банка государство выступает как гарант защиты его исключительного права на занятие банковской деятельностью (аналогичная деятельность других субъектов признается незаконной), а также его имущества и инфраструктуры. Оно осуществляет свою функцию через государственные органы законодательной, исполнительной и судебной власти путем:

- установления уголовной и иной ответственности за противоправные посягательства на интересы банка;
- выявления, предупреждения, пресечения, расследования преступлений и иных правонарушений, наказания виновных и возмещения ущерба;
- осуществления государственного контроля и надзора за выполнением банком установленных законодательством требований безопасности.

Банк России участвует в обеспечении безопасности кредитных организаций путем применения методов регулирования и надзора за их деятельностью. Он осуществляет разрешительные, надзорные, контрольные и административные функции в отношении кредитных организаций для поддержания стабильности банковской системы, защиты интересов вкладчиков и кредиторов.

Формы участия правоохранительных органов (в частности, милиции) в обеспечении безопасности банковской деятельности определяются их принадлежностью к числу государственных органов исполнительной власти, основной функцией которых является охрана законности и правопорядка.

Указанную функцию они реализуют путем предотвращения, выявления, пресечения и расследования преступлений и административных правонарушений, посягающих на безопасность банка.

Прокуратура, как субъект обеспечения безопасности в сфере банковской деятельности, реализует свои функции путем надзора за соблюдением законности, а также уголовного преследования лиц, совершающих преступления в банковской сфере. Для выполнения этих функций прокуратура проводит прокурорские проверки исполнения законов, осуществляет предварительное

следование преступных посягательств на интересы банка. В случ
лости прокурор на основании ст. 28.4. КоАП РФ вправе также
о об административном правонарушении и провести админи
следование.

Органы судебной власти осуществляют правосудие по уголовн
елам об административных правонарушениях, связанных с посяг
на безопасность банка. Их решения в сфере защиты интересов
явлены на наказание виновных и возмещение ущерба, причине
ству и инфраструктуре кредитной организации.
Акционерный коммерческий банк выполняет законодательно
е обязанности обеспечения собственной безопасности путем за
ства и инфраструктуры. Для выполнения этих функций он прим
а и методы правового, организационного, технического, сыск
налистического характера.

Служба внутреннего контроля банка представляет собой об
уктурное подразделение кредитной организации, без создани
ик не может получить государственную регистрацию. Она участ
ении безопасности банка путем разработки мер предупреждения
я действий и решений персонала, содержащих потенциальный
причинения вреда имуществу и порядку функционирования ба

Служба безопасности банка является учрежденным по иници
дства банка охранно-сыскным предприятием. В отличие от сл
него контроля, ее создание для банка не обусловлено обязател
гивными предписаниями. Основной задачей службы является з
енности и инфраструктуры банка от противоправных посягате
полнения своих функций служба применяет средства и методы
ганизационного, технического, сыскного, охранного и криминал
характера.

Юридические и физические лица, вступающие с банком в дого
шения, участвуют в защите имущества и инфраструктуры банка
язательств, принятых на себя по соответствующим договорам.

3.3. Средства и методы обеспечения безопасности банка

Под методом принято понимать способ осуществления определе
ьности в виде последовательных действий, выполняемых на ос
нтролируемого плана. Методы обеспечения безопасности банка в
в зависимости от специфики подлежащих решению задач и от
и участвующих субъектов. В свою очередь выбор средств обеспеч
ности банка, т. е. приемов или специальных орудий предопредел
, в рамках которых их планируется использовать.
В соответствии с логикой обеспечения банковской безопасност
методы могут быть сведены в две
имую

группы. В первую из них входят методы законодательного и нормативного
правового регулирования (описанные во второй главе настоящей работы).
Вторую группу составляют методы реализации законодательных и иных нор-
мативных правовых предписаний.

Целью данного параграфа является рассмотрение методов и средств реали-
зации правовых и иных нормативных предписаний, которые применяются
кредитными банками и их подразделениями. Поскольку методы и средст-
ва, применяемые другими субъектами (органами государственной власти
Российской России), широко освещены в специальной литературе, они будут
рассматриваться лишь в той мере, в которой деятельность этих субъектов в сфере
обеспечения банковской безопасности соприкасается с деятельностью банка
и его подразделений.

При реализации банком законодательных и иных нормативных предпи-
саний в области обеспечения безопасности выполняются посредством приме-
нения системы методов, среди которых принято выделять:

организационные;
технологические;
защиты конфиденциальной информации;
административного контроля;
финансового контроля;
режимной и охранной деятельности;
криминалистики.

Каждый из названных методов может быть разделен на составляющие его
по непосредственной сфере применения, применяющим его подраз-
делениям и другим основаниям.

Организационные методы обеспечения безопасности включают в себя
общие методы осуществления производственной, управленческой, фи-
нансовой, коммерческой, кадровой и иной функциональной деятельности
банка, имеющие целью предупредить причинение ущерба как в результате
преднамеренных действий, так и вследствие ошибки. В рамках организационных
методов формируются специальные подразделения защиты интересов банка;
осуществляется совершенствование структуры руководящих и контролирующих
органов; принимаются решения об ограничении и разграничении полномо-
чий должностных лиц в отношении объема и состава банковских операций,
распоряжении денежными средствами и иным имуществом банка; разгранi-
чиваются полномочия операционистов и кассиров при осуществлении расчет-
ных операций; устанавливается индивидуальная ответственность кон-
кретных лиц за обеспечение процедур выполнения отдельных операций и по-
хранения ценностей; организуется система отчетности банка и система
работы с персоналом.

Субъектом применения указанных методов является банк в лице руководя-
щих органов, наделенных

ствами реализации указанных методов являются организационные реше
ı, закрепленные в форме распорядительных документов банка.

рамках технологических методов разрабатываются безопасные технол
банковских операций, не позволяющих преступникам использовать из
тные практике способы совершения преступлений. В их число входят тех
югии открытия счетов, заключения договоров, кассового обслуживани
ıентов банка, работы пунктов обмена валюты, оформления, выдачи и опла
ценных бумаг и т. д.

Профилактический эффект методов технологического характера долже
ючаться, с одной стороны, в продуманной последовательности и способа
юлнения соответствующих операций, а с другой — в установлении запре
их нарушение. Вследствие этого противоправные действия (и в ряде случа
даже подготовка к ним) приобретают характер грубого нарушения устано
ного порядка конкретным лицом. Скрыть такое нарушение практичес
юзможно, и процесс его обнаружения при надлежащей организации раб
занимает очень незначительный промежуток времени.

Технологические методы обеспечения безопасности банка основываются н
тветствующих рекомендациях Банка России, разработках собственны
разделений банка, на научных и практических рекомендациях специали
в в области борьбы с преступлениями в финансовой сфере (например
фере вексельного обращения). Реализуются указанные методы руководя
ми органами банка, а также его структурными подразделениями в рамка
тветствующих направлений банковской деятельности. Средствами их ре
ации являются технологические решения, закрепленные распорядител
ми документами.

Методы защиты конфиденциальной информации призваны обеспечить вы
нение требований ст. 26 (Банковская тайна) Закона о банковской деятел
сти, ст. 857 (Банковская тайна) ГК РФ, п. 2 ст. 7 Закона о противодействи
ализации преступных доходов (порядок обеспечения конфиденциальн
информации), а также других законодательных актов, предписывающи
ку хранить в тайне иные виды конфиденциальной информации (в част
сти, коммерческую и налоговую тайну, персональные данные сотрудник
р.).

Методы защиты конфиденциальной информации весьма многообразн
хватывают широкий спектр действий организационного, программно-а
ратного и контрольного (проверочного) характера. В целом они могут бы
дены в четыре основных группы, каждая из которых нацелена на решени
носительно самостоятельных задач:

1) закрытие свободного доступа к сведениям конфиденциального харак
а;

2) выявление, предупреждение и пресечение попыток неправомерного з
дения сведениями и документами конфиденциального характера;

3) организация защиты конфиденциальной информации, обрабатываемой средствами вычислительной техники, от несанкционированного доступа;

4) организация защиты конфиденциальной информации от утечки по техническим каналам.

Каждая из названных групп включает в себя ряд самостоятельных методов, рассмотрение которых выходит за рамки настоящего параграфа.

Средствами реализации методов защиты конфиденциальной информации служат нормативные правовые документы предписывающего, рекомендательного и запретительного характера, а также специальные компьютерные программы и устройства.

Субъектом применения методов и средств защиты информации являются специальные подразделения защиты информации банка. Контроль за обеспечением мер защиты информации с ограниченным доступом в негосударственных структурах осуществляется органами государственной власти.

Методы административного контроля в сфере обеспечения безопасности банка имеют целью проверку наличия и правильного функционирования системы подбора и расстановки кадров; проверку содержания заключенных с работниками трудовых соглашений (контрактов), проверку наличия инструкций, регламентирующих должностные обязанности сотрудников.

Кроме того, административными методами обеспечивается проведение операций только уполномоченными на то лицами и в строгом соответствии с определенными банком полномочиями и процедурами принятия решений по проведению операций.

Методы финансового контроля призваны обеспечить проведение операций в строгом соответствии с принятой и закрепленной документами политикой банка применительно к разным видам финансовых услуг и их адекватного отражения в учете и отчетности.

Финансовый контроль должен с достаточной степенью надежности обеспечить фиксацию операций в соответствии с установленными требованиями, реальное отражение состояния активов и пассивов банка и обеспечение составления предусмотренных форм отчетности; ведение финансовых документов с достаточной полнотой, их соответствие фактическим обстоятельствам и осуществление проверок с установленной периодичностью.

Субъектом реализации методов административного и финансового контроля является Служба внутреннего контроля банка. Средствами административного и финансового контроля являются: формальная и фактическая проверки; подтверждение; обследование; опрос; аналитические тесты; логическая и арифметическая проверки.

Методы и средства сыскной и охранной деятельности регламентированы Законом о частной детективной деятельности.

Методы сыска применяются в целях сбора сведений по гражданским делам; изучения рынка, сбора информации для деловых переговоров, выявления некредитоспособных или ненадежных деловых партнеров; установления

стоятельств недобросовестной конкуренции, а также разглашения сведе
й, составляющих коммерческую тайну; выяснения биографических и дру
х характеризующих личность данных об отдельных гражданах (с их пись
ного согласия) при заключении ими трудовых и иных контрактов; поиск
ыченного имущества; сбора сведений по уголовным делам.

Реализация методов охраны осуществляется в целях защиты жизни и здоро
сотрудников банка; охраны имущества; проектирования, монтажа и экс
атационного обслуживания средств охранной и пожарной сигнализации.

Законодательно установленными методами сыскной деятельности являются
ный опрос граждан и должностных лиц (с их согласия); наведение справок
чение предметов и документов (с письменного согласия их владельцев)
ешний осмотр строений, помещений и других объектов; наблюдение дл
лучения необходимой информации.

Закон о частной детективной деятельности допускает применение в рамка
занных методов видео- и аудиозаписи, кино- и фотосъемки, технически
ных средств, не причиняющих вреда жизни и здоровью граждан и окружаю
й среде, а также средств оперативной радио- и телефонной связи. В случа
сопряженных с опасностью для жизни и здоровья, лицам, осуществляю
м сыск и охрану, разрешается использование специальных средств и огне
ельного оружия.

Субъектом применения методов и средств сыскной и охранной деятельно
является Служба безопасности банка.

Несмотря на то, что *методы и средства криминалистики* исторически разра
ывались исключительно в целях обеспечения профессиональной деятельно
специальных субъектов — сотрудников правоохранительных, прокурор
х, судебных органов и экспертных организаций, — в настоящее время он
роко используются службами безопасности банков. Это объясняется не
лькими обстоятельствами. Во-первых, отсутствием неких других «специ
но детективных» средств и методов, способных заменить криминалистиче
е в сфере обеспечения банковской безопасности. Во-вторых, отсутствие
онодательных ограничений на использование криминалистических средст
етодов (в отличие от содержащегося в Федеральном законе от 12 августа
5 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (в ред. от 29 ап
я 2008 г. № 58-ФЗ) (далее — Закон об оперативно-розыскной деятельно
), запрета на осуществление оперативно-розыскных действий, отнесен
к исключительной компетенции органов дознания). В-третьих, сотруд
и службы безопасности банка, имея по условиям лицензирования и
тельности соответствующие знания и навыки (юридическое образование
циальную подготовку для работы в качестве частного сыщика, а также
к работы в оперативных или следственных подразделениях), достаточно
готовлены для применения указанных средств и методов в процессе сво
еятельности.

По служебной роли в обеспечении банковской безопасности криминалистические методы и средства делятся на:

- устанавливающие причины и условия, способствовавшие совершению или сокрытию преступлений;
- способствующие для получения информации о готовящихся преступлениях;
- защищающие имущество банка от преступных посягательств и создающие благоприятные условия для возникновения доказательственной информации.

По источнику происхождения применяемые в указанных случаях методы и средства разграничиваются на три основные криминалистические группы:

а) техника;
б) тактика;
в) методика.

Средства предупреждения преступлений, разработанные в рамках раздела «криминалистическая техника», являются наиболее распространенным видом технико-криминалистических средств, используемых специальными подразделениями банка в целях обеспечения его безопасности. По непосредственному целевому назначению эти средства делятся на такие, применение которых:

а) затрудняет или исключает возможность совершения преступного посягательства;

б) создает благоприятные условия для возникновения доказательственной информации.

В рамках первой из названных групп банки широко применяют охранную сигнализацию, запирающие устройства, устройства технической защиты компьютерных сетей от неправомерного доступа, программные средства защиты компьютерных сетей банка и циркулирующей в них информации.

В рамках второй группы средств используются технологические видеокамеры, позволяющие фиксировать действия преступника на месте преступления; специальные ловушки, оставляющие на преступнике следы стойкой краски при попытке совершить преступление (например, взлом банкомата); компьютерные программы, фиксирующие попытку незаконного проникновения в компьютерную сеть, адрес периферийного устройства, с которого такая попытка предпринималась, и характерные признаки, присущие субъекту посягательства.

Рекомендации и приемы, разработанные в рамках раздела «криминалистическая тактика», используются для построения системы собственной безопасности банка, организации ее функционирования и контроля над ее надежностью.

В первую очередь речь идет о *планировании* мероприятий по выявлению причин и условий, способствующих совершению преступлений на основе фактических данных. Тактические рекомендации о порядке проведения и оценки результатов *следственного эксперимента* используются для осуществления

дного непроцессуального действия, нацеленного на проверку надежност
защиты банка на конкретном участке его деятельности. Этот прием пе
дически применяется, в частности, для проверки надежности системы за
ы компьютерных сетей банка и содержащейся в них информации. Пр
проведении проверяющие, с санкции руководства банка, организуют по
ки контролируемого «взлома» системы защиты с использованием послед
«достижений» в области программирования и дешифрования, в том числ
менявшихся преступниками.

Кроме того, при построении системы безопасности банка важную роль иг
г использование такого тактического приема, как *построение версии* о ви
и характере потенциальных угроз и способах защиты от них.

Рекомендации, разработанные на основе криминалистической методики, ис
ьзуются для создания методик внутреннего расследования и предотвраще
отдельных видов преступлений.

Система средств и методов криминалистики, применяемых для обеспече
безопасности банка, предполагает возможность дальнейшего структури
ания по мере появления практических потребностей. Основаниями дл
ее детальной классификации средств и методов защиты могут быть избра
объекты структуры банка, виды угроз и другие объекты системы банков
й защиты.

Субъектом применения методов и средств криминалистики в коммерче
м банке является в основном служба безопасности кредитной организа
. Не исключается, однако, что названные методы и средства могут исполь
ить при необходимости служба внутреннего контроля и служба защиты ин
мации банка.

3.4. Организация внутреннего контроля банка

Система внутреннего контроля банка — важный инструмент обеспечения
ежного функционирования кредитной организации, назначение которого
ючается в установлении режима безусловного исполнения работниками
ка законодательных и иных нормативных требований, направленных
беспечение банковской безопасности.

Подразделение (служба) внутреннего контроля банка создается в соответ
ии с требованиями ст. 24 Закона о банковской деятельности. Создание
й структуры в соответствии со ст. 12 Закона о банковской деятельности яв
ется обязательным условием государственной регистрации кредитной орга
ации и выдачи ей лицензии на осуществление банковских операций. Не
людение же требований к порядку комплектования и функционирования
разделения внутреннего контроля служит основанием для отказа в госу
ственной регистрации кредитной организации и выдачи лицензии на осу
твление банковских операций (ст. 16 Закона о банковской деятельности),

либо для отзыва названной лицензии (ст. 20 Закона о банковской деятельности).

Еще одним актом федерального законодательства, устанавливающим обязанность кредитной организации создать службу внутреннего контроля, является Закон о противодействии легализации преступных доходов. Пункт 2 ст. 7 Закона о противодействии легализации преступных доходов дополняет ранее зафиксированные обязанности службы внутреннего контроля специальной задачей: противодействием конкретному виду преступной деятельности — легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Порядок организации и функционирования служб внутреннего контроля банка детально регламентирован Положением Банка России № 242-П. Дополнительной нормативной регламентации со стороны Банка России подверглись такие направления внутреннего контроля, как деятельность кредитной организации на финансовых рынках и в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем (Письмо Банка России от 13 июля 2005 г. № 99-Т «О методических рекомендациях по разработке кредитными организациями правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»).

Служба внутреннего контроля организуется органами управления банка, уполномоченными на это учредительными документами кредитной организации. Ее создание начинается с внесения соответствующего раздела в Устав банка и принятия Положения о службе внутреннего контроля, которым регламентируются цели и задачи службы, организация ее деятельности, требования к руководителю и сотрудникам, их права и обязанности. Это Положение разрабатывается в соответствии с названными выше нормативными предписаниями Банка России и утверждается советом директоров банка.

Руководитель службы внутреннего контроля назначается на должность и освобождается от должности органом управления банка. Это должно обеспечить независимость службы от исполнительного органа банка при выполнении функций внутреннего контроля.

Согласно предписаниям Банка России, руководитель Службы и его заместители должны иметь высокий уровень профессиональной подготовки, обладать опытом руководства структурным подразделением кредитной организации, связанным с совершением банковских операций и других сделок.

Дополнительные квалификационные требования к отдельным категориям работников службы внутреннего контроля сформулированы в Указании Банка России от 9 августа 2004 г. № 1486-У «О квалификационных требованиях к специальным должностным лицам, ответственным за соблюдение правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма и программ его осуществления в кредитных организациях».

Согласно этим требованиям ответственный сотрудник структурного под деления по противодействию легализации (отмыванию) доходов, получен к преступным путем, и финансированию терроризма (далее — структурно разделение) должен иметь высшее юридическое или экономическое обра ание и опыт руководства отделом, иным подразделением кредитной орга ации, связанным с осуществлением банковских операций, не менее одного а, а при отсутствии указанного образования — опыт работы в сфере проти ействия легализации (отмыванию) доходов, полученных преступным пу , и финансированию терроризма не менее двух лет или опыт руководств разделением кредитной организации, связанным с осуществлением бан ских операций, не менее двух лет.

Сотрудники структурного подразделения должны иметь высшее образова и опыт работы в подразделении кредитной организации, связанном с осу твлением банковских операций, не менее шести месяцев, а при отсутстви шего образования — опыт работы в сфере противодействия легализаци ыванию) доходов, полученных преступным путем, и финансировани роризма не менее одного года или опыт работы в подразделении кредит организации, связанном с осуществлением банковских операций, не ме одного года.

Ответственный сотрудник и сотрудники структурного подразделения счи тся не соответствующими квалификационным требованиям при наличии:

- судимости за совершение из корыстных побуждений преступлени в сфере экономики;
- административного правонарушения в области финансов, налогов и сбо ров, рынка ценных бумаг, а также в области государственного надзор (контроля) за выполнением законодательства в банковской сфере;
- фактов расторжения трудового договора по инициативе работодателя в соответствии с п. 7 ст. 81 ТК РФ, в течение двух лет, предшествующих дню назначения на соответствующую должность.

Основные цели создания и функционирования Службы заключаются в обес ении:

- сохранности активов (имущества) банка и достижения им уставных це лей;
- порядка функционирования банка, установленного для его сотрудников федеральными законами, постановлениями Правительства РФ, указа ниями Банка России и иными регулятивными требованиями, а также стандартами деятельности и нормами профессиональной этики, внут ренними документами, определяющими политику и регулирующими деятельность банка;
- контроля за деятельностью персонала банка, направленной на своевре менное обнаружение (идентификацию), оценку и принятие мер по ми нимизации рисков (в том числе возникающих в результате действий противоправного характера);
- противодействия банка легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Основные направления деятельности службы внутреннего контроля включа ют в себя:

- контроль за соблюдением установленных процедур и полномочий при принятии любых решений, затрагивающих интересы банка, его собственников и клиентов;
- обеспечение принятия руководством банка своевременных и эффективных решений, направленных на устранение выявленных недостатков и нарушений в деятельности банка;
- обеспечение выполнения персоналом требований по эффективному управлению рисками банковской деятельности;
- осуществление контроля за эффективностью применения процедур защиты конфиденциальной банковской информации, за доступом работников к имеющейся в банке информации в зависимости от их компетенции;
- разработку системы мер противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также организацию ее функционирования;
- организацию взаимодействия со структурными подразделениями банка в целях защиты от противоправных посягательств на интересы банка.

Указанные цели и направления деятельности Службы реализуются осуществлением контроля над:

- организацией деятельности кредитной организации;
- функционированием системы управления банковскими рисками и оценка банковских рисков;
- распределением полномочий при совершении банковских операций и других сделок;
- управлением информационными потоками (получением и передачей информации) и обеспечением информационной безопасности;
- функционированием системы внутреннего контроля в целях оценки степени ее соответствия задачам деятельности кредитной организации;
- организацией выявления недостатков, разработки предложений и реализацией решений по совершенствованию системы внутреннего контроля кредитной организации.

О результатах своей деятельности служба внутреннего контроля отчитывается перед органами управления банка на основании и в порядке, установленном положением банка о службе внутреннего контроля.

3.5. Организация службы безопасности банка

Непосредственной правовой основой возникновения и функционирования служб безопасности банка является Закон о частной детективной

ительности, однако в широком понимании проблемы источниками право-
о регулирования деятельности служб служит ряд других законов и отрасле-
ва, а также нормативные правовые акты ведомств и Банка России.
В первую очередь, это Конституция РФ, гарантирующая зашиту частно-
ственности; Закон о банковской деятельности, открывший возможност-
явления коммерческих банков; нормы Уголовного кодекса РФ, устанавли-
ющие уголовную ответственность за деяния, с которыми призвана бороться
жба безопасности; нормы Уголовно-процессуального кодекса РФ, регла-
тирующие порядок использования в уголовном судопроизводстве данных
ученных службой безопасности; положения Гражданского кодекса РФ
рудового права, устанавливающие порядок и процедуры использования ма-
иалов, добытых службой безопасности.
Нормативные акты, регламентирующие порядок организации и функцио-
ювания службы безопасности банка, могут иметь в своей основе один
двух видов законодательства. В тех случаях, когда в деятельности службы
опасности предполагается использовать средства и методы частной сыска
и охранной деятельности, она учреждается на основании Закона о част-
детективной деятельности. Право на осуществление указанной деятель-
ти у службы безопасности возникает после получения ее руководителем
отрудниками лицензии частного детектива в соответствии с положениями
4, 6, 11 и 12 Закона о частной детективной деятельности.
Внутренним нормативным актом, регламентирующим деятельность служ-
безопасности, является ее устав, утвержденный руководителем юридиче-
го лица и согласованный с органом внутренних дел по месту учреждения
жбы (ст. 14 Закона о частной детективной деятельности и п. 20. Инструк-
«Об организации работы по лицензированию и осуществлению органами
тренних дел контроля за частной детективной и охранной деятельностью
ерритории Российской Федерации», утвержденной приказом МВД России
9 июня 2006 г. № 4471).
Для осуществления процедуры согласования устава руководитель службы
опасности юридического лица представляет в уполномоченное подразделе-
органа внутренних дел заявление с приложением подлинника и копии ус-
, утвержденного руководителем юридического лица, а также документы
атериалы, установленные законодательными и иными нормативными пра-
ыми актами Российской Федерации.
Обязательные требования к сотрудникам службы безопасности, использую-
средства и методы сыскной и охранной деятельности, установлены на-
ной выше Инструкцией. В соответствии с этим документом руководитель
трудники службы безопасности обязаны:

получить (иметь) лицензию (разрешение органов внутренних дел) для утверждения в должности руководителя или сотрудника службы безопасности;

- быть пригодными по состоянию здоровья заниматься сыскной или охранной деятельностью;
- иметь гражданство России, юридическое образование, специальную подготовку для работы в качестве частного детектива либо стаж работы в оперативных или следственных подразделениях не менее трех лет (для сотрудников, выполняющих функции охраны, наличие юридического образования не обязательно).

В структуре банка служба безопасности представлена в качестве обособленного подразделения (с правом открытия текущих и расчетных счетов) для осуществления охранно-сыскной деятельности в интересах собственной безопасности учредителя.

Если же банк не намерен использовать в деятельности службы безопасности специфические детективные и охранные средства и методы (планирует, например, обойтись методами анализа открытой информации), она создается в качестве одного из структурных подразделений в порядке, предусмотренном Гражданским кодексом РФ и Законом об акционерных обществах. Правовым основанием для функционирования службы в таких случаях является Положение о структурном подразделении банка (службе безопасности, службе защиты интересов). Названный документ утверждается советом директоров или исполнительным органом банка в зависимости от полномочий, зафиксированных в Уставе (п. 13 ст. 65 Закона об акционерных обществах).

В последнем случае служба безопасности организуется органами управления банка, уполномоченными учредительными документами кредитной организации. Ее создание начинается с внесения соответствующего раздела в устав банка и разработки и принятия внутреннего нормативного акта — устава (положения) о службе безопасности банка, которым регламентируются цели и задачи службы, организация ее деятельности, требования к руководителю и сотрудникам, их права и обязанности. Положение о службе безопасности банка утверждается советом директоров банка. Руководитель службы безопасности назначается и освобождается от должности органом управления банка.

Штатный состав службы безопасности комплектуется на основе заключения трудовых договоров с лицами, способными по своим личным и деловым качествам, образованию, профессиональным навыкам и состоянию здоровья выполнять возложенные на них обязанности. Квалификационные требования к руководителю подразделения и его сотрудников разрабатываются и принимаются самим банком.

Наряду со штатными подразделениями банк может создавать нештатные структуры службы безопасности в виде временных или постоянных комиссий из сотрудников других структурных подразделений, выполняющих экспертные и контрольно-ревизионные функции (комиссии по защите банковской тайны, по проверке конфиденциального делопроизводства, по проведению внутреннего (служебного) расследования нарушения требований банковской

зопасности и др.). Деятельность внештатных структур службы безопасности относится к числу лицензированных.

Детальное нормативное регулирование целей и задач деятельности службы зопасности, порядка и форм ее выполнения с учетом особенностей банковой сферы осуществляется путем принятия внутренних (локальных) нормативных актов банка (специальных инструкций, других нормативных документов), которые разрабатываются банком в соответствии с законодательством. дготовленные документы должны фиксировать следующие обязательные ложения.

Основные цели службы безопасности заключаются в обеспечении безопас сти имущества и инфраструктуры банка от противоправных посягательств необоснованных притязаний в гражданско-правовой сфере.

Основными направлениями деятельности службы безопасности[1] являются:

- обеспечение безопасности банковских операций;
- обеспечение охраны имущества (включая деньги и приравненные к ним ценности), зданий, помещений, оборудования, технических средств обеспечения банковской деятельности;
- защита информации (банковской, коммерческой, налоговой тайны, иных сведений конфиденциального характера, компьютерной информации) и информационной инфраструктуры;
- защита системы кадрового обеспечения банка;
- обеспечение личной безопасности руководства банка;
- организация взаимодействия с правоохранительными органами в сфере обеспечения банковской безопасности;
- разработка и реализация мер профилактики противоправных посягательств на интересы банка.

Основные функциональные обязанности службы безопасности включают бя:

1) осуществление сыскной деятельности в целях:
   - оценки надежности и кредитоспособности предполагаемых клиентов, выявления в их действиях признаков противоправных посягательств на интересы банка при подготовке и совершении банковских операций, принятия мер по предупреждению готовящихся противоправных посягательств либо к возмещению причиненного ими вреда (в случае совершения);
   - выявления, предупреждения и пресечения преступных посягательств на безопасность банковских операций, на имущество и инфраструктуру банка (включая конфиденциальную и компьютерную информацию, систему кадрового обеспечения) со стороны лиц, не являющихся клиентами банка;

[1] Здесь и далее речь идет о службах безопасности, имеющих право осуществления частной тивной и охранной деятельности.

   - подготовки полученных материалов о готовящихся или совершенных противоправных посягательствах к направлению в правоохранительные органы для решения вопроса о возбуждении уголовного дела в соответствии со ст. 140 УПК РФ;
   - участия в расследовании по возбужденным уголовным делам на основании п. 7 ст. 3 Закона о частной детективной и охранной деятельности;
   - направления правоохранительным органам в соответствии со ст. 74 УПК РФ информации, могущей иметь отношение к расследованию по возбужденным уголовным делам;
   - розыска лиц, совершивших посягательства на интересы банка или подозреваемых в их совершении, а также принятия в пределах своей компетенции мер по возмещению нанесенного банку ущерба;
   - выяснения биографических и других характеризующих данных в отношении лиц, заключающих трудовой договор с банком или оформляющих допуск к работе с денежными средствами (их эквивалентами) и охраняемой информацией;
   - выявления в действиях сотрудников банка фактов грубых нарушений порядка обеспечения безопасности банка (требований безопасности), установленного внутренними нормативными актами, подготовки предложений о наложении на этих лиц дисциплинарных взысканий (включая расторжение трудового договора);
2) осуществление охранной деятельности посредством:
   - организации и обеспечения пропускного и внутриобъектного режима в помещении банка;
   - организации оборудования здания и помещений банка средствами охранно-пожарной и тревожной сигнализации;
   - организации оборудования кассового узла банка согласно требованиям к его устройству и технической укрепленности;
   - организации и осуществления контроля за соблюдением режима ограничения доступа персонала в помещения, предназначенные для хранения и обработки денег и других ценностей, конфиденциальных документов, обработки, хранения и передачи компьютерной информации;
   - организации и осуществления охраны имущества банка в процессе инкассационных операций;
   - организации оборудования инкассаторского спецавтотранспорта средствами защиты и вооружения, необходимыми для обеспечения безопасности сотрудников инкассации и сохранности перевозимых ценностей;
3) обеспечение личной охраны руководства банка путем создания и организации функционирования систем:

- физической защиты руководства (далее — охраняемого) в местах его пребывания и на маршрутах перемещения;
- выявления признаков подготовки преступного посягательства;
- действий по предупреждению и пресечению преступных посягательств на жизнь, здоровье и имущество охраняемого;
- действий по обеспечению безопасности охраняемого в чрезвычайных ситуациях;
- локализации последствий посягательства, оказанию помощи охраняемому;

) осуществление деятельности по защите информации банка путем:

- закрытия свободного доступа к сведениям конфиденциального характера, составляющим банковскую, коммерческую, налоговую тайны и иным видам охраняемой информации и их защиты от посторонних,
- организации конфиденциального делопроизводства, исключающего несанкционированное получение сведений конфиденциального характера, а также свободный доступ посторонних к компьютерной информации и информационной инфраструктуре банка;
- организации работы по административной и инженерно-технической защите сведений конфиденциального характера, а также компьютерной информации и информационной структуры банка;
- выявления и перекрытия возможных каналов утечки сведений конфиденциального характера, циркулирующих в технических средствах и помещениях банка;

) осуществление деятельности нормативного характера в целях разработки принятия организационно-распорядительных документов, регламентирующих порядок создания и функционирования систем:

- собственной безопасности банка;
- защиты информации банка;
- пропускного и внутриобъектного режима банка;
- личной безопасности руководства банка;

) разработка и реализация мер предупреждения противоправных посягательств на интересы банка:

- изучение причин и условий, способствующих совершению противоправных посягательств в банковской сфере;
- выявление наиболее уязвимых объектов обеспечения безопасности банка, оценка степени их защищенности от угроз противоправного посягательства;
- разработка средств и методов повышения надежности защиты конкретных участков деятельности банка.

ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. Что представляет собой система безопасности банка?
2. Раскройте содержание основных принципов создания и деятельности системы безопасности банка.
3. Какие ведущие структурные элементы составляют систему безопасности банка?
4. Кто входит в круг субъектов, участвующих в обеспечении безопасности банка, какие формы и методы использует для этого каждый из них?
5. Перечислите методы, которыми банк реализует законодательные и иные нормативные предписания в области обеспечения безопасности, и сферы их применения.
6. Какие законодательные акты обязывают банк создать службу внутреннего контроля?
7. Какова правовая процедура организации банком службы внутреннего контроля?
8. Каковы основные цели и задачи службы внутреннего контроля банка?
9. Какие нормативные акты являются правовой основой создания и функционирования службы безопасности банка?
10. Каковы порядок учреждения службы безопасности и обязательные требования к ее сотрудникам?
11. Каковы основные направления деятельности службы безопасности?

Глава 4

ТЕХНИКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАНКА

- Система технических средств обеспечения безопасности банка
- Технические средства охраны
- Технические средства защиты банковских операций и продуктов
- Технико-криминалистические средства

4.1. Система технических средств обеспечения безопасности банка

Технические средства обеспечения безопасности современного банка пред
ляют собой совокупность (систему) взаимосвязанных друг с другом эле
тов. Задача этой системы состоит в создании единого, целостного фронт
вления, предупреждения и пресечения посягательств на интересы банк
ем использования возможностей инженерной защиты и специально при
собленных для этого средств техники. Главными ориентирами для по
ения системы являются:

) нормативные правовые предписания;

) особенности охраняемого объекта;

) специфика преступных посягательств, от которых должны защитит
ические средства.

Следует отметить, что правовое регулирование применения технических
ств безопасности банка распространяется лишь на отдельные сферы функ
нирования кредитных организаций, оставляя за собственником право само
тельно достраивать соответствующую систему защиты с учетом особенно
защищаемого объекта. Поэтому наряду с методологическими основами
овых предписаний при построении системы технических средств обеспе
ия безопасности банк использует накопленный опыт борьбы с преступны
посягательствами, а также рекомендации, разработанные в рамках крими
стики.

Прямые нормативные правовые предписания государства, регламентирую
организацию инженерно-технической защиты банка, касаются, в первую
едь, средств обеспечения безопасности специальных помещений банка
, расчетных узлов, обменных пунктов), а также информационных ресур
анка.

оложение Банка России № 199-П предписывает банку:

оснастить работников кассы техническими средствами и методиками для выявления неплатежных и поддельных денежных знаков;

оборудовать кассовый узел банка согласно требованиям к его устройству и технической укрепленности в целях обеспечения сохранности денег и других ценностей;

- соблюдать установленные требования к специальному оборудованию инкассаторского спецавтотранспорта, к средствам защиты и вооружения, необходимые для обеспечения безопасности сотрудников инкассации и сохранности перевозимых ценностей.

Заключение о готовности кредитной организации к проведению банковских операций, в том числе обеспеченности ее зданием (помещением), отвечающим требованиям по техническому оборудованию банковского помещения и укрепленности кассового узла, по результатам осмотра на месте выдает территориальное учреждение Банка России.

В случае привлечения милицейских подразделений МВД России для охраны коммерческих банков, филиалов, операционных касс вне кассовых узлов и обменных пунктов заключения по их оборудованию инженерно-техническими средствами охраны, кроме должностных лиц территориального учреждения Банка России, подписываются и представителями вневедомственной охраны.

Нормативное описание инженерно-технических средств охраны банков, охраняемых или подлежащих передаче под охрану подразделениям вневедомственной охраны, содержится в руководящем документе РД 78.36.003–2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств», утвержденном МВД России 6 ноября 2002 г. Названный документ включает в себя требования более пятидесяти ГОСТов, условий и рекомендаций, регламентирующих: требования к защитным качествам стен, дверей, запирающих устройств, сейфов и хранилищ ценностей, пулестойкого стекла, к защитным конструкциям для дверных и оконных проемов, к системам тревожной сигнализации, пожаротушения и пожарно-охранной сигнализации, а также к системам охранного телевидения, охранного освещения, к машинам, приборам, другим техническим изделиям и т. д.

Обязательный набор технических и программных средств защиты информации банка регламентирован Приказом Банка России от 31 января 1995 г. № 02–13 «О вводе в действие в системе Центрального банка Российской Федерации государственных стандартов Российской Федерации». Этот нормативный правовой акт посвящен техническим и программным средствам защиты информации, циркулирующей в системе Банка России и в коммерческих банках, находящихся с ним в информационном взаимодействии.

Система технических средств обеспечения безопасности банка включает в себя весьма широкий набор приспособлений. Однако в целом их можно разделить по функциональному назначению на три основных вида:

1) технические средства охраны имущества и персонала банка;

2) технические средства защиты банковских операций и инструментов, предназначенные для выявления и предупреждения преступных посягательств, совершаемых под видом банковских операций;

3) технико-криминалистические средства, предназначенные для поиск фиксации информации, имеющей значение для выявления, предотвраще и расследования преступных посягательств на интересы банка.

Предложенное выше разграничение в определенной мере условно, по-льку в реальной практике конкретный вид технических средств обеспече- безопасности может выполнять одновременно несколько функциональ- х задач. Так, например, технические средства обнаружения тревожных си- ций (видеокамеры) могут использоваться для фиксации информации ющей значение для расследования. Технические средства зашиты банков их операций и инструментов могут одновременно выполнять роль техни криминалистических средств. Тем не менее классификация технически дств по названным основаниям вполне оправдана в методологических це .

4.2. Технические средства охраны

Технические средства охраны банка применяются на трех основных на влениях обеспечения безопасности. Во-первых, они выполняют роль ме ического укрепления в целях защиты от преступного посягательств имущество, персонал и посетителей банка. Во-вторых, используются дл аружения несанкционированного проникновения на объект и завладени ществом банка. В-третьих, применяются для облегчения розыска преступ а и создания доказательственной информации в случае совершения пре ного посягательства.

К числу средств инженерно-технического укрепления банка относятся струкции по усилению металлической арматурой, стальными листами п. защитных свойств стен, перекрытий, перегородок зданий, технологиче к и специальных помещений (хранилищ), дверных и оконных проемов способления для механической защиты вентиляционных коробов, люков угих технологических каналов.

Составными элементами системы инженерно-технических средств являют спытанные по специальным методикам на устойчивость к взлому и пуле кость: защитные двери, зашитные многослойные стекла, падающие бро ованные жалюзи, люки, механические и электромеханические защитные струкции для дверных и оконных проемов, установки пожаротушения гнализации.

К указанной группе инженерно-технических средств, кроме того, относят проверенные по соответствующим методикам замки соответствующих сов защиты, а также испытанные на устойчивость к взлому и огнестой- ь сейфы, хранилища ценностей и защитные кабины.

По усмотрению банков в качестве технических средств защиты могут приме ся средства и системы контроля и управления доступом, которые обеспечи- возможность разграничения и контроля доступа персонала в помещения

с помощью идентификационных пластиковых карточек или других средств идентификации (в частности, на основе биометрических данных), учет рабочего времени и трудозатрат, а также запись сведений о передвижении сотрудников, и могут блокировать вход и выход из помещения в случае тревоги. Вход в банк может быть оборудован шлюзом безопасности (металлической кабиной с автоматическими системами сдвижных дверей из пулестойкого стекла), выполняющим функции защиты от несанкционированного проникновения, разделения людских потоков и обнаружения оружия.

Механическая защита информационных систем банка от доступа посторонних лиц, умышленного разрушения или повреждения, огня, противопожарной воды и считывания информации на расстоянии осуществляется путем оборудования специально защищенных помещений, использования сейфов для особо важных серверов, сейфов для магнитных архивов, а также защищенных компьютерных рабочих мест.

Применение средств технической (механической) защиты существенно снижает опасность насильственных посягательств на деньги и иное имущество банка, уменьшает вероятность реализации угроз жизни и здоровью персонала и посетителей, способствует предупреждению преступных посягательств на интересы банка в целом.

Так, например, в январе 2003 г. при совершении разбойного нападения на филиал Сбербанка в г. Иркутске бронестекло, которым в соответствии с установленными требованиями было оборудовано рабочее место кассира, спасло жизнь сотрудникам филиала и сберегло материальные ценности. Заметив, что кассир нажимала кнопку тревожной сигнализации, преступник дважды выстрелил в нее из пистолета Макарова, однако разрушить стеклянную перегородку не смог.

Для обнаружения несанкционированного проникновения на объект и завладения имуществом применяется система охранной сигнализации. Ее технические средства предназначены для своевременного обнаружения тревожных ситуаций и оповещения о них охраны. В число элементов системы охранной сигнализации входят телекамеры и иные элементы (датчики) для обнаружения изменений состояния среды и формирования сигнала извещения об этом (извещатели). Последние предназначены для передачи сигналов на пульт централизованного наблюдения и обеспечения процедур постановки и снятия объекта с охраны. Еще одним видом элементов охранной сигнализации являются оповещатели, предназначенные для подачи звуковых или световых сигналов тревоги персоналу службы охраны.

Современные системы контроля и управления средствами сигнализации управляются при помощи компьютера. Это дает возможность, используя телекамеры, получать на экране монитора в реальном времени планы охраняемых помещений, визуально оценивать данные о возникших тревожных ситуациях в них, а также вести электронный протокол наблюдений и сообщений.

По информации МВД, в последние 5 лет НИЦ «Охрана» Главного управле
я вневедомственной охраны (ГУВО) МВД России разработаны, внедрен
ерийное производство и рекомендованы к применению в кредитных учре
ениях 28 типов современных технических средств охранной сигнализации
которые из них формируют сигнал тревоги независимо от действий персо
ла. Необходимость в этом выявилась в 2002 г., когда в четырех из пяти слу
в нападений на пункты обмена валюты в Москве кнопка тревожной сигна
ации по причине стрессового состояния кассиров была нажата спуст
-30 минут после совершения преступления.

В число извещателей охранной сигнализации входят радиосистема дистан
онной беспроводной тревожной сигнализации РСТС «Радиокнопка», изве
гель «Шорох-2» для защиты банкоматов от вандализма и вскрытия сейф
звещатель ИО 102–31 для блокировки банкоматов на открывание и пере
шение.

Извещатель «Радиокнопка» выпускается в двух модификациях: в виде но
ого «радиобрелока», передающего тревожное сообщение при нажати
опки, и «радиокуклы» — имитации пачки банкнот, посылающей извещени
изменении ее местоположения[1].

Наиболее распространенными техническими средствами, которые приме
ются для розыска преступника и создания доказательственной информаци
учае совершения преступного посягательства на интересы банка, являют
системы телевизионного наблюдения и так называемые химические ло
ки.

Телевизионное наблюдение в целях обеспечения охраны банка ведется от
тыми и скрытыми телекамерами. Последние размещаются в местах наибо
вероятной угрозы со стороны преступников: на улице перед банком
иентском зале, в хранилище ценностей, в местах установки банкоматов
жение ведется в автоматическом и управляемом режиме с пульта наблюде
. Изображение записывается на стандартную видеокассету и хранится
чение нескольких суток. В случаях, когда камера фиксирует совершени
ступления, запись используется в целях розыска преступника и доказыва
его вины. Так, благодаря записям системы видеонаблюдения одного
рилиалов Сбербанка в начале 2007 г. был опознан грабитель, отнимавший
ги у клиентов кредитной организации.

В другом филиале Сбербанка видеонаблюдение было использовано для
упреждения преступления. Сотрудники отдела безопасности филиала об
ли внимание на необычное поведение двух мужчин, которые внимательно
осматривали датчики охранно-пожарной сигнализации, однако услугами
ка не воспользовались. Фотографии неизвестных были распечатаны с за
и системы видеонаблюдения и переданы в местное управление по борьбе

Подробнее об «извещателях» см.: *Крахмалев А. К.* Безопасность учреждений кредитно-фи
вой системы. Технические средства охранной сигнализации // Банковское дело 2003. № 5.

с организованной преступностью. Посетители филиала были опознаны как лица, ранее участвовавшие в разбойном нападении на инкассаторов. Принятые меры позволили задержать преступников на стадии подготовки к совершению преступления[1].

Химические ловушки (далее — ловушки) представляют собой снаряженные (обработанные) специальными химическими веществами (красящими или запаховыми) приспособления или устройства, закамуфлированные под различные предметы, с помощью которых такие вещества переносятся на тело и одежду человека. В отличие от других технических средств защиты порядок их применения регламентирован нормативным актом — «Инструкцией о порядке применения химических ловушек в раскрытии краж имущества, находящегося в государственной, муниципальной, частной собственности, собственности общественных объединений (организаций), утвержденной приказом МВД России от 11 сентября 1993 г. № 423.

Организация взаимодействия органов МВД России и кредитных организаций, входящих в структуру Ассоциации Российских банков (далее — АРБ) при использовании ловушек, регламентирована совместным указанием МВД России от 9 августа 1996 г. № 1/13 736 и АРБ от 9 августа 1996 г. № А-05/1с-684 «О мерах по повышению эффективности использования специальных химических веществ в борьбе с преступностью».

Установка ловушки в целях блокирования объекта документируется работником милиции составлением соответствующего акта. В случае кражи ценностей и срабатывания ловушки в протоколе осмотра места происшествия обязательно указывается факт обнаружения распыленных химических веществ. При задержании подозреваемых в краже лиц к протоколу приобщается одежда, предметы со следами химических веществ, а также смывы красителя с кожных покровов задержанного. Сравнительное исследование химических веществ, изъятых с кожных покровов и одежды подозреваемого лица и образца химического вещества, установленного и нарушенного на заблокированном объекте, производится экспертно-криминалистическими подразделениями МВД России.

Ныне применяющиеся ловушки классифицируются в зависимости от свойств применяемых в них химических веществ, на красящие, люминесцирующие и запаховые.

Красящие, люминесцирующие и запаховые вещества составляют основу химических ловушек, применяемых для блокировки различных объектов. Химические ловушки — это снаряженные (обработанные) специальными химическими веществами приспособления или устройства, закамуфлированные под различные предметы, с помощью которых такие вещества переносятся на тело и одежду человека. Ловушки могут быть активного и пассивного

[1] *Логвинова Н.* Видеонаблюдение в банках переводится на «цифру» и IP // Банковское обозрение. 2007. № 003. 14 марта. С. 81–87.

ов. В ловушках активного типа химические вещества переносятся на объ
при срабатывании механического или пиротехнического распылителя
т момент, когда преступник пытается взять какой-либо предмет, открыть
ь, окно, форточку; вскрыть коробку, упаковку. При срабатывании из ло
ки направленно выбрасывается порошок или раствор специального хими
кого вещества, который попадает на части тела и одежду преступника.
Наиболее распространенными ловушками, рекомендованными к исполь
нию в настоящее время, являются: «Кукла-МГ», «Кредит», «Мини-Кре
-Л» и «Скунс».
Изделие «Кукла-МГ» имитирует банковскую упаковку денег. Эта ловушк
батывает мгновенно при похищении: опыляет преступника несмываемы
ящим веществом малинового цвета и воздействует на него слезоточивы
м.
Ловушка «Кредит» имитирует банковскую упаковку денег (10 пачек) и пред
ляет собой комбинированное изделие активного действия. В момент кра
или разбойного нападения она обеспечивает включение сигнала тревог
ульте охраны.
Через пять минут после кражи изделия или передачи ловушки преступник
ледняя выбрасывает специальные химические вещества, подает звуково
ал, а также интенсивно выделяет облако оранжевого дыма.
Мини-Кредит-Л» имитирует банковскую пачку денег (100 листов). Ло
ка подает сигнал тревоги на пульт охраны в момент совершения преступ
ия, а через три минуты после похищения, либо разбойного нападения, вы
ывает специальные химические вещества, подает звуковой сигнал и выде
облако оранжевого дыма.
апахово-маркирующая ловушка «Скунс», снабженная пиротехническим
ылителем, выбрасывает на похитителя несмываемые маркирующий и за
вый составы. Применение в указанных составах люминесцирующих ком
ентов позволяет на длительное время надежно пометить преступника
оже значительно облегчить его поиск по оставленным следам с помощью
искных собак.
зарубежной практике применяются ловушки, встроенные в банкоматы.
устройства выбрасывают трудносмываемое красящее вещество при по
ке взлома или похищения банкомата.
Помимо пиротехнических ловушек «активного действия» в целях розыска
тупников и создания доказательственной информации на случай совер
ия противоправного посягательства применяются ловушки в виде специ
о помеченных купюр (которые обнаруживаются при попытке сдать
банк), либо купюр, обработанных бесцветным веществом, окрашиваю
кожные покровы и одежду преступника.
пецифической разновидностью систем охранной сигнализации являются
ратно-программные комплексы, предназначенные для выявления попыток
нкционированного проникновения в компьютерную сеть и оповещения

о них персонала службы защиты информации. Такие системы, наряду с функциями технической защиты от нелегитимных команд злоумышленника и извещения о них службы защиты информации, выполняют задачи выявления адреса периферийного устройства, с которого предпринималась попытка несанкционированного проникновения, и характерных признаков, присущих субъекту посягательства, а также протоколируют факт и обстоятельства правонарушения.

Важным направлением обеспечения безопасности банка является защита кредитной организации от информационного проникновения путем несанкционированного прослушивания телефонов и рабочих помещений. В качестве технических средств противодействия угрозам указанных видов применяются широко представленные на отечественном рынке «акустические сейфы» для телефонов, а также устройства защиты телефонных линий и маскираторы конфиденциальных переговоров.

«Сейфы» предназначены для активной защиты речевой информации от несанкционированного прослушивания через находящийся в помещении телефон. Защитные функции «сейфа» срабатывают автоматически в случае попытки негласной дистанционной активации микрофона.

Современные устройства защиты телефонных линий обеспечивают: кодовый доступ к линии от телефонного аппарата; блокировку набора номера вне защищенной области; блокировку звонка, исходящего в неурочное время; защиту от устройства «телефонное ухо»; защиту от ВЧ-навязывания; запись в память до 1000 попыток нештатного использования телефонной линии с привязкой по времени.

Акустический маскиратор конфиденциальных переговоров в помещении маскирует речь в помещении методом радиозашумления.

Для выявления и нейтрализации различного рода электронных подслушивающих устройств широко используются автоматические поисковые приемники, профессиональные локаторы нелинейности и индикаторы поля.

4.3. Технические средства защиты банковских операций и продуктов

Согласно данным статистики правоохранительных органов России и практике служб безопасности коммерческих банков наиболее распространенными способами посягательств на имущество банков, совершенных с использованием банковских операций и инструментов, являются:

1) использование поддельных денег, ценных бумаг и иных платежных документов;

2) хищение «электронных» денежных средств с использованием неправомерного доступа к компьютерной информации банка;

3) хищение денежных средств с банковского счета с использованием пластиковых карт.

Данные МВД России свидетельствуют о том, что изготовление и сбыт под
ьных денег является весьма распространенным явлением в нынешней Рос
и. В 2007 г. органами милиции было зарегистрировано 46 272 преступлени
го вида. За указанный период сотрудники ДЭБ МВД России пресекли дея
ьность 42 организованных групп фальшивомонетчиков.
В структуре выявленных фактов фальшивомонетничества превалирую
дельные денежные знаки Банка России — купюры достоинством в 100
00 руб. По ним возбуждено более 77% от общего числа уголовных дел ука
ной категории. Однако это не означает, что преступники отказываются
подделки денежных знаков другого номинала (табл. 1).

Таблица

Подделка денежных знаков Банка России в I квартале 2008 г.

Номинал денежного знака купюры, монеты достоинством, руб.	Количество денежных знаков
5000	4
1000	27 062
500	1281
100	718
50	150
10	55
5	103
1	1

Удельный вес поддельной иностранной валюты в общей массе фальшиво
колько снизился. На долю долларов США приходится 21,8%, евро — 0,8%
ако количество этих «денежных знаков» остается весьма высоким (табл. 2)

Таблица

Структура поддельных денежных знаков иностранных государств, выявленных в I квартале 2008 г.

Наименование валюты	Количество денежных знаков
лар США	1488
ро	128
дская крона	1
айский юань	2
го поддельных денежных знаков	1619

Значительную часть фальшивок составляют так называемые суперподдел
В конце 2007 г. органы МВД России пресекли канал поставки в Россию
ельных долларов США из стран Южной и Юго-Восточной Азии. По

заключению экспертов Министерства финансов США, эти подделки были произведены на профессиональном оборудовании и имели имитацию значительного числа элементов защиты подлинных купюр (тиснение, выдавленный рельеф, металлизированная полоса, соответствующее свечение при облучении детекторами валют). Выявить подделки при помощи обычных детекторов валют, использующихся в торговых точках, не представлялось возможным.

В настоящее время практически все коммерческие банки России время от времени выявляют среди представленных клиентами наличных денежных средств фальшивые купюры того или иного достоинства. Как правило, клиенты банка в таких случаях о подделках не осведомлены.

Наряду с поддельными денежными знаками кредитные организации встречаются с попытками преступников использовать в банковских операциях и сделках поддельные векселя, облигации, платежные поручения и другие документы.

Известен случай, когда филиал ныне несуществующего Инкомбанка перечислил по фальшивому платежному поручению (с поддельными подписью и печатью) со счета института «Теплоэлектропроект» на счет фирмы-однодневки 400 тыс. долл. Эти деньги были похищены, а фирма исчезла. Аналогичным образом были похищены около 200 млн руб. в «Мосбизнесбанке» и 1,5 млн долл. в «Российском национальном коммерческом банке».

Одним из основных направлений защиты банковских (в первую очередь — кассовых) операций и инструментов от противоправных посягательств с использованием подделок является выявление последних путем применения специальных технических средств и приборов.

Принцип действия указанных приборов заключается в определении подлинности защитных признаков изучаемого объекта. К числу защитных признаков относятся свойства бумаги, красок, внедренных цветных защитных волокон, специальные технологии печати, графические элементы защиты (рамки, сетки, розетки, узоры); оригинальные шрифты; магнитные полосы, микротекст; скрытое изображение; цифровые и штриховые коды; порядковые номера.

Надежная проверка подлинности банкнот и ценных бумаг требует контроля защищенных документов по максимальному числу защитных признаков. В настоящее время банки имеют возможность приобретать технические средства, позволяющие с высокой степенью надежности устанавливать наличие (либо отсутствие) любого из применяющихся защитных признаков, либо их имитацию[1].

Наиболее распространенными техническими средствами выявления фальшивых денежных знаков и ценных бумаг являются детекторы и счетчики

[1] Точное одновременное воспроизведение всего комплекса защиты — весьма сложная и дорогостоящая задача, поэтому на фальшивках обычно воспроизводится часть защитных признаков, некоторые из них могут отсутствовать, а другие имитироваться с использованием упрощенных технологий.

оты различных модификаций и видов контроля, различного назначени
зуализаторы и лупы, а также приборы для комплексного визуального ко
ля, оснащенного, кроме того, точными магнитными, инфракрасным
ругими датчиками.

В современной банковской практике широко используются собственны
дства и методы защиты ценных бумаг и платежных документов. Суть пред
инимаемых для этого защитных мер заключается в использовании скрыто
окировки документов, отсутствие которой свидетельствует о подделке. Пр
аче векселя, например, в документ включается так называемая вексельна
ка — тайный знак, о содержании которого осведомлен предельно узки
т лиц. В частности, «метка» может быть исполнена невидимым при обы
и освещении составом, который наносится специальным маркером и св
ся в УФ- или иных лучах. Отсутствие метки при предъявлении векс
плате свидетельствует о том, что вместо подлинника предъявляется выс
ачественная копия, а сам подлинник будет предъявлен другим лицом. Со
сно действующему законодательству в подобной ситуации банк будет до
погасить вексель вторично.

Контрольные метки могут включаться в печати и подписи клиентов бан
взаимному соглашению с банком в целях защиты от поддельных платеж
поручений, накладных, сертификатов ценных бумаг. Они выполняют
мя основными способами. Первый — внесение в печать мельчайших, нез
ных для постороннего, дополнительных элементов и «погрешностей
поддающихся воспроизведению. Второй — включение в печать скрыто
бражения, не видимого без специального шаблона и также не поддающе
подделке. Третий — использование в оттиске печати или подписи упол
оченного лица химической метки, которая появляется или меняет цве
воздействием лучей простейшего детектора валют.

В случаях использования клиентом печатей и подписей со специальны
ками, он предоставляет банку описание использованных средств защит
струкцию о порядке контроля оттиска, а также обеспечивает банк необ
имыми средствами контроля — шаблонами и ключами.

Хищение «электронных» денежных средств, как правило, сопряжено с ис
зованием неправомерного доступа к компьютерной информации банка
ступление совершается путем несанкционированного перевода денежны
ств на расчетный счет соучастников хищения. Неправомерный досту
формационной системе банка и управление счетами могут совершаться
извне кредитной организации — так называемыми хакерами, так и со
никами банка (инсайдерами).

Средствами защиты от внешних посягательств на компьютерные сети яв
ются: антивирусные программы, межсетевые экраны, инструменты (моду
атчики) обнаружения, реагирования на обнаруженную атаку и блокиро
ия несанкционированного вторжения.

Защита компьютерной информации банка от «внутренних факторов» — противоправных действий собственного персонала (и бывших работников) — осуществляется на основе технологий и средств разграничения доступа к информационной среде[1]. Наиболее успешно эта задача решается с использованием смарт-карт или USB-ключа, хранящихся у сотрудников. Наряду с ключом сотрудник использует известный только ему PIN-код. Данная технология позволяет допустить в помещение, к компьютеру и в систему только подлинного пользователя и одновременно провести его авторизацию для доступа к конкретным разделам информации и используемым приложениям. Одновременно система ведет протокол (историю) действий пользователя в информационном пространстве, которые при необходимости могут быть воспроизведены в целях анализа, проверки или расследования. В случае интеграции системы с данными службы персонала система блокирует попытки использования посторонними смарт-карты и PIN-кода сотрудника, находящегося в отпуске или командировке. Некоторые системы разграничения доступа используют вместо смарт-карты биометрические средства идентификации пользователя — отпечатки пальцев и радужную оболочку глаз.

Хищение денежных средств с использованием пластиковых карт является весьма распространенным видом посягательства на имущество банка. По оценкам МВД России ущерб от этого вида преступлений, совершаемых в России ежегодно возрастает в полтора раза.

К числу технических средств защиты от карточного мошенничества относятся средства защиты:

- карт от несанкционированного использования;
- процессинговых центров, обрабатывающих операции с картами;
- банкоматов для выдачи наличных денег.

Средства защиты карт от несанкционированного использования включают в себя оборудование по изготовлению пластикового носителя, нанесению на него специальными методами печати соответствующих реквизитов — банка и платежной системы, а также технические средства для включения в карту специальных средств защиты: голограммы, штрих-кода, магнитной полосы или микрочипа.

В картах со штрих-кодом в качестве идентифицирующего элемента используется штриховой код, аналогичный коду, применяемому для маркировки товаров.

Карты с магнитной полосой (пленкой на обратной стороне) содержат в памяти номер карты; имя держателя; срок ее действия; сервис-код, определяющий допускаемые для данной карты типы операций. На магнитной полосе могут также записываться другие коды, позволяющие обнаружить устройством,

[1] Согласно оценкам экспертов, «внутренние факторы» представляют наибольшую опасность для информационной безопасности банков. См.: *Мартынова Т.* Люди — самое слабое звено // Банковское обозрение. 2004. № 10. С. 40–43.

олняющим операцию, неверно введенный персональный идентификаци
ный номер (ПИН) или нарушение соответствия на магнитной полосе ин
ормации.

Для повышения защищенности карт этого вида, эмитируемых системам
SA и MasterCard/Europay используются дополнительные графические сред
за защиты: голограммы и нестандартные шрифты для эмбоссирования (на
сения рельефного шрифта). Для защиты информации на магнитной полос
итенты ввели проверочные коды, например, код CVV в системе VISA ил
/C в системе Europay. Введение CVV и CVC снизило потенциальную воз
ожность использования карт с перекодированной магнитной полосой, н
защитило от копирования информации.

В картах с микрочипом (смарт-картах) носителем информации являет
кросхема с объемом памяти от 32 байт до 16 килобайт. Карты подраздел
ся на два типа: с незащищенной (полнодоступной) и защищенной пам
о. Уровень защиты карт памяти выше, чем у магнитных карт, и они мог
ть использованы в прикладных системах, включая те, в которых финанс
е риски связаны с мошенничеством. В настоящее время разрабатываютс
едства защиты карт на основе биометрических данных владельца (отпеча
в пальца и радужной оболочки глаз).

Защита процессинговых центров, обрабатывающих операции с картам
мошенничества осуществляется путем применения технических и крипт
ифических средств защиты компьютерных сетей и средств защиты баз дан
х от взломщиков извне.

Для защиты от неправомерных действий персонала применяются средст
ограничения доступа сотрудников банка, ведающих пластиковыми картам
истеме управления операциями.

Весьма важную роль в предупреждении преступлений с картами играют авто
гизированные системы обнаружения мошенничества, разработанные ком
ниями HNC Software Financial Solutions, Inc., Nestor, Inc., AT&T, MasterCar
циональная Лаборатория в Лос-Аламосе, Visa International, IBM, Тех
truments и др. Такие системы позволяют выявлять подозрительные на мо
нничество операции с высокой степенью вероятности в реальном режим
емени и блокировать их до проведения проверочных мероприятий.

Технические средства защиты банкоматов для выдачи наличных денег при
ны обезопасить эти устройства как от попыток их примитивного механиче
ого взлома с целью изъятия денег, так и от посягательств на обрабатывае
ю банкоматами компьютерную информацию процессингового центра. Та
о информацию преступники могут добывать не только путем подключени
линиям связи банкомата, но и другими весьма изощренными способами
оторых пойдет речь далее.

В число технических средств защиты от указанных посягательств входя
оминавшиеся ранее извещатель «Шорох-2» для защиты банкоматов от ванда
зма и вскрытия сейфа и извещатель ИО 102–31 для блокировки банкомато

на открывание и перемещение. Одновременно с извещателями используются системы скрытого видеонаблюдения для проверки переданных извещателями сигналов о подозрительных манипуляциях с банкоматом и фиксации сути события.

4.4. Технико-криминалистические средства

Современная криминалистика предлагает классифицировать технико-криминалистические средства по различным основаниям. В частности, *по источнику происхождения* (специально созданные криминалистические средства; средства, заимствованные из других областей человеческой деятельности и приспособленные для нужд криминалистики; средства, перенесенные в криминалистику из других областей человеческой деятельности без изменений) и *по целевому назначению* (предназначенные для применения при производстве следственных действий, для экспертных исследований криминалистических объектов; а также для решения иных криминалистических задач, в том числе для предупреждения преступлений). Последние являются наиболее распространенным видом технико-криминалистических средств, используемых в целях обеспечения банковской безопасности. В обеспечении безопасности банка средствами криминалистической техники участвуют (в соответствии с задачами и функциями, установленными законодательством) субъекты двух категорий:

а) правоохранительные органы, наделенные правом применять средства и методы криминалистики в рамках уголовного процесса и оперативно-розыскной деятельности;

б) негосударственные структуры, реализующие разработанные криминалистикой меры противодействия преступлениям в рамках Закона о частной детективной деятельности и корпоративного права[1].

Настоящий параграф посвящен использованию технико-криминалистических средств службой безопасности банка, которая играет ведущую роль в числе субъектов второй группы[2].

Главным отличием средств криминалистической техники от описанных в предыдущих параграфах технических средств охраны и технических средств защиты банковских операций и инструментов является их специальная предназначенность для предупреждения *и расследования* преступлений (в порядке, предусмотренном Уголовно-процессуальным кодексом) и правонарушений (в рамках внутреннего расследования организации).

---

[1] Подробнее об особенностях использования средств криминалистики указанными субъектами см.: *Гамза В. А., Ткачук И. Б.* Безопасность коммерческого банка: Организационно-правовые и криминалистические проблемы: монография. М.: Изд-ль Шумилова И. И., 2002. С. 65–67.

[2] Вопросы применения названных средств правоохранительными органами подробно исследованы в криминалистической литературе.

Перечень видов названных средств определяется основными задачам
ужбы безопасности банка, в частности: обеспечением сохранности имуще
ва кредитной организации, безопасности банковских операций и порядк
нкционирования банка, а также защитой охраняемой информации и систе
ı кадрового обеспечения банка от противоправных посягательств.

Нынешние средства технико-криминалистического обеспечения деятел
сти службы безопасности банка, как правило, включают в себя широки
бор приспособлений, начиная с классических средств выявления и фикса
и различного рода следов и заканчивая последними разработками в област
соких технологий[1].

Так, для обнаружения подделок документов, совершенных лжеклиентам
бо недобросовестными сотрудниками банка, применяются оптические пр
ры: лупы различной кратности, измерительные лупы, портативные карма
е микроскопы, источники невидимых лучей — портативные ультафиолет
е осветители, электронно-оптические преобразователи.

Вполне оправданным в определенных случаях является использован
ɜдств выявления на документах (в том числе на ценных бумагах) пальцевы
печатков злоумышленника. Так, отпечатки пальцев преступников, обнар
нные в 2004 г. службой безопасности одного из коммерческих банков М
ы на предъявленных к оплате фальшивых расчетных чеках, позволил
ороткое время установить личности мошенников, использовавших паспо
ругих лиц, и явились доказательствами их вины в суде.

К числу средств обнаружения при предварительном исследовании следо
относятся порошки последнего поколения ПМД-Ч, ПМД-Б, ПМДЛ-С
юшки в аэрозольной упаковке, изделия «Кит» для выявления следов пал
парами йода, широкозахватные магнитные кисти для работы с порошк
Для фиксации и изъятия следов рук можно использовать «Материал лип
ı пленочный» (МЛПД) и следокопирующий состав в аэрозольной упаковк
ıпия».

Средства обнаружения и фиксации следов рук могут использоваться в це
внутренних расследований по фактам посягательства на конфиденциаль
ı и компьютерную информацию, на личное имущество сотрудников, нахо
ıееся в служебных помещениях.

Вполне допустимым в целесообразных случаях является применени
ıств фиксации запаховых следов человека и объектов-носителей запаха
ледующее использование современных приемов выборки объекта по запа
роводится без участия подозреваемых (проверяемых) лиц, не связан
облемами ущемления прав и достоинства проверяемого.

В число приборов для фиксации хода и результатов внутреннего расследо
ия входят фото- и видеокамеры, цифровые звукозаписывающие устройств

[1] Все эти средства находятся в свободной продаже и специальных разрешений на их приоб
ие не требуется.

(весьма полезные для записи и последующего анализа пояснений опрашиваемых лиц), а также устройства для документирования следов устной речи (в случаях вымогательства, угроз, шантажа в отношении сотрудников банка).

В случаях наблюдения за изучаемым объектом в рамках ст. 5 Закона о частной детективной деятельности могут использоваться специальные оптические приборы (дневного и ночного видения), а также средства телевизионного наблюдения (стационарные, мобильные, записывающие информацию на специальный носитель или передающие ее в режиме реального времени).

В 2005 г. в одном из московских банков в ходе внутреннего расследования по фактам неоднократных попыток незаконного доступа во внерабочее время к компьютерной информации была использована замаскированная телекамера, начинавшая запись одновременно с включением используемого злоумышленником компьютера. На вторую ночь после установки техника зафиксировала субъекта противоправных действий, которым оказался охранник банка.

К числу технико-криминалистических средств, разработанных на базе высоких технологий, следует отнести активно внедряющиеся в сферу обеспечения безопасности банка информационно-аналитические комплексы (далее — ИАК), а также устройства, известные в настоящее время под названием «полиграф».

Применение ИАК нацелено на обработку в сжатые сроки большого объема разноплановой информации (хранящейся в электронном виде в различных базах данных банка), извлечение из нее определенного вида данных, их правильной оценки и принятия по результатам анализа обоснованных и своевременных решений. К числу непосредственных задач ИАК относится выявление и блокирование случаев мошенничества в кредитной сфере, злоупотреблений полномочиями со стороны персонала, неправомерных посягательств на охраняемую информацию, предупреждение и расследование других опасных для банка действий и событий, а также для противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Так, целям предупреждения злоупотреблением полномочиями и защиты порядка функционирования банка может служить автоматизированный поиск в массиве текущей (и архивной) информации признаков нарушений процедур, функций и полномочий по принятию решений в действиях любого из сотрудников банка и его филиалов.

При этом комплекс представляет сведения о содержании и других характеристиках операции, о сути допущенного нарушения, а также о конкретных нормативных предписаниях и обязательствах (инструкции, договоре), которые нарушил виновный. По команде пользователя комплекс группирует информацию по времени и видам нарушений, по сотрудникам банка, совершившим нарушения, по клиентам, связанным с выделенными операциями и т. д.

Заданные комплексу параметры помогают аналитику в выявлении в иссл
:мых массивах информации сведений о сотрудниках банка, которые мог
ть признаны лицами, заинтересованными в операциях (сделках).
Описанная методика поиска признаков нарушений процедур, функци
юлномочий субъектов успешно применяется в целях защиты информаци
ıка. В практическом плане поиск следов противоправной деятельност
ıассивах компьютерной информации нередко сравним с поиском небезы
тной «иголки в стоге сена», поскольку необходимые для расследован
ные скрыты в большом объеме не относящихся к делу сведений. Так, н
ımер, в одной из обследованных авторами российских организаций объ
формации только в одном из регистрирующих файлов достигает в течен
ючего дня 5 млн записей.
Поиск необходимых сведений «вручную» — путем построчного просмот
роверки каждой из записей по ряду необходимых для расследования пар
ров — практически невыполнимая задача.
В то же время ИАК, использующий программные продукты компан
ıal Analytics Inc. (США) и отечественной компании «Институт пробле
опасности и анализа информации» позволяют не только выявлять необх
ıую информацию по характерным признакам, присущим действиям зл
ıшленника, но и представлять результаты поиска в удобной для пользов
я визуальной форме.
Аналитические системы, созданные на основе данных технологий сп
ны преобразовывать в единый формат данные, поступающие с различн
тролируемых объектов. Их применение позволяет проследить последов
ьность действий злоумышленника, установить способ совершения и ма
овки преступления, цель неправомерного доступа и местонахождение сл
. Полученные данные представляются в виде визуальной схемы, понятно
только специалистам, но и другим лицам (следователю, понятым, су
д.).
Существенным направлением информационно-аналитической поддерж
кбы безопасности является возможность представления результатов сыс
(проверочной) деятельности предполагаемого клиента или проведенно
треннего расследования в виде визуальных моделей, отражающих:

- обстоятельства, подлежащие проверке;
- мероприятия, которые необходимо выполнить в целях проверки;
- факт выполнения и результаты выполненных мероприятий, источни
  и материалы для обоснования принятого решения;
  степень полноты полученных сведений, позволяющих принять оконча
  тельное решение по делу[1].

Подробнее об ИАК см.: *Гамза В. А., Чокпаров М. К., Ткачук И. Б.* Специальные аналитич
технологии в сфере безопасности банка // Оперативное управление и стратегический м
мент в коммерческом банке. 2005. № 3(25). С. 121–125.

Полиграф, как известно, представляет собой устройство, объективно регистрирующее психофизические реакции человека и нашедшее практическое применение в области криминалистического обеспечения банковской безопасности, для решения задач:

- выявления, предупреждения и раскрытия преступлений и правонарушений;
- установления лиц, их подготавливающих, совершающих или совершивших преступления и правонарушения;
- подготовки и осуществления сыскных мероприятий в целях сбора, обработки и фиксации данных, имеющих значение в процессе внутреннего расследования и уголовно-процессуального доказывания;
- проверки истинности пояснений, полученных в ходе внутренних расследований.

Необходимость применения полиграфа в банковской сфере не ограничивается борьбой с преступными посягательствами. Весьма обширный перечень опасных для банка деяний выступает в виде гражданско-правовых деликтов и служебных проступков. По этой причине функциональные обязанности службы безопасности включают в себя также задачи, связанные с выявлением и расследованием служебных проступков работников, нарушением норм трудового и гражданского права, внутренних (локальных) нормативных актов банка; с обеспечением возмещения ущерба, причиненного указанными проступками.

Служба безопасности банка использует полиграф при выполнении задач внутреннего контроля, проведении внутренних расследований, подготовке материалов для принятия решений о полной материальной ответственности работника или коллектива (бригады) работников. Результаты опросов с использованием полиграфа (далее — ОИП) могут служить одним из оснований для принятия решения о расторжении трудового договора с работником, непосредственно обслуживающим денежные или товарные ценности, в связи с утратой доверия к нему со стороны работодателя.

Применение полиграфа открывает новые возможности поиска, проверки и оценки информации в случаях, когда из-за особенностей технологии (операций) традиционные методы и средства не дают возможности установить конкретного виновника события (речь идет об участках, где с работниками обычно заключается договор о коллективной ответственности). В качестве типичного примера можно назвать обнаружение недостачи денег в сейфе, к которому имеет доступ определенный круг лиц. При этом свидетели и доказательства отсутствуют. В сложившейся ситуации сотрудники, имеющие доступ к сейфу, заинтересованы в собственной реабилитации. Применение ОИП в данном случае является практически единственным методом установления истины.

Полиграф необходим также для повышения качества и сокращения сроков проверки кандидатов на работу в банк и в ряде других отношений

Использование технологии ОИП позволяет выявлять у кандидатов на ра
гу такие «факторы риска», как склонность к злоупотреблению алкоголе
отребление наркотиков, связь с криминальными структурами и т. д. Перио
ческое проведение ОИП в коллективе позволяет освободиться от лиц, пр
ретающих указанные факторы уже в период работы, т. е. проводить профи
стику правонарушений.

Все более широкое применение в обеспечении безопасности банков в по
днее время находят различного рода негосударственные учеты, содерж
е информацию о фактах, субъектах, предметах и следах противоправно
тельности. Они представляют собой разновидность криминалистическ
тов, разработанных в рамках теоретических положений и рекомендаци
риминалистической техники. Такие специализированные информационны
стемы создаются в каждом отдельном банке, а также в рамках межбанко
их организаций и активно используются в целях предупреждения престу
ний, в первую очередь в кредитной сфере и сфере вексельного обращения.
Так, собственным информационным массивом об участниках вексельно
нка и фактах противоправных посягательств в указанной сфере облада
данная при поддержке Банка России в 1996 г. некоммерческая организ
я — Ассоциация участников вексельного рынка (АУВЕР)[1]. Последняя пр
тавляет всем заинтересованным постоянно пополняемую информаци
охищенных и утраченных векселях и бланках векселей; о признании ко
тных векселей недействительными (в связи с наложением на них аре
дователем или судом) или вышедшими из законного обращения (факт в
а из законного обращения устанавливается решением суда); о поддельн
селях (их реквизитах и признаках подделки). Показательно, что в после
время у служб безопасности банков и других добросовестных участник
сельного рынка появилась возможность официально получать и использ
, в целях предупреждения преступных посягательств и сведения, содерж
ся в криминалистических учетах правоохранительных органов. В частно
информацию о фальшивых векселях, исполненных на поддельных бла
предоставляет Экспертный криминалистический центр МВД России.

[1] Адрес: 107140, Москва, а/я 107 (для АУВЕР), тел./факс: (495) 692–9488, 264–9177. E-ma
@auver.ru (www.auver.ru).

ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. Какие три элемента являются основными ориентирами при построении системы технических средств обеспечения безопасности банка?
2. Назовите основные виды технических средств обеспечения безопасности банка в соответствии с их функциональным назначением.
3. На каких основных направлениях обеспечения безопасности банка применяются технические средства охраны?
4. Назовите основные виды средств:
   - инженерно-технического укрепления банка;
   - обнаружения тревожных ситуаций;
   - способствующих розыску преступника и созданию доказательственной информации;
   - защиты конфиденциальной информации.
5. Какие технические средства применяются в целях защиты от использования поддельных денег, ценных бумаг и иных платежных документов; «электронных» денежных средств, а также поддельных и похищенных пластиковых карт?
6. В чем заключается главное отличие средств криминалистической техники от технических средств охраны и технических средств защиты банковских операций?
7. Какие виды криминалистической техники применяются в банках в настоящее время в целях обеспечения безопасности?

Глава 5

ЗАЩИТА ОТ ПРЕСТУПЛЕНИЙ, ПОСЯГАЮЩИХ НА СОБСТВЕННОСТЬ БАНКА

- Хищения денежных средств при совершении кредитных операций
- Хищения денежных средств с незаконным использованием пластиковых карт
- Хищения денежных средств с использованием аккредитивов
- Хищения денежных средств с использованием чеков
- Хищения денежных средств с использованием платежных поручений

5.1. Хищения денежных средств при совершении кредитных операций

Выдача кредитов представляет собой наиболее распространенную услу
:дитных организаций. Правовой основой взаимоотношений кредитор
аемщика является кредитный договор (ст. 819 ГК РФ), по которому бан
и иная кредитная организация (кредитор) обязуются предоставить денеж
е средства (кредит) заемщику в размере и на условиях, предусмотренны
оворам, а заемщик обязуется возвратить полученную денежную сумм
платить проценты на нее.

Согласно общим правилам кредитования, банковские кредиты предостав
ются как физическим, так и юридическим лицам (включая предпринимате
без образования юридического лица). Юридические лица получают кре
ную сумму только путем безналичного зачисления на расчетный, текущи
г. Физические лица — как в безналичном порядке, так и наличными де
ными средствами.

Наиболее распространенными формами банковского кредита являются:

- срочный кредит — разовое предоставление денежных средств на опре
  деленный срок;
- кредитная линия — многократное предоставление средств в рамках ус
  тановленного лимита;
- ипотека — кредит под залог недвижимости;
- потребительский кредит (для физических лиц).

Потребительский кредит предоставляется населению на приобретение то
ов длительного пользования и на неотложные нужды (оплата образования
онта в доме и т. д.). Основные формы потребительского кредита:

- покупка товаров в рассрочку;
- покрытие кредитной карты;
- персональные ссуды на личное потребление.

Договор займа в соответствии со ст. 814 ГК РФ может быть заключен с ус
ием использования заемщиком полученных средств на определенные цели
евой заем). В этом случае заемщик обязан обеспечить возможность осу
ствления заимодавцем контроля за целевым использованием суммы займа.

Кредитор вправе отказаться от предоставления заемщику предусмотренного кредитным договором кредита полностью или частично при наличии обстоятельств, свидетельствующих о том, что предоставленная заемщику сумма не будет возвращена в срок (ст. 821 ГК РФ).

В случае нарушения заемщиком предусмотренной кредитным договором обязанности целевого использования кредита (ст. 814 ГК РФ) кредитор вправе также отказаться от дальнейшего кредитования заемщика по договору.

Кредиты, предоставляемые банком, могут обеспечиваться залогом недвижимого и движимого имущества, в том числе государственных и иных ценных бумаг, банковскими гарантиями и иными способами, предусмотренными федеральными законами или договором (ст. 33 «Обеспечение возвратности кредитов» Закона о банковской деятельности).

Наиболее распространенными видами залога являются:

1) залог товаров в обороте;
2) твердый залог (заклад) — имущество, переданное залогодержателю во владение;
3) ценные бумаги — переданные в депозитарий или в банк;
4) недвижимое имущество.

При нарушении заемщиком обязательств по договору банк вправе досрочно взыскивать предоставленные кредиты и начисленные по ним проценты, если это предусмотрено договором, а также обращать взыскание на заложенное имущество в порядке, установленном федеральным законом.

Распространенность кредитных операций сделала указанную сферу весьма привлекательной для лиц с противоправными устремлениями. Случаи незаконного завладения имуществом (деньгами) банка под видом получения кредита широко распространены как в современной России, так и за рубежом. В частности, речь идет о мошенничестве.

Мошенничество, т. е. хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием — уголовно наказуемое деяние, предусмотренное ст. 159 УК РФ.

По данным правоохранительных органов, этот способ хищения составляет около 80% от общего числа преступлений, совершенных в кредитно-финансовой сфере. С обманным получением и невозвратом кредитов связаны наибольшие потери российских банков. Преступные посягательства этого вида широко распространены как в сфере потребительского кредитования, так и в сфере кредитования юридических лиц.

Мошенничество в сфере потребительского кредитования

Получение кредита физическим лицом не обусловлено залогом и, как правило, ограничено относительно небольшой суммой заемных денежных средств. Однако опасность этого способа хищения заключается в лавинном росте числа преступных посягательств этого рода. В итоге указанные действия

собны поставить под угрозу стабильность функционирования отдельны
ечественных банков и банковской системы в целом.

По данным АРБ, объем потребительского кредитования в 2006 г. превыси
трлн руб. Однако этот процесс сопровождается ростом невозвращенных кре
гов. За первое полугодие 2006 г. размеры просроченной задолженности у бан
з по розничным кредитам возросли более чем на 40% и превысили 33 млр
., что составляет 2,6% от общего объема займов (1,5% в 2005 г.). Проанализи
зав деятельность 200 крупнейших кредитных организаций в сфере потреби
ьского кредитования, Банк России отнес 40 из них к группе риска.

По оценке П. Бойко, президента Инвестсбербанка, занимающего 14-е ме
среди 300 крупнейших банков по объему кредитов, выданных населени
50 до 75% сумм невозвращенных кредитов похищается мошенниками[1]. АР
ценивает криминальную ситуацию на рынке потребительского кредитова
как угрожающую.

Наиболее уязвимым сегментом потребительского кредитования являето
дача кредитов на приобретение товаров в рассрочку — объем невозвращен
х долгов превышает 10%. Показательно, что объем невозврата так называе
х автокредитов, к выдаче которых банки подходят более взвешенно, со
вляет менее 1% выданных денежных средств.

Способы мошенничества в сфере потребительского кредитования. Схема ор
изации потребительского кредитования выглядит следующим образом
говая компания заключает договор с банком (кредитной организацией)
орый предлагает будущим покупателям воспользоваться целевым потреби
ьским кредитом на приобретение товаров в конкретном магазине. В подго
ке и реализации товаров в кредит участвуют специалист банка в точке про
и специалист торговой точки, оформляющий заявки.

Потенциальный заемщик представляет лицу, оформляющему заявки, доку
ты, необходимые для оформления кредита. Оформленные заявки переда
я сотруднику банка. Как правило, перечень указанных документов вклю
г в себя: паспорт гражданина России (или иной документ, удостоверяю
ю личность), справку о доходах, а также собственноручно заполненное
вление. В заявлении указываются наименование приобретаемого товара
о стоимость.

По результатам рассмотрения этих документов банк принимает решени
даче кредита. При этом в соответствии со ст. 821 ГК РФ он имеет право
зать в займе без каких-либо объяснений. В случае принятия решения
редоставлении кредита деньги перечисляются торговой организации. Товар
ается заемщику только после подтверждения факта зачисления денежных
ств на счет магазина.

Схема мошенничества включает в себя оформление кредита на покупку то-
без намерения возврата денежных средств, получение товара и его

[1] «Банкроты» и «мошенники» // Национальный банковский журнал. 2006. Март. С. 80.

продажу (обычно по заниженной цене) с целью извлечения наличных денежных средств. Правоохранительной практике известны многочисленные случаи перепродажи полученных мошенническим путем предметов сложной бытовой техники, компьютеров и даже автомобилей.

Для уклонения от ответственности за хищение мошенники используют приемы, позволяющие маскировать их собственное участие в совершении преступления. К числу основных направлений маскировки относятся следующие.

1. *Получение кредитов через подставное лицо.* Получение кредитов через подставное лицо заключается в использовании неких лиц (с их согласия, за небольшое вознаграждение) без постоянного источника дохода, имеющих паспорт с отметкой о постоянной регистрации. Такие субъекты снабжаются поддельными справками о наличии соответствующих доходов. В отдельных случаях такому участнику мошенничества могут обещать, что деньги на обслуживание кредита будут регулярно выплачиваться. Естественно, что возвратить кредит такие лица по причине отсутствия средств просто не в состоянии.

Одним из условий, побуждающих недобросовестных заемщиков (подставных лиц) к получению кредитов на свое имя, является отсутствие уголовной ответственности за предоставление банку заведомо ложных сведений о своем хозяйственном положении либо финансовом состоянии. Дело в том, что ст. 176 «Незаконное получение кредита» УК РФ устанавливает уголовную ответственность за совершение указанных действий только в отношении индивидуальных предпринимателей или руководителей организаций. Физические лица субъектами указанного преступления не являются и несут ответственность перед кредитором в гражданско-правовом порядке[1].

2. *Использование чужих паспортов.* В указанных случаях сотруднику банка предъявляются потерянные, похищенные или полученные под обманным предлогом паспорта. К ним, как и в указанных выше случаях, прилагаются поддельные справки о доходах. При утраченных или похищенных документах не исключено использование грима и других приемов маскировки, а также отвлечение внимания сотрудника различными приемами.

В числе обманных предлогов для временного завладения паспортом широко распространены объяснения о намерении оформить по ним на работу не имеющих регистрации лиц из других регионов или государств. Как правило, обманутый получает за временное предоставление паспорта в распоряжение мошенника небольшое вознаграждение.

Получению кредитов с использованием поддельных и чужих документов способствуют соревнование банков за лидерство в сфере потребительского кредитования, способствующее упрощению проверочных процедур, недостаточная квалификация и отсутствие опыта у работников банка (как правило,

[1] Указанная оговорка не относится к действиям субъектов, организующих и использующих указанных лиц как посредников в получении кредита. Их деяния рассматриваются как мошенничество.

студенты, работающие по 12-часовому графику), сжатые сроки принятия
дений об оформлении кредита, требования руководства о расширении объ
в кредитования, недобросовестность, а в ряде случаев и прямой сговор ра
ников магазинов и банков с преступниками.

Немаловажен и тот факт, что торговая организация мало интересуется пла
еспособностью или правопослушностью покупателя. Поскольку деньг
овар, выданный мошенникам (и некредитоспособным лицам), переходя
обственность магазина в момент их зачисления на счет, а убытки от мо
ничества и невозврата кредита несет банк, торговая организация заинте
ована лишь в том, чтобы продать товар в кредит в возможно большем ко
естве.

Поучительным примером мошенничества в сфере потребительского креди
ания могут служить действия организованной группы преступников, в ко
ую входили лица без определенных занятий — К. и Б., а также специалис
ела продаж магазина ООО «Скиф Электрофлот» М. Согласно заранее ого
енному распределению преступных ролей двое первых занимались приоб
ием паспортов для оформления кредитов на имя не осведомленны
итом владельцев документов и последующим сбытом полученной в магази
ехники. М. же, в обязанности которого в магазине входило заполнени
чков кредитных договоров и их сверка с оригиналами документов, запол
заведомо безвозвратные договоры кредитования с коммерческим банко
. Его доля преступной наживы от хищений составляла 5% от сумм оформ
ных потребительских кредитов. Указанная группа организовалась в ноябр
г. До июня 2005 г. мошенники похитили материальные ценности, выдан
по 74 кредитным договорам. Общая сумма похищенных средств ООО «Х
авила более 17,5 млн руб.[1]

Следует отметить, что «Х» в 2005–2006 гг. являлся обладателем «бронзы
ынке потребительского кредитования в России. Банк удерживал треть
го по количеству выданных кредитов, обладая 31% рынка потребительско
редитования и уступая лишь Сбербанку и «Русскому стандарту». Вмест
м, кредитный портфель банка в 2005 г. больше чем на четверть состоял
росроченных ссуд. В 2005 г. Службой безопасности банка выявлено более
фактов мошенничества в сфере потребительского кредитования на об
сумму более 108 млн руб. Из них более чем в 2000 случаев возбуждены
овные дела.

. *Получение кредитов действительным владельцем паспорта с последую-
отказом от факта получения кредита* под предлогом того, что документ
похищен и использовался для получения кредита другим лицом. Такие
ления неоднократно поступали в 2006 г. в отдельные московские банки.
ще случаев обман удалось выявить, используя в качестве доказательств

Обвинительное заключение по уголовному делу № 227608 относительно К. А. Матросова, Козлова и Л. Б. Бородиной, расследованному СУ УВД ЮЗАО г. Москвы.

заключения экспертов-почерковедов о том, что заявления на кредит выполнены законными владельцами паспорта, а также записи скрытых камер видеонаблюдения, фиксировавших процедуру оформления кредитов.

4. *Использование юридических лиц* (*фирм-однодневок*) для организации хищения денежных средств банка под видом организации потребительского кредитования.

Механизм обмана в таких случаях заключается в выполнении ряда подготовительных действий в виде учреждения фиктивной торговой организации, аренды помещения, покупки незначительного количества товаров (для оформления витрин) и заключения соответствующего договора об участии в коммерческом кредитовании с банком. Затем банку представляются данные о якобы заключенных кредитных договорах. Время действия «фирмы» ограничено наступлением срока первого платежа в счет погашения кредита. После перечисления денег на счет «фирмы» они обналичиваются и присваиваются, а сама организация исчезает.

В марте 2006 г., используя описанный выше способ, группа мошенников учредила под видом некоего ООО в г. Пятигорске Ставропольского края фирму-однодневку, открыла расчетный счет, взяла в аренду помещение, закупила компьютерную технику и заключила договор об участии в потребительском кредитовании с одним из коммерческих банков. Не опускаясь до прямого общения с потенциальными заемщиками, мошенники сфабриковали более тысячи подложных кредитных договоров. Для этого они использовали базу данных о реквизитах паспортов и фотографии местных жителей. Содействие группе оказывал сотрудник банка. В результате преступных действий сообщникам удалось похитить из средств, перечисленных банком на цели потребительского кредитования, более 8 млн руб.[1]

Мошенничество в сфере потребительского кредитования, первоначально характерное для Москвы и Московской области, в настоящее время получило широкое распространение во всех регионах России. За 2005 г. по фактам хищения физическими лицами средств «Русского Стандарта» в Омской области было возбуждено 108 уголовных дел. Десятки уголовных дел по фактам мошенничества, совершенных указанным способом в 2006 г. возбуждены в Республике Башкортостан, во Владивостоке, Краснодарском крае, Оренбургской, Саратовской, Рязанской и других областях.

Меры обеспечения безопасности в процессе потребительского кредитования

Даные меры являются составной частью общих мер обеспечения безопасности кредитных операций, о которых речь пойдет ниже. В то же время они имеют определенную специфику, предопределенную особенностями технологии оформления потребительского кредита.

[1] Пятигорская лавка мошенников // Парламентская газета. 2006. 24 нояб.

К числу традиционных способов определения надежности заемщиков от тся проверка подлинности предоставленных сведений и документов. Ча всего в качестве документов, удостоверяющих личность, мошенники ис ьзуют поддельный паспорт (иногда военный билет и другие документы) ичными способами подделки паспорта являются полная либо частична ена фотографии владельца документа и замена листов документа. Призна замены фотографии является несовпадение оттиска печати, след разреза фотографии, видимый на просвет, следы клея и удаления ламината, следы ены листов (в виде несовпадения серии и номера вставленного листа с ре зитами других листов). В отдельных случаях реквизиты листов паспорт еняются путем срезания, дорисовки и вклейки новых цифр. Выявлени занных признаков не требует специальной подготовки и сложного обору ания (достаточно воспользоваться лупой). О подделке паспорта могут сви ельствовать логические противоречия в тексте: между записями о дате ро ния и датой выдачи паспорта (дата выдачи паспорта свидетельству ом, что документ был «выдан» до достижения лицом срока получения пас та); расхождение между местом выдачи паспорта и местом 1-й регистра (по правилам они должны совпадать).

Несмотря на высокую вероятность обнаружения подделки, получение по бительских кредитов по фальшивым паспортам — явление весьма распро ненное. Летом 2006 г. некто М. сумел получить кредиты на приобретени аров в торговых точках Москвы по трем поддельным паспортам, в которы а вклеена его собственная фотография (об этом свидетельствовали ксеро ии предъявлявшихся паспортов). Во всех трех паспортах местом регистра был указан несуществующий адрес. Именно это совпадение и привел имке мошенника, поскольку один из банков вносил в свои «черные спи » не только фамилии заемщиков, но и места их регистрации.

Признаком подделки трудовой книжки, например, может стать выполне записей с якобы различных мест работы одним и тем же почерком.

В качестве нетрадиционных способов определения надежности заемщика ользуются приемы оценки, получившие в английском языке название ско г (*scoring* — подсчет, вычисление очков сообразно с правилами конкретной ы) и профайлинг (*profiling* — краткий биографический очерк).

Применяемые банками методики скоринга, как правило, представляют со специальные программы, позволяющие сопоставлять доходы и расходы щика, делать вывод о том, сколько он может платить. Клиент заполняет ету, в которой указывает место работы, состав семьи, образование и проч. каждому параметру он попадает в определенный диапазон, в соответствии торым ему присваиваются баллы. Сумма баллов определяет «кредитоем ь» заемщика. На основе этого банк рассчитывает максимальную сумму

По данным Ассоциации российских банков, поддельные паспорта и справки о доходах фи ких лиц предъявляются 30% кандидатов на получение кредита.

кредита. Настройки скоринга у каждого банка индивидуальны: они нарабатываются с опытом, корректируются с учетом российской специфики. С учетом различия применяемых методик одному и тому же заемщику в разных банках могут быть предложены совершенно разные условия[1].

Кроме оценки документальных данных, сотрудникам, оформляющим кредит, рекомендуется обратить внимание на поведение заемщика; его внешний вид; на наличие (отсутствие) расхождений в информации о заемщике, отраженной в различных документах; соразмерность доходов клиента с размерами кредита и стоимостью потенциальной покупки. Само собой разумеется, следует тщательно проверить личные документы на предмет выявления признаков подделки.

С 2007 г. возможности проверки банками подлинности паспортных данных заемщика значительно расширились за счет организации взаимодействия с Федеральной миграционной службой Российской Федерации (далее — ФМС РФ). ФМС РФ предоставляет банку возможность получить через свой официальный сайт (www.fms.gov.ru) в автоматическом режиме сведения:

- о соответствии указанных заемщиком паспортных данных информации, содержащейся в базе данных ФМС РФ;
- о лицах, использующих утраченные, похищенные или поддельные паспорта;
- о лицах, находящихся в розыске.

Ответ ФМС РФ на запрос банка включает в себя следующие сведения:

1. Фамилия.
2. Имя.
3. Отчество.
4. Дата рождения.
5. Серия, номер паспорта с указанием статуса документа:
   - действителен;
   - выдан незаконно или в нарушение порядка и подлежит изъятию;
   - утрачен;
   - утерян или похищен бланк паспорта.
6. Адрес регистрации с расшифровкой статуса владельца:
   - умер;
   - убыл за продлением московской регистрации;
   - проживает в Москве постоянно;
   - проживает в Москве временно;
   - проживает в Московской области постоянно;
   - проживает в Московской области временно;
   - проживал в Москве временно (закончилась временная регистрация);
   - проживал в Московской области временно (закончилась временная регистрация).

[1] *Маркевич Т.* Как минимизировать потери в области потребительского кредитования коммерческого банка // Бизнес-разведка. 2006. № 4 (23).

7. Сведения о нахождении субъекта в розыске:
   - не в розыске;
   - находится в федеральном/местном розыске.

Время получения ответа на запрос банка составляет не более двух минут.

Визуальная оценка поведения и внешнего облика потенциального заемщ , проведенная по четким критериям, разработанным банком, позволя большой долей вероятности выявить «обстоятельства, свидетельствующ том, что предоставленная заемщику сумма не будет возвращена» (ст. 8 РФ) и отказаться от предоставления кредита.

Такими обстоятельствами следует считать, например, нервное поведени способность внятно ответить на вопросы сотрудника банка, обращен ответами к сопровождающим лицам, порванная обувь и одежда, нахожд е в состоянии опьянения и т. п. О причастности лиц, сопровождающ лиентов», к мошенническим группировкам может свидетельствовать их н нократное появление в точках кредитования торговой организации с ра ими «заемщиками».

Эффективным средством предупреждения потерь от мошенничества в сф потребительского кредитования является ведение «черных списков» ли горым по тем или иным причинам было отказано в получении потреб ьского кредита. Постоянный анализ и обмен этими данными позволят и кать ошибок при повторном обращении «заемщика» в один и тот же, ли ругой банк.

Во избежание мошеннических действий со стороны торговых организ й, предлагающих сотрудничество в целях потребительского кредитовани дует проводить предварительную и текущую проверку предполагаем ействующих партнеров по методике оценки надежности юридических ли исанной ниже (включая негласный выезд сотрудников банка в торгов ки и непосредственное наблюдение за процессом оформления кредитов).

Способы мошенничества в сфере кредитования юридических лиц

При совершении мошенничества указанным выше способом завладени ежными средствами совершается от имени юридического лица. Тако ем позволяет значительно увеличить сумму займа, а также существенн рудняет раскрытие подлинных намерений мошенников и привлечени к уголовной ответственности, поскольку принятие обязательств и распоря ие имуществом потерпевших осуществляется под видом обычной финан о-хозяйственной деятельности.

Нередко в целях обмана в кредитной сфере совершается еще одно смежно ошенничеством преступление — лжепредпринимательство. Согласно ст. 173 РФ лжепредпринимательство заключается в создании коммерческой орга ации без намерения осуществлять предпринимательскую или банков ю деятельность с целью получения кредитов, освобождения от налогов,

извлечения иной имущественной выгоды или прикрытия запрещенной деятельности, причинившей крупный ущерб гражданам, организациям или государству.

Основные способы обмана и злоупотребления доверием, которые при этом применяются, включают в себя предоставление банку ложной информации:

а) о будущем заемщике;

б) о подлинных целях будущего займа;

в) о предмете и условиях обеспечения предполагаемой сделки.

Наиболее распространенными видами ложной информации о предполагаемом заемщике являются несоответствующие действительности сведения и документы: о правоспособности и дееспособности фирмы и ее репутации; о личности ее руководителя (представителей), наличии у них соответствующих полномочий на получение кредита; о финансовых возможностях фирмы-заемщика (способности заработать средства для погашения долга, размерах вложения в дело собственного капитала).

Одним из типичных приемов, применяемых для присвоения денежных средств, являются случаи умышленного нарушения процедуры заключения кредитного договора, в частности оформление и получение кредита лицом, не наделенным соответствующими полномочиями. Эта уловка позволяет мошенникам впоследствии отказаться от возврата полученных сумм на формальных основаниях, а претензии кредитора перевести из сферы действия уголовного закона в разряд гражданско-правового спора, имеющего мало перспектив на возмещение ущерба потерпевшему.

Для создания видимости финансовой устойчивости и надежности заемщика, достаточности вложения собственного капитала в кредитуемое дело мошенники зачастую идут на подлог балансовых счетов, оборотно-сальдовых ведомостей, расчетно-кассовых документов и другой документации первичного учета.

В августе 2006 г. Следственное управление УВД Томской области направило в суд уголовное дело по фактам кредитного мошенничества. Как установлено следствием, обвиняемый, выступая в качестве директора двух магазинов, предоставлял банку с целью получения кредитов фиктивные справки о финансовом положении торговых организаций. По сравнению с данными отчетов, направляемых в налоговую инспекцию, в справках для получения банковского кредита сумма собственных средств — активов и прибыли была увеличена на десятки миллионов, а заемные средства и кредиторская задолженность уменьшены на 70%. Не удосужившись провести элементарную проверку путем сопоставления документов, 4 коммерческих банка перечислили на счета магазинов кредитных средств на общую сумму 26 млн руб. Подделки были обнаружены лишь после того, как истекли сроки возврата кредитов[1].

[1] Томские новости. 2006. 15 авг.

Своеобразный «рекорд» по числу кредитов, полученных мошенническим
тем, поставил в 2006 г. некий башкирский предприниматель. Как сообщил
спубликанская прокуратура, используя фиктивные документы, он сумел за
ючить 300 кредитных договоров с коммерческими банками Ишимбая, Уф
Стерлитамака, задолжав им в общей сложности 43 млн руб., после чег
ыился. Суд признал предпринимателя виновным в совершении преступле
й, предусмотренных ст. 159 УК РФ (мошенничество) и ст. 327 УК РФ (под
ка документов), и приговорил его к шести годам лишения свободы[1].

Обман, связанный с предоставлением банку ложной информации о под
ных целях будущего займа, о предмете и условиях его обеспечения, чащ
го заключается в несоответствующих действительности сведениях о наме
иях заемщика использовать полученный кредит для проведения реально
изводственной или коммерческой деятельности (фальшивые бизнес-пр
ы и планы), в подложных документах об обеспечении кредита — о вторич
источниках погашения долга (о предмете залога и правах на него залого
еля, о банковской гарантии, поручительстве, о наличии договора страхова
и условиях страхования), предусмотренных в кредитном договор
тдельных случаях несоответствующие действительности сведения о якоб
ешной деятельности заемщика распространяются через средства массово
юрмации с целью создать у кредиторов впечатление о финансовой надеж
ги потенциального заемщика.

Весьма показательными в этом плане явились действия мошенников, мас
овавшихся под вывеской некоего агрохолдинга «Русагрокапитал». В сооб
иях отечественных СМИ (введенных в заблуждение мошенниками) гене
ьный директор агропромышленного холдинга «Русагрокапитал» К. бы
ставлен «финансистом с большим опытом работы в банковской сфер
«Инкомбанк», МЕНАТЕП, Банк Москвы, МДМ-банк), собравшим ко
ду профессионалов и успешно реализовавшим проекты по модернизации
изводства». Сам агрохолдинг, по оценке СМИ, характеризовался как «про
ионально управляемая компания, перерабатывающая около 1,7 млн т
а в год, с ежегодным оборотом более 230 млн долл. и приносящая ста
ный доход своим акционерам»[2].

Пассированная информационная обработка потенциальных потерпевших
олила К. обмануть более 20 крупнейших банков России.

спользуя сформированное через СМИ мнение о «Русагрокапитале» как
юцветающей» компании, К. сумел получить у этих банков кредиты на об
сумму более 100 млн долл. В качестве средства обеспечения кредитов бы
ключены договоры о залоге около 300 тыс. т, якобы принадлежащего
нгу и хранившегося на ОАО «Ржевский комбинат хлебопродуктов»

За обман кредиторов директор фирмы поплатился свободой. Федеральное Агенство Фин
ой нформации. 2006. 14 марта (http://www.buhgalteria.ru/news/9925).
Карьера. 2004. № 6 (69). Июнь (http://kariera.idr.ru.pitem=20).

зерна. По истечении сроков займа руководство «Русагрокапитала» отказалось возвращать взятые кредиты, мотивируя отказ «сложным финансовым положением» холдинга. Обнаружилось, что полученные им кредитные средства «исчезли», реальные активы «Русагрокапитала» и входящих в него организаций ничтожно малы. Упомянутых выше 300 тыс. т заложенного зерна у «Русагрокапитала» не было изначально.

В ходе проверки было установлено, что ОАО «Ржевский комбинат хлебопродуктов» никогда не осуществлял услуг по хранению зерна. Это подтвердилось «Журналами количественно-качественного учета хлебопродуктов». Договор хранения зерна на комбинате хлебопродуктов, приложенный «Русагрокапиталом» к договору залога, являлся подложным и был подписан от имени ОАО «Ржевский комбинат хлебопродуктов» самим К., не имеющим на это полномочий.

С целью избежать уголовного преследования К. и руководители входивших в холдинг организаций пытались перевести разбирательство в русло арбитражного спора. Уголовное дело по факту мошенничества было возбуждено лишь после его широкого обсуждения на слушаниях в Госдуме[1].

Другим способом обмана может быть использование поддельных документов на реально существующее имущество, принадлежащее другим лицам; поддельные банковская гарантия, поддельное поручительство, страховое свидетельство.

Так, например, в 2004 г. некий бизнесмен из Новороссийска, имевший положительную деловую репутацию, получил мошенническим путем в виде кредитов от местных банков более 60 млн руб. В качестве залога при заключении кредитных договоров банками были приняты фальшивые документы о праве собственности мошенника на семь тысяч кубометров первосортного леса, 900 путевок в пансионаты Сочи и Геленджика, а также на большое количество металла. Все перечисленное имущество, как выяснилось впоследствии, существовало реально, однако принадлежало другим собственникам. Фальшивые документы на залоговое имущество были отпечатаны в одной из типографий города.

Обращает на себя внимание то обстоятельство, что каждый раз при подготовке к заключению договоров представители банков выезжали на места. Однако мошенник встречал проверяющих на месте нахождения предлагаемого к залогу имущества и участвовал совместно с работниками банка в его осмотре. Обману способствовало также высокое качество изготовления поддельных документов на предметы «залога». Получив в кредит солидные суммы якобы на ремонтные работы, новороссиец переводил их на семь разных счетов в московских банках. В день получения денег договор о ремонтных работах расторгался, а деньги обналичивались[2].

[1] *Гуркина Е.* На зерновом рынке России совершена «афера века» // Крестьянская Россия. 2004. 26 июля.

[2] *Лубинец Е.* Преступление по Шарлю Перро: мошенник обобрал банки на 60 миллионов рублей // Российская газета (Кубань). 2004. № 3462. 22

Ложная информация о предмете залога может заключаться в несообщени
огодержателю (вопреки требованию ст. 342 ГК РФ) сведений о наличи
е существующих залогов данного имущества. В таких случаях требовани
огодержателя (кредитора), в соответствии со ст. 342 ГК РФ, удовлетвор
ся лишь после удовлетворения требований предшествующих залогодерж
ей. Умолчание о предыдущих залогах позволяет мошенникам многократ
ладывать одно и то же имущество и присваивать суммы, намного превы
ющие размеры залога без опасения быть привлеченными к уголовной о
ственности.

Мошенничество может заключаться в несанкционированной продаже кр
ором заложенного имущества и присвоении вырученных денежных средст
ом 2006 г. Следственное управление при ГУВД Пермского края направи
д уголовное дело по факту кредитного мошенничества, совершенного н
М. Последний, получив кредит в сумме 4 млн руб. под залог имущест
главляемой им компании, продал заложенное имущество, присвоил креди
крылся[1]. Правоохранительной практике известны также случаи инсцени
ки краж заложенного имущества.

В числе уловок, делающих недействительным договор поручительства, м
быть умышленное умолчание в его тексте о том, за исполнение како
зательства дано поручительство. С таким случаем столкнулся коммерч
й банк, предоставивший предприятию кредит под гарантийное письм
мы. В нем гарант поручился за возврат ссуд, которые будут выданы заем
ку банком-кредитором до указанного в письме срока. Однако в договор
учительства отсутствовали данные о том, по какому кредитному договор
о поручительство и какова сумма ссуды, подлежащая передаче заемщик
к информировал поручителя о принятии его гарантийного письма. Пр
смотрении требования банка о возврате ссуды, предъявленного к заемщи
гаранту, арбитражный суд в иске отказал, отметив, что договор поручи
ства не содержит данных об обязательстве, в обеспечение которого дан
учительство, и поэтому его следует считать незаключенным[2].

Следует иметь в виду, что гарантийное обязательство будет недействитель
(не возникает) и при несоблюдении такого существенного условия его
ючения, предусмотренного ст. 374 ГК РФ, как указание срока, на кото
выдана гарантия.

Меры обеспечения безопасности кредитных операций

иск понести убытки от мошенничества в сфере кредитования может быть
ственно снижен путем осуществления ряда предупредительных мер,

[1] Новости Бухгалтерии. 2006. 13 окт.

[2] Обзор практики рассмотрения споров, связанных с исполнением и расторжением кредитоговоров. Письмо Высшего Арбитражного Суда РФ от 26 января 1994 г. № ОЩ-7/О.

которые осуществляют служба внутреннего контроля, юридическая служба и служба безопасности банка.

Названные службы банка должны, как минимум, выполнить следующие действия.

1. Проверить подлинность сведений и документов, удостоверяющих право организации заключать договор займа в объеме и на условиях, предусмотренных проектом договора. Это требование не было выполнено при заключении кредитных договоров между банками-кредиторами и упоминавшимся выше «Русагрокапиталом». В процессе расследования кредитного мошенничества были исследованы договоры о принятии на хранение ОАО «Ржевский комбинат хлебопродуктов» зерна, якобы поступившего от входящего в «Русагрокапитал» ОАО «Финистхлеб». Напомним, что указанного зерна (предмета залога) в природе не существовало. В то же время обнаружилось, что договоры хранения мифического зерна были подписаны от имени ОАО «Ржевский комбинат хлебопродуктов» генеральным директором «Русагрокапитал» К., который никаких правовых оснований на их заключение не имел. Более того, некоторым банкам-кредиторам в качестве документального подтверждения наличия залога вместо договоров хранения были предъявлены договоры переработки зерна, подписанные тем же К.

Следует проверить также подлинность документов, удостоверяющих личность руководителя или представителя организации, наличие у них соответствующих полномочий на получение кредита, правильность оформления доверенности и т. д. В особо важных случаях будет нелишним снять ксерокопии с предъявленного паспорта и доверенности, попросить снабдить доверенность заверенной фотографией уполномоченного лица.

При проверке информации о руководителе предприятия-заемщика необходимо выяснить, не является ли данное лицо учредителем или руководителем других фирм. Если, например, выяснится, что заемщик «руководит» рядом фирм, можно почти наверняка подозревать, что вы имеете дело с подставным лицом. Сомнения в надежности заемщика возникают и в тех случаях, когда он числится владельцем или руководителем крупного предприятия, но при этом не владеет ни квартирой, ни машиной, ни акциями предприятий.

При исследовании документов потенциального заемщика необходимо обращать внимание на такие признаки фиктивности, как логические несоответствия в тексте. Эти несоответствия могут иметь формы взаимоисключающих записей в содержании одного документа либо противоречий в содержании нескольких взаимосвязанных документов.

2. Получить сведения, подтверждающие реальное существование организации заемщика, путем изучения уставных документов, сведений из налоговых органов и др. Установить, соответствует ли кредитуемая сделка законодательству и уставным документам заемщика. При выполнении указанных проверочных действий желательно не ограничиваться только изучением документов. Дополнительные сведения о реальности существования организации-заемщика

жет дать информация о наличии у фирмы постоянных производственны
кладских помещений, а также об объемах товаров или продукции, которы
располагает фирма.

3. Установить способность заемщика заработать средства для погашени
га и возвратить кредит. С этой целью анализируются сведения о продол
тельности присутствия фирмы на рынке товаров и услуг, наличие положи
ьных экономических показателей. Изучаются кредитная история (полу
ли заемщик кредиты в других кредитных организациях, не допускал л
рушений при их получении; как использовались деньги, полученные в к
тве кредита; не было ли проблем с возвратом денег банку) и репутаци
еловом мире партнеров (контрагентов, кредиторов, банков).

4. Проверить достаточность вложения собственного капитала заемщи
редитуемое дело. Об этих показателях можно судить по данным балансовы
омостей, расчетно-кассовых документов и другой документации первичн
чета. Соответствующим подтверждением добросовестности намерений з
щика может служить наличие у него достаточных объемов реального това
продукции.

5. Провести тщательную юридическую и фактическую оценку подлинно
документов о вторичных источниках погашения долга (договора о залог
нтии, поручительства, страхового свидетельства). В частности, проверит
очное соответствие нормам гражданского законодательства, наличие воз
ных признаков материального и интеллектуального подлога. Выяснить
жен ли факт выдачи гарантийного письма, страхового свидетельств
оч. в соответствующих документах поручителя. При этом следует учиты
имевшие место случаи, когда недобросовестные коммерческие банки
являли фальшивыми реально выданные ими гарантии.

. Получить четкие ответы относительно целей испрашиваемого кредита
кже сведения, раскрывающие содержание и механизм предполагаемог
тракта по всей технологической цепочке от момента производства до дос
и к месту реализации; о характере деятельности предполагаемых контр
тов потенциального заемщика; о возможности контрагентов поставить за
ику товар ожидаемой номенклатуры и качества в названные сроки, вид
личество транспортных единиц, которые предполагается использовать,
чие соответствующих договоров на доставку товара (сырья). Нелишними
т сведения о наличии у заемщика в собственности производственных
адских помещений, товаров в обороте или готовой продукции.

оучительным примером просчета при проверке заявленных целей полу
я кредита стал случай в одном из московских банков в 2005 г. Согласно
ставленному заявлению, кредит предназначался для замены лифтов
тинице «Россия». В качестве вторичного источника погашения долга (за
предлагались приобретаемые лифты. Рассмотрев материалы, банк при
решение о выдаче кредита. От крупного ущерба банк спасло стечение

обстоятельств: в период незначительной задержки с выдачей кредита стало известно о предстоящем сносе гостиницы[1].

После заключения кредитного договора контролировать ход его исполнения с целью своевременного выявления обстоятельств, могущих препятствовать возврату кредита. При возникновении таких обстоятельств принимать меры к минимизации ущерба.

Примером просчетов в организации контроля за исполнением кредитного договора может служить случай исчезновения 89 млн долл. из 150, выделенных Московским банком Сбербанка России в 1998 г. ОАО «Кейстоун» в качестве кредитной линии на строительство многофункционального офисного комплекса «Царев сад» на Софийской набережной в Москве. Афера завершилась в 2001 г. Как выяснилось в ходе следствия, кредит Сбербанка расхищался с участием российских и иностранных финансовых структур. Схема воровства была предельно простой: в течение трех лет в Сбербанк поступали счета на оплату строительных работ, которые на самом деле не проводились. А деньги переводились в зарубежные банки, в том числе и на счет фирмы, зарегистрированной в Лихтенштейне. Дело о хищении денег было возбуждено по заявлению руководства Сбербанка, которое (по прошествии трех лет) обратило внимание на подозрительно медленные темпы строительства «Царева сада».

Следствием был установлен факт грубого нарушения уполномоченными лицами Сбербанка специального Положения, согласно которому банк должен был вести текущий контроль использования выделенных «Кейстоуну» кредитных средств. Тем не менее, судьбой 150-миллионного кредита в Сбербанке озаботились лишь после того, как он был выплачен полностью[2].

Источники документальной информации, позволяющей проверить факт существования организации заемщика, подлинность сведений и документов, удостоверяющих право организации заключать договор займа, установить способность заемщика заработать средства для погашения долга, а также подтвердить факт принадлежности заемщику имущества, предлагаемого в качестве залога описаны в главе 9 «Информационное обеспечение безопасности банка».

5.2. Хищения денежных средств с незаконным использованием пластиковых карт

Банковская пластиковая карта представляет собой финансовый инструмент платежной системы, позволяющий держателю осуществить операции по его счету как с целью снятия наличных денег или оплаты товаров и услуг, так и для получения информации о состоянии данного счета.

---

[1] Финанс. 2006. № 39 (176). Окт. С. 28.

[2] Найдена часть кредита Сбербанка на строительство «Царева сада» // Независимая газета. 2003. 28 апр.

Правовое положение пластиковых карт в сфере денежного обращения о
еделяется договором банковского вклада (ст. 834 ГК РФ). По этому догово
на сторона (банк), принявшая поступившую от другой стороны (вкладчик
ли поступившую для нее денежную сумму (вклад), обязуется возвратить су
у вклада на условиях и в порядке, предусмотренных договором.

Пластиковая карта в данном случае является средством идентифика
держателя, подтверждающим право на осуществление операций по банко
кому вкладу. Не обладая сами по себе конкретной стоимостью (затра
на их изготовление в расчет не берутся в силу их относительной незначител
ости), пластиковые карты не могут быть предметом хищения в правовом п
нтии этого слова. Противоправное завладение пластиковыми картами п
личии соответствующего умысла квалифицируется как приготовление к х
ению.

Согласно общепринятому подходу, пластиковые карты принято класси
ировать по механизму и виду проводимых расчетов, по характеру исполь
ния, по способу записи информации на карту, по принадлежности к учре
нию-эмитенту, по сфере, территории и времени использования и т. д.[1]

Механизм расчетов с использованием пластиковых карт может включа
себя два вида систем: двусторонние (для оплаты товаров и услуг в конкре
ой организации или предприятии, выдавшей карту) и многосторонние (п
воляющие оплачивать товары и услуги любого числа организаций и предпр
ий, принимающих эти карты). С целью оптимизации затрат на обслужива
ржателей пластиковых карт, выпустивший их банк-эмитент, как правил
ключает договоры с другими банками (банками корреспондентами). По
ледние обслуживают держателей банка-эмитента через установленны
их помещениях банкоматы.

По видам платежных схем пластиковые карты делятся на кредитные, ра
тные и дебетные.

Кредитная схема позволяет владельцу карты пользоваться кредитом пр
плате товаров и услуг, а также получать в кредит определенное количест
личных денег (размер одного платежа по кредитной карте ограничивает
учетом состоятельности клиента).

Расчетная схема является частным случаем кредитной. Согласно договору
ржатель карты должен в установленный срок оплатить всю сумму произве
нных в долг расходов.

Дебетная схема дает возможность держателю осуществлять платежные опе
ции в пределах остатка денежных средств на собственном счете.

По характеру использования пластиковые карты делятся на индивидуаль
ые, семейные и корпоративные. Два первых вида предполагают использова
ие держателями собственного счета физического лица. Корпоративная ж

[1] *Гамза В. А.* Настольная книга предпринимателя. Банковские операции, финансовые инст
менты, консалтинговые услуги: учеб.-практ. пособие. М.: Изопроект, 2004. С. 261–272.

карта позволяет ее держателю (физическому лицу) проводить операции по счету юридического лица.

В современной отечественной практике информация на пластиковую карту наносится путем графических записей, термической обработки и давления, кодирования на магнитной полосе, установки электронного чипа (микропроцессора и памяти, обеспечивающих более высокий уровень защиты информации и принципиально иную технологию обслуживания по сравнению с магнитной полосой).

Реквизиты пластиковой карты включают в себя наименование и логотип эмитента (банка или другой выпустившей ее организации), номер карты, срок ее действия, фамилию, имя и отчество (либо инициалы) ее владельца. Образец подписи владельца карты и адрес эмитента располагаются на внутренней стороне карты. Магнитная полоса или чип помещаются между внешней и внутренней сторонами карты.

Среди пластиковых карт, эмитированных в России зарубежными банками, наиболее распространены «VISA», «Eurocard/MasterCard», «Europay-Card» и «Europay Intern». Более 230 банков России являются участниками Всемирной межбанковской финансовой телекоммуникационной сети (СВИФТ), созданной для повышения эффективности международных валютно-кредитных и расчетных операций, в том числе с использованием одноименных пластиковых карт[1].

Удобства хранения, перемещения и использования банковских пластиковых карт, возможность проведения операций по счету на весьма значительные суммы в любое время и без личного контакта с работниками банка сделали эти карты весьма привлекательными не только для законопослушных граждан, но и для криминальных элементов. В настоящее время на хищения с использованием поддельных банковских карт приходится самая большая доля потерь платежной системы.

Хищения денежных средств банка, совершаемые с использованием пластиковых карт, с позиций Уголовного кодекса РФ рассматриваются как *мошенничество*, правовые признаки которого описаны в предыдущем параграфе.

По способу совершения они условно делятся на три большие группы:

1) хищения с использованием подлинных карт, утраченных владельцами (в результате утери либо неправомерного завладения злоумышленниками);

2) хищения с использованием поддельных карт;

3) хищения с использованием подлинных карт, оформленных злоумышленниками в установленном порядке.

Способы неправомерного завладения банковскими картами. По сообщениям правоохранительных органов, неправомерное завладение банковскими пластиковыми картами в целях хищения денежных средств стало устойчивой

[1] Международные валютно-кредитные и финансовые отношения: учеб. / под ред. Л. Н. Красавиной. 2-е изд., перераб. и доп. М.: Финансы и статистика, 2000. С. 418

...зновидностью деятельности организованных преступных групп. Следствие ...истематически выявляет сети скупщиков самих карт, а также украденных ...их использованием товаров.

Как правило, карты похищаются тайно (нередко у заранее выбранных дер...ателей) путем карманных краж либо другим способом (кражи из квартиры, ...томашины, из почтовых отправлений при пересылке карты по почте и даже ...ийства). Согласно зарубежной статистике хищения денег и товаров с ис...льзованием украденных пластиковых карт составляют более 70% от общего ...сла случаев неправомерного использования карт. Представляется, что ...исло «утраченных» статистика включает пластиковые карты, похищенные ...и обстоятельствах, не очевидных для владельца.

Процедура блокирования счета по похищенной (утраченной) карте может ...ять до трех суток. Именно в это время использование карты для получения ...аров, услуг или наличных денег наиболее вероятно. Похищению карт в оп...еленной мере способствует своеобразие психологии клиентов, проявляю...х к ним меньше внимания, чем к наличным деньгам.

Показательный случай заранее спланированного завладения кредитно...той и ее последующего использования для хищения денежных средств ...изошел в июне 2005 г. в Екатеринбурге. Карта была украдена вместе с су...кой, в которой она находилась. Пропажа была обнаружена сразу же. ...7 ч 02 мин. потерпевшая Д. сообщила о ней в обслуживающий банк «Се...ная казна». В 17 ч 05 мин. банк уведомил ее о принимаемых мерах по бло...ованию счета. Однако похитители оказались проворнее банковских работ...ов. Как выяснилось впоследствии, в период между 15 ч 04 мин. и 15 ...ин. со счета Д. в несколько приемов были сняты 10 тыс. долл.

Подделка банковских пластиковых карт является преступлением, предус...ренным ст. 187 УК РФ. В соответствии с названной статьей основанием ...наступления уголовной ответственности является «изготовление в целях ...а или сбыт поддельных кредитных либо расчетных карт, а также иных ...ежных документов, не являющихся ценными бумагами».

...татья 187 УК РФ устанавливает наказание за совершение двух самостоя...ных действий:

изготовление с целью сбыта;

сбыт поддельных кредитных либо расчетных карт, а также иных пла...ых документов, не являющихся ценными бумагами.

...редметом преступления, ответственность за которое предусмотрена ч. 1 ...7 УК РФ, являются: кредитная или расчетная (дебетовая, дисконтная, ...ронная телефонная, электронная проездная и т. д.) карта; иные платеж...окументы, не являющиеся ценными бумагами.

...готовление указанных выше карт и иных документов может быть пол...ибо частичным. Под сбытом в данном случае следует понимать выпуск ...редметов в обращение (непосредственное использование или передачу

другим лицам с целью использования). Способы их изготовления и сбыта рассматриваются ниже.

Максимальное наказание за совершение преступления, предусмотренного ч. 1 ст. 187 УК РФ, — лишение свободы на срок до шести лет.

Часть 2 ст. 187 УК РФ предусматривает ответственность за изготовление или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами, совершенные неоднократно или организованной группой.

Максимальное наказание за совершение преступления, предусмотренного ч. 2 ст. 187 УК РФ, — лишение свободы на срок до семи лет.

По способам подделки фальшивые карты дифференцируются по трем основным видам:

а) полностью поддельные карты, внешне имитирующие подлинные;

б) карты, подделанные путем внесения изменений во внешние реквизиты;

б) карты, подделанные путем перекодирования информации, содержащейся на магнитном носителе. В последнем случае внешние реквизиты и данные магнитного носителя могут не совпадать.

Для перекодирования может быть использована подлинная карта банка, оформленная с соблюдением установленных формальных процедур после внесения минимально необходимой денежной суммы. В качестве владельца счета и карты указывается подставное лицо либо лицо, утратившее паспорт. После этого преступники изменяют информацию на магнитной полосе карты внося кодовый номер, фамилию, имя и отчество держателя с более солидным счетом. Кроме того, может меняться информация, *эмбоссированная* на лицевой стороне карты, и подделываться подпись законного держателя. Следует отметить, что процесс изменения преступниками эмбоссированной информации неизбежно оставляет следы, которые могут быть выявлены не только экспертным путем, но при внимательном визуальном осмотре карты. Признаками подделки в данном случае являются:

- волнообразные следы и искажение эмбоссированных надписей от термообработки (наличие вмятин на шрифте, смещение цифр и букв);
- наличие замененных путем переклейки букв и цифр, эмбоссированных в плоскости карты.

В ряде случаев преступники используют поддельные карты, не имеющие детального внешнего сходства с подлинными (так называемый белый пластик), однако снабженные фальсифицированными магнитными носителями.

Подготовка к хищению с использованием похищенных и поддельных пластиковых карт включает в себя добывание информации о кодах и номерах карт действительных клиентов. Для этого преступники совершают целенаправленные действия. Осуществляют перехват информации с применением технических средств (подсматривание номера набираемого кода с использованием микровидеокамер, считывание номера кода, конфигурации карты и остатка денег на счете путем установки на щель для карты специальных

итывающих рамок «скиммеров» от английского «skim» («снимать»), уст
вки на клавиатуру банкомата специальных накладных панелей, фиксиру
их вводимые клиентом цифры, и даже путем установки фальшивых банко
тов). В конце декабря 2006 г., установив накладные панели на банкомат
нка ВТБ-24 в Москве, мошенники сняли информацию с 9 тыс. карт. Изго
вленные с использованием добытых сведений подделки использовали
границей. На банкоматы ВТБ-24 обрушился поток хищений, вынудивш
нк заблокировать несколько тысяч пластиковых карт.

В ряде случаев мошенники выведывают информацию о карте путем зама
рованного опроса ее владельца либо других осведомленных лиц. Вовлека
незаконное получение сведений о картах работников банков и организаци
ющих непосредственный доступ к сети и базам данных.

В 2002 г. французские власти предъявили обвинение в мошенничест
вшему начальнику службы информационной безопасности процессингово
мпании Union Card в России Г., который в течение нескольких лет обесп
вал группу международных преступников информацией о пластиковых ка
иностранцев, обслуживавшихся процессинговым центром Union Card. О
я сумма похищенных денег осталась неизвестной, однако о масштабах пр
тной деятельности свидетельствует тот факт, что одна лишь Europ
изнала «скомпрометированными» около 65 тыс. карт, побывавших в Ро
и.

Полученная от Г. информация использовалась для изготовления упомина
гося «белого пластика». Выйти на след мошенников помогло случайное з
жание одного из них при попытке получить деньги в банкомате по «белом
истику»[1].

Способы хищения с использованием пластиковых карт

*Использование злоумышленниками пластиковых карт, похищенных у их вл
ьцев.* В основе всех способов мошенничества с использованием пластиковы
т лежит незаконное списание денег со счетов клиента в банке-эмитент
о осуществляется путем несанкционированного вмешательства в применя
е банком процедуры расчетов, независимо от того, осуществляются ли он
основе бумажных либо электронных носителей.

Широко распространенным способом хищения денег с использование
линных пластиковых карт является *овердрафт* с мошенническим примене
м карты.

Под овердрафтом понимается форма краткосрочного кредита, предостав
ие которого осуществляется списанием средств по счету клиента банка
езультате чего образуется дебетовое сальдо. Овердрафт предоставляется
более надежным клиентам по договорам, в которых устанавливаются

[1] *Буйлов М.* Карточке — место // Коммерсантъ. 2002. № 184 (2553). 10 окт.

максимальная сумма овердрафта, условия предоставления кредита, порядок погашения[1].

Указанный способ мошенничества применяется в системах *банк-мерчант* (предприятие торговли или сферы услуг, принимающее банковские карты к обслуживанию), использующих для фиксации факта списания денег со счета бумажные носители (*слипы* — расходные документы, содержащие оттиск реквизитов карты и подпись ее владельца). Мошенник, располагая кредитной картой с незначительной суммой на счете, в короткое время проводит как можно больше операций по выплате денег со счета, незаконно завладевая деньгами и товарами. Расчеты злоумышленников основаны на том, что банки и магазины сдают слипы (квитанции) в банк раз в две недели, поэтому факт хищения денег по карте обнаруживается со значительным опозданием.

Овердрафт с мошенническим применением карты может быть совершен и в тех мерчантах, где для списания денег со счета используется электронная система банк-мерчант. Однако в таких случаях время между совершением хищения и его обнаружением значительно сокращается.

Использование злоумышленниками поддельных пластиковых карт. Поддельные пластиковые карты (кредитные и дебетовые) используются для получения денег, оплаты товаров и услуг с реально существующих счетов владельца подлинной карты.

В отдельных случаях хищения денег по поддельным картам с реквизитами карты подлинного владельца совершаются сотрудниками организаций, осуществляющих обслуживание по кредитным картам. Известны случаи, когда для совершения указанного вида хищений специально создавались фирмы (торговые организации). Похитив определенную сумму денег по поддельным картам клиентов, организаторы мошенничества скрывались. Информацию о кодах клиентов и номерах их счетов мошенники получают также в результате специальных манипуляций, осуществляемых в процессе оплаты владельцем карты товаров или услуг.

Использование подлинных пластиковых карт, заведенных злоумышленниками для совершения хищений. Карта, оформленная с соблюдением установленных формальных процедур, чаще всего используется злоумышленниками в качестве инструмента получения денег со специально открытого дебетового счета. Деньги на указанный счет незаконно переводятся с других счетов путем непосредственного вмешательства злоумышленников в операционную систему банка, а затем изымаются через банкомат либо реализуются путем получения товаров или услуг.

Указанный способ обычно применяется компьютерными взломщиками (чаще всего из числа работников банка — настоящих или бывших). Карта оформляется на подставное лицо либо на имя лица, утратившего паспорт.

[1] Финансово-кредитный энциклопедический словарь / под общ. ред. А. Г. Грязновой. М.: Финансы и статистика. 2002. С. 672.

Механизм противоправных действий работников банка, участвующих в со-ршении хищений, с использованием пластиковых карт. Среди противоправны-йствий сотрудников банка с использованием пластиковых карт приня-личать: неправомерное увеличение кредитного лимита на конкретную ка-и последующее похищение денежных средств; несанкционированную уст-зку в авторизационной системе специального статуса счета, позволяюще-пределенных пределах снимать средства с карты (разновидность кредитн-лимита); несанкционированное пополнение счета карты; выпуск пара-льной карты-двойника; несанкционированный выпуск пластиковых карт.

Хищение 12,5 млн руб. со счетов БСТ-банка в Новокузнецке совершил-ем несанкционированного выпуска пластиковых карт бывший заместите-ıальника отдела вкладов населения этого банка по пластиковым карта-За два года работы в указанной должности она оформила выдачу клиента-ıее 2 тыс. банковских карт. Отсутствие должного контроля и просчеты в о-изации работы отдела позволили П. сначала списать 13 карт как испорче-е, а затем зачислить на них указанную выше сумму. Впоследствии денеж-е средства снимались П. (и ее сожителем) через городские банкоматы.

Имея доступ к компьютерному обеспечению банка и свой персональны-юль, П. могла не только пополнять карточные счета, но и редактирова-:тупавшие к ней в электронном виде выписки о движении по ним денеж-к средств на случай документальных и электронных проверок. Хищени-)должались в течение двух лет. Начало расследованию положил факт обна-:ения недостач наличности в ряде банкоматов. Проведенная выборка запи-о выдаче денежных средств показала, что часть наличных была получен-пластиковым картам, которые клиентам не выдавались. Согласно учетны-ным, начисление и списание денежных средств по этим картам так-производилось.

Непосредственному разоблачению мошенницы способствовала архивна-еозапись одного из банкоматов, на которой был зафиксирован факт полу-ия П. денежной суммы по одной из «испорченных» банковских карт.

В отдельных случаях работники банка не гнушаются элементарным похи-нием карты, оформленной на имя клиента. В 2007 г. в Уральском федерал-ı округе была раскрыта группа мошенников, действовавших в Тюмени-ске, Кургане, Златоусте и ряде других городов. В эту группу, по данны-прокуратуры, входили менеджеры филиалов банка «Русский Стандарт-отрудники почты. Названный банк высылал кредитные карты клиентам за-ными письмами. Пин-код сообщался держателю карты по телефону посл-), как клиент называл оператору банка свои паспортные данные.

Роли участников преступной группы распределялись следующим образом-отники почты по наводке работников банка перехватывали заказные письма-редитными картами. Затем участники преступной группы посещали под ви-работников банка квартиры граждан, на имя которых были оформлены кар-и под благовидным предлогом выведывали паспортные данные клиентов.

Полученные сведения позволяли мошенникам получать от операторов банка по телефону пин-коды и снимать с карт через банкоматы кредитную сумму. После этого карта с нулевым остатком на счете по почте отправлялась подлинному клиенту. Всего группа похитила около 10 млн руб. Потерпевшими по данному делу признаны около 200 клиентов банка[1].

Завершая тему участия работников банка в противоправных действиях с пластиковыми картами, следует отметить, что общее количество таких случаев относительно невелико. В 2006 г., например, по данным Департамента экономической безопасности (ДЭБ) МВД России, из 206 выявленных лиц, участвовавших в изготовлении и сбыте поддельных пластиковых карт, число сотрудников кредитных организаций составило 5 человек. Тем не менее, каждый такой случай становится предметом тщательного изучения банковского сообщества, поскольку потенциальные потери денежных средств и урон репутации кредитных организаций значительно выше, чем при совершении преступных посягательств лицами «со стороны».

Предупреждение хищений денежных средств банка с использованием пластиковых карт. Программы предупреждения хищений денежных средств банка с использованием пластиковых карт, как правило, содержат комплекс мер организационного и технологического характера.

Организация выпуска карт должна начинаться с письменного согласования определенных мер между подразделениями, участвующими в указанной процедуре. В процессе согласования инициатор выпуска готовит мотивированное предложение об изготовлении карт; бухгалтерия подтверждает факт наличия средств на выпуск карты; служба защиты интересов банка (безопасности) высказывает свое мнение о необходимых мерах защиты изготовления и использования карт; группа изготовления карт готовит предложения производственно-технологического характера. Эти меры направлены на предотвращение возможного несанкционированного выпуска карт.

В число организационных мер входит проведение предварительной проверки персональных данных будущих владельцев пластиковых карт и разработка рекомендаций для повышения надежности их хранения. Пристальное внимание соответствующих подразделений банка уделяется также проверке предполагаемых организаций-партнеров, предлагающих обслуживание клиентов банка по пластиковым картам.

Меры технологического характера предполагают повышение надежности процедуры передачи информации платежной системы и идентификации владельца карты.

Внедрение так называемых смарт-карт — платежных карт со встроенным микропроцессором, обеспечивающим качественно новый уровень защиты содержащейся в ней информации, например, «Экономкарта», эмитированная Агрохимбанком. Зарубежные банки, в частности, внедряют идентификационные

[1] *Ковалева Е.* Чем счет не шутит // Деньги. 2007. № 8. 5 марта

стемы с использованием биометрических (голос, отпечатки пальцев рук .) параметров держателей карт.

Самостоятельными направлениями являются обеспечение мер безопасно в процессе изготовления карт и их рассылки: сохранности изготовленны т, их заготовок и расходных материалов; соблюдение требований по разде нию уровней доступа к различным этапам изготовления карт с целью пре ьного ограничения числа лиц, осведомленных о вносимой в карту ключе информации.

Система контроля за операциями с пластиковыми картами реализуето вух направлениях: внешнем и внутреннем. Первое направление призван леживать операции с пластиковыми картами вне банка. В число его зад дит, в частности, ведение и публикация специального банковского реест омерами блокированных пластиковых карт (стоп-листа).

Задача второго направления — вести контроль за расчетами непосредс но в подразделениях, осуществляющих выпуск пластиковых карт и расч с их использованием.

Технические средства защиты от хищений денежных средств банка путе аконного использования пластиковых карт включают в себя средства з ты:

- карт от несанкционированного использования;
- процессинговых центров, обрабатывающих операции с картами;
- банкоматов для выдачи наличных денег.

Технико-криминалистические средства выявления, предупреждения и пр ения хищений в процессе использования пластиковых карт позволяют вы ять описанные выше признаки подделки карт и личных документо ержателей.

5.3. Хищения денежных средств с использованием аккредитивов

Аккредитив является ценной бумагой, выполняющей функции платежног умента. Расчеты по аккредитиву служат одним из средств безналичны четов, широко используемых в имущественном обороте. В качестве разно ности банковских операций аккредитив представляет собой условное де ное обязательство банка, выставляемое на основании поручения его кли а в пользу контрагента по договору.

В соответствии со ст. 867 ГК РФ при расчетах по аккредитиву банк-эми т, действующий по поручению и в соответствии с указанием плательщик открытии аккредитива, обязуется произвести платежи получателю средст о отдать полномочия о производстве платежей другому банку (исполняю му банку).

Особенность аккредитивной формы расчетов по сравнению с расчетами тежными поручениями заключается в том, что плательщик не переводит ежные средства на счет получателя, а выделяет, «резервирует» те из них,

за счет которых будут вестись расчеты с получателем. Выплата с аккредитива наличными деньгами не допускается.

Кроме того, для получения денежных средств по аккредитиву их получатель (бенефициар) должен выполнить условия аккредитива, содержащиеся в договоре с плательщиком. Содержание этих условий (отправка партии товара и т. п.) дублируется в поручении аккредитиводателя банку на открытие аккредитива.

Российское законодательство предусматривает возможность использования нескольких видов аккредитивов, применяемых в банковской практике: покрытого (депонированного) и непокрытого (гарантированного) аккредитива; отзывного и безотзывного аккредитива; подтвержденного аккредитива.

Покрытый (депонированный) аккредитив открывается при условии перечисления банком-эмитентом суммы аккредитива (покрытия) исполняющему банку на срок действия аккредитива. Покрытие аккредитива осуществляется из средств плательщика либо за счет выданного ему банком-эмитентом кредита.

Непокрытый (гарантированный) аккредитив открывается без перечисления суммы аккредитива банку-эмитенту. Гарантией возмещения выплаты по непокрытому аккредитиву служит ведущийся в исполняющем банке корреспондентский счет банка-эмитента. Закон предоставляет право банку-исполнителю списывать с этого счета всю сумму аккредитива без уведомления банка-эмитента. Таким образом, непокрытый (гарантированный) аккредитив может использоваться лишь в тех случаях, когда банк-эмитент и исполняющий банк имеют корреспондентские отношения.

Отзыв аккредитива не создает каких-либо обязательств банка-эмитента перед получателем средств.

В каждом аккредитиве должно быть ясное указание на то, является он отзывным или безотзывным. В случае отсутствия указания в тексте на безотзывность аккредитива он признается отзывным. Отзывный аккредитив (ст. 868 ГК РФ) может быть изменен или отменен банком-эмитентом без предварительного уведомления получателя средств. Вид аккредитива (в том числе его отзывность либо безотзывность) определяется в договоре, по которому осуществляются расчеты. Согласно ст. 868 ГК РФ всякий аккредитив предполагается отзывным, если в его тексте не будет прямо указано на то, что он является безотзывным.

По просьбе банка-эмитента исполняющий банк может подтвердить безотзывный аккредитив. Такое подтверждение означает принятие исполняющим банком дополнительного к обязательству банка-эмитента обязательства произвести платеж в соответствии с условиями аккредитива, а аккредитив приобретает качество «подтвержденного».

Исполняющий банк обязан осуществить платеж или иные операции по отзывному аккредитиву, если к моменту их совершения им не получено уведомление об изменении условий или отмене аккредитива.

Безотзывный аккредитив (ст. 869 ГК РФ) не может быть отменен без со
ıсия получателя средств и является твердым обязательством банка-эмите
Согласно рекомендациям специалистов в области банковского права, пр
нение отзывной формы аккредитива требует существования определенно
рмы доверия между партнерами. В остальных случаях следует использова
ютзывный и желательно подтвержденный аккредитив[1].

Порядок осуществления расчетов по аккредитиву регулируется Гражда
им кодексом РФ, а также установленными в соответствии с ним банковск
правилами и применяемыми в банковской практике обычаями делово
орота. Согласно Положению Банка России № 2-П, для получения средс
аккредитиву получатель, отгрузив товары, должен представить в испо
ощий банк документы, подтверждающие выполнение всех оговоренн
ием условий: четыре экземпляра реестра счетов и отгрузочные, почтов
ругие предусмотренные условиями аккредитива документы. Первый экз
ıр реестра счетов оформляется подписями лиц, имеющих право подпис
четных документов, и оттиском печати. При нарушении хотя бы одно
этих условий исполнение аккредитива не производится.

Обязанность проверить соблюдение *бенефициаром* всех условий аккредит
возлагается на исполняющий банк. Указанная проверка носит докуме
ьный характер. Установление подлинности изложенных в документах бен
циара фактов в задачу исполняющего банка не входит. Документы, пре
вленные получателем в качестве подтверждения исполнения услов
редитива, исполняющий банк направляет банку-эмитенту.

Факты хищений при расчетах по аккредитивам обычно связаны с испол
анием непокрытых (гарантированных) аккредитивов и представляют со
разновидность мошенничества — преступления, предусмотренного ст. 15
РФ.

Мошенничество при расчетах по аккредитивам большей частью связан
явлением ложных сведений об исполнении основного договора. Механиз
ения, как правило, выглядит следующим образом. Мошенники, выступа
мени некоей организации (как правило, фирмы-прикрытия, учрежденно
ставными лицами по утраченным либо похищенным документам), откры
т расчетный счет в одном из банков, а затем предлагают покупателю по
зить определенные товары с оплатой по аккредитиву. Указанная форм
четов в известной мере повышает доверие к поставщику, поскольку выпла
енежных средств предполагается после поставки товаров, в проверке усло
оплаты аккредитива участвует исполняющий банк.

После получения от исполняющего банка сведений об открытии аккредити
ошенники предъявляют в названный банк поддельные документы об ис
нении обязательств, поддельный паспорт на имя лица, выступающего

[1] *Эриашвили Н. Д.* Банковское право: учеб. для вузов. М.: Закон и право; Юнити-Дана, 1999
9–190.

от имени получателя средств по аккредитиву, а в необходимых случаях и поддельную доверенность на право совершения соответствующих действий. В тех случаях, когда условиями аккредитива предусмотрено участие в приеме и отправке товара представителя покупателя, используются поддельный паспорт и доверенность на имя мнимого представителя, а также поддельное письмо покупателя с подтверждением факта отправки (получения) товара и разрешением на раскрытие аккредитива. Обусловленный договором товар в действительности не поставляется. В ряде случаев покупателю отправляется некая товарная «кукла» — малоценный груз, не имеющий ничего общего с предметом договора. Поступившие на счет лжекоммерческой организации (фирмы-прикрытия) денежные средства переводятся в наличность и похищаются.

Нередко мошенники по причине правовой неосведомленности предъявляют исполняющему банку поддельные документы, не соответствующие условиям аккредитива даже по формальным признакам.

При установлении несоответствия документов условиям аккредитива по внешним признакам исполняющий банк должен отказать в их принятии, незамедлительно уведомив об этом получателя средств и банк-эмитент. В случае принятия исполняющим банком документов, не соответствующих условиям аккредитива по внешним признакам, он несет имущественную ответственность в размере сумм, неправомерно выплаченных покупателю.

На практике факты раскрытия исполняющими банками аккредитивов на основании фиктивных документов с признаками несоответствия условиям аккредитива встречаются нередко. Причина этого, в одних случаях, объясняется недостаточным уровнем знаний и навыков сотрудников банка в сфере документального оформления первичных документов, подтверждающих осуществляемые хозяйственные операции, а также перевозочных документов (что не позволяет сотрудникам банка обнаружить указанное выше несоответствие). В других — правомерно вести речь о халатности сотрудников, не обративших внимания на несоответствие по небрежности.

Примером мошенничества с использованием внешних признаков соответствия документов условиям аккредитива могут служить следующие случаи.

Организация «Роспродукт» представила исполняющему банку в качестве документов, подтверждающих исполнение договора купли-продажи сахарного песка с аккредитивной формой расчетов, счет-реестр от 6 апреля 1995 г. с указанием даты отгрузки сахара 14 апреля 1995 г. и 15 апреля 1995 г., счет-фактуру от 5 апреля 1995 г. и четыре железнодорожные квитанции о приеме груза. На основании указанных документов банк выплатил денежные средства по аккредитиву в размере 496 033 000 руб. Однако сахарный песок контрагенту по договору не был поставлен. Непосредственный изготовитель продукта пояснил, что сахара по указанным поставщиком транспортным документам он не отгружал. Грузовые квитанции оказались поддельными. По данному факту было возбуждено уголовное дело по обвинению в хищении руководителя ООО

оспродукт». Имущественные претензии к банку арбитражный суд призна
состоятельными.

Однако на практике весьма распространенными являются случаи обма
ешние признаки которого должны были выявить работники банка.

Так, например, в декабре 2001 г. исполняющий банк выплатил ЗАО «Ал
йпромзерно» 4 560 000 руб. с аккредитива в качестве оплаты договора куп
-продажи сухого молока ООО «Молагро». Выплата по аккредитиву пред
атривала представление обществом «Алтайпромзерно» железнодорожны
кладных, сертификата качества, удостоверения качества, счета-фактур
самом деле вместо сухого молока ЗАО «Алтайпромзерно» отгрузило в ад
нтрагента отруби. Об этом прямо свидетельствовали представленные в и
няющий банк документы, однако его сотрудники на это обстоятельст
имания не обратили.

В другом случае АОЗТ «Пласт» получило от исполняющего банка дене
е средства по аккредитиву, представив в подтверждение исполнения дого
ра купли-продажи железнодорожные накладные об отгрузке покупателю са
ла третьими лицами. Названные *документы не содержали сведений не тольк
участии в поставке самого АОЗТ «Пласт», но и о выполнении обязательст
чет контракта от 1 февраля 2004 г. № 49/А-5.* В сертификатах качест
происхождения товаров такие данные также отсутствовали. Таким образом
ержащиеся в документах данные не позволяли считать условия аккредити
выполненными. Как выяснилось впоследствии, сахар поставщиком отгру
л не был, а предъявленные в банк документы оказались поддельными.

В последних двух случаях, наряду с привлечением похитителей к уголов
й ответственности, иски о возмещении вреда в гражданском порядке был
дъявлены исполняющим банкам.

Несоблюдение условий оплаты аккредитива может выражаться также в от
ствии реквизитов документов, подтверждающих исполнение договора,
есоответствии вида документов, места исполнения договора и других об
ятельств, оговоренных контрактом.

Так, при расследовании хищения денежных средств АОЗТ «Магнитогор
й комбинат хлебопродуктов» в 2003 г. было установлено, что преступники,
учившие деньги по аккредитиву за якобы отгруженную в адрес покупателя
еницу, представили в исполняющий банк железнодорожные накладные
сто железнодорожных квитанций, счет-фактуру и реестр счетов без указа
номеров перевозочных документов, акт приема-передачи, составленный
танции, не указанной в договоре.

Указанные обстоятельства свидетельствовали о ненадлежащем исполнении
отниками кредитной организации обязанностей по проверке внешних
знаков соответствия документов условиям аккредитива и послужили осно
ием для взыскания с банка 700 000 руб., которые были неправомерно вы
чены по аккредитиву.

Одним из способов хищения денег банка является открытие подложных аккредитивов сотрудниками банков в соучастии с посторонними лицами.

Меры защиты от хищений с использованием аккредитивов

С целью предупреждения потерь от мошенничества при расчетах по аккредитиву соответствующие службы банка должны выполнить как минимум следующие действия.

Покупателю необходимо получить сведения, подтверждающие факт реального существования организации-продавца, надежность предполагаемого контрагента и наличие возможности выполнить предполагаемую поставку, используя для этого:

- данные Единого государственного реестра юридических лиц (далее — ЕГРЮЛ) — адрес (место нахождения) постоянно действующего исполнительного органа юридического лица; фамилию, имя, отчество и должность лица, имеющего право без доверенности действовать от имени юридического лица, а также его паспортные данные или данные иных документов, удостоверяющих личность в соответствии с законодательством, и ИНН при его наличии; сведения о лицензиях, полученных юридическим лицом; сведения о филиалах и представительствах юридического лица; сведения о возможном нахождении юридического лица в процессе ликвидации, а также другую важную для проверки информацию[1];
- рекомендации от прежних партнеров организации;
- посещение рабочих (складских) помещений потенциального контрагента;
- проверку функционирования сообщенных предполагаемым контрагентом номеров телефонов, факсов, электронных адресов организации;
- проверку фактической возможности осуществления схемы предполагаемой поставки товара. На практике нередки случаи, когда посредник указывает в качестве изготовителя продуктов организацию либо регион, в которых такие продукты не изготавливаются.

Предупредительные меры банка должны включать в себя:

- выполнение аналогичных проверочных мероприятий в рамках процедуры заключения договора банковского счета с будущим клиентом;
- тщательную проверку соответствия представленных для оплаты документов и их реквизитов условиям аккредитива на основании самих документов. Несоответствия могут выражаться не только в расхождениях между документами на оплату и условиями аккредитива, но и в разно-

[1] Доступ к этим ресурсам свободен для всех заинтересованных лиц. Процедура доступа регламентирована приказом ФНС России от 21 октября 2004 г. № САЭ-3–09/7@ «Об утверждении Порядка предоставления в электронном виде сведений, содержащихся в Едином государственном реестре юридических лиц и в Едином государственном реестре индивидуальных предпринимателей».

чтениях в тексте одного из документов, например, расхождение между написанием фамилии директора, нотариуса или другого уполномоченного лица в текстовой части документа и расшифровкой подписи, различия в названии организации на бланке документа и оттиске печати;
- внимательное исследование соответствия подписей и печати получателя средств образцам, указанным в карточке с образцами подписей и оттиска печати;
- проверку подлинности документов, удостоверяющих личность получателя средств, наличие у него соответствующих полномочий на получение денег, правильность оформления доверенности;
- проверку подлинности документов, удостоверяющих личность представителя покупателя (плательщика по аккредитиву) и его доверенности (если участие представителя в приемке товара предусмотрено договором).

Предупреждению хищений с использованием аккредитива в определенной ре способствует точное соблюдение правил открытия банковского счета по ателя средств. В соответствии с ними банку должны быть представлены пии учредительных документов юридического лица и карточка с образцами подписей соответствующих физических лиц. В вызывающих сомнения чаях соответствующим службам банка следует проверить подлинность ных документов, реальность существования юридического лица и его едпринимательской деятельности.

5.4. Хищения денежных средств с использованием чеков

Согласно гражданскому законодательству чек представляет собой один видов ценных бумаг, содержащий ничем не обусловленное распоряжение одателя банку произвести платеж указанной в нем суммы чекодержателю 877 ГК РФ).

Порядок и условия использования чеков в платежном обороте регулируются ст. 877–885 ГК РФ, а в части, им не регулируемой, — другими законами станавливаемыми в соответствии с ними банковскими правилами.

Плательщиком по чеку может быть только банк, где чекодатель имеет дства, которыми он вправе распоряжаться путем выставления чека. Участками чековой формы расчетов могут быть как юридические, так и физические лица. Однако расчеты чеками между физическими лицами запрещены.

В соответствии со ст. 878 ГК РФ чек должен содержать ряд обязательных визитов: наименование «чек», включенное в текст документа; поручение тельщику выплатить определенную денежную сумму; наименование пла ьщика и указание счета, с которого должен быть произведен платеж; указа валюты платежа; указание даты и места составления чека; подпись лица, писавшего чек (чекодателя). Кроме того, в него могут быть включены дополнительные реквизиты, определяемые спецификой банковской деятельности

и налоговым законодательством. Форма чека определяется кредитной организацией самостоятельно.

Отсутствие в документе необходимых реквизитов лишает его силы чека. Чек, не содержащий указание места его составления, рассматривается как подписанный в месте нахождения чекодателя. Указание о выплате процентов по чеку в тексте документа не допускается (считается ненаписанным — в случае внесения такой записи в текст). Форма чека и порядок его заполнения определяются законом и установленными в соответствии с ним банковскими правилами. Бланки чеков изготовляются по единому образцу и брошюруются в книжки установленного образца по 10, 25 и 50 листов. Бланки чеков являются предметом строгой отчетности и хранятся в порядке, установленном нормативными актами Банка России.

В соответствии с Положением о безналичных расчетах в Российской Федерации банки перед выдачей чеков своим клиентам (юридическим и физическим лицам) обязаны заполнить чеки, проставив на них:

а) *наименование головного банка* и его местонахождение (рядом с наименованием головного банка может быть проставлено и его фирменное обозначение) в верхней левой части чека, а в случае выдачи чека филиалом банка — также и наименование филиала и его местонахождение (в верхней правой части чека);

б) условный номер банка по классификации Международных Финансовых Организаций, а при переходе на 8-значную систему кодирования — его 8-значный номер. Номер банка проставляется в нижней части чека, в соответствующей секции целевого поля. В случае, если филиалу не открыт корреспондентский субсчет в расчетно-кассовом центре или он открыт в учреждении коммерческого банка, в чеке проставляется номер, присвоенный головному банку, или, по согласованию с коммерческим банком, его номер. В последнем случае рядом с наименованием филиала банка должно быть проставлено наименование и местонахождение соответствующего коммерческого банка;

в) *номер лицевого счета чекодателя*. Этот номер должен быть проставлен в соответствующей части целевого поля в нижней части чека, а также может быть проставлен в тексте чека;

г) *наименование чекодателя* — юридического лица (или фамилия, имя, отчество физического лица), номер его счета. Эти данные проставляются в специальной зоне в нижней левой части чека;

д) *предельный размер суммы, на которую может быть выписан чек* (на оборотной стороне чека). Сумма лимита чека указывается цифрами и прописью, заверяется печатью и подписями должностных лиц банка.

Чек оплачивается за счет средств чекодателя. Покрытием чека в банке чекодателя могут быть средства, депонированные чекодателем на отдельном счете, либо средства, имеющиеся на соответствующем счете чекодателя.

Закон обязывает плательщика по чеку удостовериться всеми доступными ему способами в подлинности чека, а также в том, что предъявитель чека

ляется уполномоченным по нему лицом. При оплате *индоссированно*
меющего подпись, удостоверяющую переход права по документу к друго
щу) чека плательщик обязан проверить правильность индоссаментов. Одн
проверка подлинности подписи индоссантов в его обязанность не входит
Ответственность за убытки, возникшие вследствие оплаты плательщик
одложного, похищенного или утраченного чека, возлагается на плательщи
и чекодателя в зависимости от того, по чьей вине они были причинены.
Оплата чека производится в порядке, установленном ст. 875 «Исполнен
кассового поручения» ГК РФ. В случае несоответствия документа по вне
им признакам инкассовому поручению, исполняющий банк обязан нем
нно известить об этом лицо, от которого было получено инкассовое поруч
е. А если устранить указанные недостатки не представляется возможны
нк вправе возвратить чек без исполнения.
Если чек подлежит оплате по предъявлении, исполняющий банк долж
елать представление к платежу немедленно по получении инкассового п
ения. В тех случаях, когда документы подлежат оплате в иной срок, испо
ющий банк должен для получения согласия на оплату (акцепта) плательщ
представить документы к акцепту немедленно по получении инкассово
ручения, а требование платежа должно быть сделано не позднее дня наст
ения указанного в документе срока платежа.
Частичные платежи могут быть приняты в случаях, когда это установле
ковскими правилами либо при наличии специального разрешения в ин
совом поручении.
Для получения денег по предъявленному чеку они должны быть предвар
ьно зачислены на счет чекодержателя.
Внутрибанковские правила проведения операций с чеками, определяющ
рядок и условия их использования, должны предусматривать:

- форму чека, перечень его реквизитов (обязательных, дополнительны
  и порядок заполнения чека;
- перечень участников расчетов данными чеками;
- срок предъявления чеков к оплате;
- условия оплаты чеков;
- ведение расчетов и состав операций по чекообороту;
- бухгалтерское оформление операций с чеками;
- порядок архивирования чеков.

Способы обмана в процессе операций с денежными чеками. Суть преступны
ствий в процессе операций с *денежными чеками* заключается в получени
ег по чеку лицом, в отношении которого не было распоряжения о выплат
се, либо в получении таким лицом суммы, превышающей распоряжение
одателя.
Совершение мошеннических действий указанного рода требует от зло
шленников ряда подготовительных действий. В их числе неправомерное за
ение чистыми бланками чеков либо заполненными чеками с последующей

подделкой ценных бумаг. В большинстве случаев бланки похищаются в организациях по месту хранения чековых книжек, чему, как правило, способствует халатность ответственных за документы лиц. Нередко одновременно с хищением бланков преступники ставят на них оттиск печати организации, которая чаще всего хранится вместе с документами строгой отчетности. В практике владельцев чековых книжек нередки случаи, когда бланки исчезают при невыясненных обстоятельствах. Отсутствие бланков по месту хранения в таких случаях принято рассматривать как их утрату, хотя в действительности значительное число таких утрат представляет собой замаскированную кражу.

Подделка денежного чека предполагает также предварительное получение преступниками соответствующей информации о банке, реквизитах организации, которая имеет в нем средства для выплаты денег по чеку, о корреспондентском счете, с которого должен быть произведен платеж. Добываются образцы подписи чекодателя. Для получения таких сведений используются соучастники преступлений либо неосведомленные о преступных намерениях лица из числа работников кредитной организации. Кроме того, изготавливаются поддельные документы для маскировки личности получателя денежных средств и другие документы, необходимые для совершения операции с чеком.

Фальсификация чеков может быть частичной или полной.

В первом случае подложная информация вносится в подлинный чек путем изменения его первоначального содержания. Таким способом изменяются суммы платежа, наименование чекополучателя и другие реквизиты.

Полная подделка чека осуществляется посредством внесения несоответствующей действительности информации в похищенный чистый бланк. При изготовлении фальшивок могут использоваться поддельные печати. Примером многоходового, тщательно организованного хищения с использованием чека могут служить действия организованной преступной группы М. и других (всего 7 человек).

Имея информацию о наличии денежных средств в сумме 140 млн руб. на счету фирмы ТОО «Э», закрытом предписанием налоговой инспекции, участники группы изготовили поддельный протокол общего собрания учредителей названной фирмы об избрании нового директора Ш. (паспорт которого был утерян владельцем). Затем мошенники выполнили поддельную удостоверительную запись от имени частного нотариуса о назначении Ш. директором ТОО «Э» и изготовили поддельное письмо из налоговой инспекции Промышленного района города Самары о разрешении проведения операций по расчетному счету ТОО «Э». Предъявив перечисленные поддельные документы, фальшивый чек и паспорт Ш. с переклеенной фотографией, М. получил в банке 139 млн руб., которые были присвоены членами организованной группы[1].

[1] О пропавшем миллиарде. 2002. Вып. 1. 25 марта: Официальный сайт прокуратуры Самарской области (http://prokuror.samara.ru/2002/1/department/11).

Получение наличных денег по поддельному чеку может быть завершени ногоходовой мошеннической операции, совершенной с участием работн ов либо руководителей (в том числе бывших) организации — владельца сч . Так, например, неустановленное лицо заключило от имени ООО «Т-Б» д овор поставки от 26 июня 2001 г. № 4к, согласно которому названная орган ация обязалась поставить обществу «Б» мини-ферму.

Во исполнение этого договора ООО «Б» перечислило на счет ООО «Т- Автобанке 3 млн руб. платежным поручением от 26 июля 2001 г. № 26. Вск е после поступления указанных денег на счет они были выданы Автобанк о поддельным чекам наличными неустановленному лицу, предъявившем альшивый паспорт. Показательно, что сотрудники банка не обратили вним ия даже на несоответствие реквизитов предъявленного фальшивого паспо еквизитам этого документа, указанным в поддельном чеке[1].

В практике банковской деятельности периодически встречаются факты х ения денег путем подделки кассовых чеков, совершенные как посторонн и лицами, так и клиентами банка, имеющими в нем собственный счет на н ачительную сумму. Для этого злоумышленники, как правило, использу опускающиеся в банке нарушения технологии выдачи наличных денег, п юляющие внедрить поддельный чек в расчетную систему, а также разрабат ют меры, позволяющие избежать ответственности за совершенное престу ние.

Несмотря на «устарелость» указанного способа мошенничества, хищени кого рода по-прежнему совершаются в банках Москвы и регионах России пичным явился случай, когда клиент одного из московских банков сум ять «со своего счета» и получить в кассе денежную сумму, на два порядк евышающую остаток принадлежащих ему денежных средств.

Имевшие место хищения стали возможными в результате грубых наруше ий порядка выдачи наличных денег из кассы: денежный чек, предъявленный оплату операционному работнику, не должен возвращаться на руки клиен- . Однако в указанных выше случаях хищений денежные чеки были выданы руки клиентам вместе с не вырезанными из бланков марками и бесконольно находились в их распоряжении в течение операционного дня. Похи тели меняли выданный чек на поддельный (значительно превосходящий сумме подлинный). Они предъявляли его в кассу, получали наличные день и скрывались. Факты хищений были обнаружены лишь при подведении гов кассовой работы в конце дня.

В ряде случаев подделка использовалась для снятия денежных сумм с чу их счетов, номера которых были известны злоумышленникам. При получе ии денег в кассу, кроме поддельного чека, предъявлялся фальшивый паспорт имя владельца счета.

[1] Постановление Президиума Высшего Арбитражного Суда РФ от 14 октября 2003 г. 5278/03.

Способы обмана в процессе операций с расчетными чеками. Обман в процессе операций с расчетными чеками может совершаться как лицом, предъявляющим чек к оплате, так и чекодателем.

В одних случаях лицо предъявляет к оплате полностью поддельный чек и другие необходимые для совершения банковской процедуры документы, согласно которым перевод денежных средств со счета чекодателя на расчетный счет организации мошенников объясняется оплатой исполненного договора.

В других ситуациях к оплате предъявляется частично подделанный чек, выписанный чекодателем. Изменения (в сторону завышения суммы) вносятся в номинал чека, а также в реквизиты счета организации-получателя. Не исключено, что в руки мошенников чек, выписанный чекодателем, попадает в результате хищения.

Обман со стороны чекодателя может заключаться в умышленном дефекте оформления расчетного документа в виде расхождения номинала на корешке с номиналом чека. В указанных случаях чекодатель заявляет банку о подделке номинала чека.

Вариантами обмана может стать выдача чека, не обеспеченного денежными средствами («резинового» чека), либо выдача чека с последующим блокированием чековой суммы после его инкассирования банком заявлением о хищении, либо выдача чека на оплату в банке, не имеющем для этого средств (банк-банкрот).

В последнее время ряд московских банков подвергся обману в результате приобретения чеков иностранных физических и юридических лиц. Суть обмана заключалась в том, что после инкассирования чеков российским банком иностранный банк вначале подтверждал наличие денег на счете чекодателя. Однако в процессе перевода денежных средств в Россию счет чекодателя блокировался по причине дефекта денег («отмытые деньги») либо заявления о хищении чека.

Меры предупреждения хищений с использованием чеков

1. В банке:
   - зачисление средств на счет чекодержателя производить только после списания средств со счета банка-плательщика;
   - проверить, не истек ли срок действия чека (чек должен быть предъявлен к оплате в учреждение банка в течение 10 дней, не считая дня его выдачи);
   - удостовериться в подлинности чека путем:

     а) проверки отсутствия внешних признаков подчисток и исправлений;

     б) наличия на документе обязательных для чека реквизитов, указанных выше;

     в) сопоставления имеющихся в чеке реквизитов с реквизитами чековой карточки, выданной банком чекодателю одновременно с бланками

чеков: номер лицевого счета чекодателя; наименование чекодателя
юридического лица (или фамилия, имя, отчество физического лица), н
мер его счета, соответствие подписей уполномоченных лиц и печати о
разцам подписей и оттиском печати, содержащимся в чековой карточке

Следует проверить также, не превышает ли сумма, на которую выпис
к, сумму лимита, указанную на его оборотной стороне; заверена ли лими
я сумма чека на его оборотной стороне печатью и подписями уполномоче
их лиц банка.

Кроме того, при оплате *индоссированного* (переводного) чека следует так
едиться в правильности оформления передаточной надписи и в том, ч
едъявитель чека является именно тем лицом, которое уполномочено сов
ать с ним операции.

Следует удостовериться в правомочности лица, участвующего в операци
олучением денег по чеку, проверить его документы.

Для подтверждения факта участия лица в совершении операции с чек
нк вправе потребовать от него расписку в получении платежа.

2. В организации-чекодателе:
   - установить ограниченный доступ сотрудников к работе с чека
     и информации о ведущихся и планируемых расчетах. В случае хищ
     ния либо выхода из владения при невыясненных обстоятельствах ч
     ковых книжек и печатей незамедлительно информировать об это
     соответствующую кредитную организацию;
   - исключить возможность несанкционированного доступа неуполно
     моченных лиц к печатям и бланкам чеков.
3. В организации — получателе средств:
   - удостовериться в надежности и платежеспособности чекодателя конт
     агента. Проверить на соответствие фактическим данным таких ре
     визитов предполагаемого контрагента, как наименование платель
     щика, номер его счета, идентификационный номер налогоплатель
     щика (ИНН); наименование и местонахождение банка плательщика,
     его банковский идентификационный код (БИК);
   - проверить соответствие суммы денежных средств, указанных в чеке,
     сумме, указанной на корешке чека.

.5. Хищения денежных средств с использованием платежных поручений

В деловой практике платежные поручения используются в качестве финан
ого инструмента для безналичных расчетов. Их применение регламентиро
о ст. 862 ГК РФ.

Любая банковская операция, в том числе расчетные операции по безналично
еречислению денежных средств, выполняется на основе банковских техно
ий, установленных законодательством и иными нормативными правовыми
писаниями. Следует отметить, что значительная часть технологических

требований нацелена на обеспечение защиты интересов участников операций от преступных посягательств. Неукоснительное выполнение соответствующих предписаний играет важную роль в предупреждении мошенничества и других видов преступлений в кредитно-финансовой сфере.

Учитывая это обстоятельство, лица, подготавливающие преступления в банковской сфере, как правило, детально изучают технологические особенности операций в поисках возможных «брешей в защите». Затем, по ходу совершения преступления, они создают ситуации, которые используются для того, чтобы убедить потерпевшего в целесообразности отхода (порой незначительного, на первый взгляд) от установленной технологии совершения сделок, либо маскируют фактически совершенные отступления различными способами. На самом деле указанные действия, как правило, являются составной частью механизма преступления, а *их наличие может служить признаком готовящегося или совершаемого мошенничества.*

Технология выполнения безналичных расчетов регламентирована Положением Банка России № 2-П. Согласно ему соответствующие документы оформляются на бланках установленного образца, изготовленных в типографии или с использованием электронно-вычислительных машин. Допускается использование копий бланков расчетных документов, полученных на множительной технике, при условии, если копирование производится без искажений.

Расчетные документы на бумажном носителе заполняются с применением пишущих или электронно-вычислительных машин шрифтом черного цвета, за исключением чеков, которые заполняются шариковыми ручками, черными, синими или фиолетовыми чернилами (допускается заполнение чеков на пишущей машинке шрифтом черного цвета). Подписи на расчетных документах проставляются ручкой с пастой или чернилами черного, синего или фиолетового цвета.

Расчетные документы должны содержать следующие обязательные реквизиты:

а) наименование расчетного документа и код формы по ОКУД ОК 011–93;

б) номер расчетного документа, число, месяц и год его выписки;

в) вид платежа;

г) наименование плательщика, номер его счета, идентификационный номер налогоплательщика (ИНН);

д) наименование и местонахождение банка плательщика, его банковский идентификационный код (БИК), номер корреспондентского счета или субсчета;

е) наименование получателя средств, номер его счета, идентификационный номер налогоплательщика (ИНН);

ж) наименование и местонахождение банка получателя, его банковский идентификационный код (БИК), номер корреспондентского счета или субсчета;

з) назначение платежа. Налог, подлежащий уплате, выделяется в расчетном документе отдельной строкой (в противном случае должно быть указание на то, что налог не уплачивается);

и) сумму платежа, обозначенную прописью и цифрами;
к) очередность платежа;
л) вид операции в соответствии с правилами ведения бухгалтерского учета Банке России и кредитных организациях, расположенных на территории оссийской Федерации;
м) подписи (подпись) уполномоченных лиц (лица) и оттиск печати (в установленных случаях).

Документы не должны иметь исправлений, в том числе с использованием ррректирующей жидкости, помарок и подчисток.

В соответствии с п. 2.12. Положения Банка России № 2-П все виды расчетных документов действительны к предъявлению в обслуживающий банк течение десяти календарных дней, не считая дня их выписки. Расчетные документы предъявляются в банк в количестве экземпляров, необходимом для ех участников расчетов (обычно от двух до четырех). Второй и последующие земпляры расчетных документов могут быть изготовлены с использованием пировальной бумаги, множительной техники или электронно-вычислительных машин.

Расчетные документы принимаются банками к исполнению при наличии *первом экземпляре* (кроме чеков) *двух подписей* (первой и второй) лиц, еющих право подписывать расчетные документы, *или одной подписи* (при сутствии в штате организации лица, которому может быть предоставлено аво второй подписи) и оттиска печати (кроме чеков), заявленных в карточке с образцами подписей и *оттиска печати*.

В рамках применяемых форм безналичных расчетов допускается использование аналогов собственноручной подписи (электронной цифровой подписи) соответствии с требованиями законодательства и нормативных актов Банка ссии.

Способы мошенничества при расчетах платежными поручениями

При осуществлении расчетов платежное поручение выступает в качестве споряжения владельца счета (плательщика) обслуживающему его банку, пе вести определенную денежную сумму на счет получателя средств, открытый том или другом банке. В данном случае это распоряжение одновременно яется расчетным документом.

Платежное поручение исполняется банком в срок, предусмотренный законодательством, или установленный договором банковского счета. При этом подписи лиц, имеющих право подписывать расчетные документы, и оттиск печати, заявленные в карточке с образцами подписей и оттиска печати, выполняются *лько на первом экземпляре* предъявляемого в банк платежного поручения.

В соответствии с установленным порядком осуществления операций между банком-респондентом и банком-корреспондентом должна быть достигнута оворенность о правилах обмена документами (на бумажном носителе,

в виде электронного документа) и форме реестра предстоящих платежей с перечислением необходимых реквизитов для совершения расчетных операций, способе и порядке его передачи (на бумажном носителе или в виде электронного документа).

Для подписания платежных поручений, подготовленных в виде электронного документа в рамках применяемых форм безналичных расчетов допускается использование аналогов собственноручной подписи, в соответствии с требованиями законодательства и нормативных актов Банка России[1].

Расчеты платежными поручениями производятся в целях, предусмотренных законодательством или договором, в том числе для оплаты поставленных (отпущенных) товаров, выполненных работ или оказанных услуг; перечисления денежных средств в бюджеты всех уровней и внебюджетные фонды; возврата кредитов и т. д.

Обязательства плательщика уплатить денежную сумму вытекают из гражданско-правового договора между плательщиком и получателем денежных средств (далее — основной договор), в котором предусматривается оплата безналичными средствами. В соответствии с условиями основного договора платежные поручения могут использоваться для *предварительной оплаты* или для осуществления *периодических платежей*. При этом, согласно п. 1.5 Положения Банка России № 2-П, банки не связаны условиями основного договора. Взаимные претензии по расчетам между плательщиком и получателем средств, кроме возникших по вине банков, решаются в установленном законодательством порядке без участия банков. Иными словами, в случае непоступления средств по исполненному основному договору, получатель вправе требовать осуществления платежа только от организации-плательщика, даже если банк плательщика утверждает о том, что перечислил денежные средства банку получателя.

Существенным обстоятельством, которое необходимо учитывать при расчетах платежными поручениями, является различие между понятиями «принятие к исполнению» (акцепт) и «исполнение» платежного поручения. Дело в том, что если поручение плательщика, согласно части 3. ст. 864 ГК РФ, исполняется банком при наличии средств на счете плательщика, то к исполнению названные расчетные документы принимаются банком *независимо от наличия денежных средств на счете плательщика* (п. 3.5 Положения Банка России № 2-П)[2].

---

[1] См. Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».

[2] Показательно, что Банковский кодекс Республики Беларусь 2001 года в целях повышения безопасности безналичных расчетов освободил банки от существовавшей ранее обязанности принимать платежное поручение к исполнению при отсутствии на текущем счете клиента достаточной суммы средств (ст. 248 «Условия принятия банком-отправителем поручения плательщика»). Научно-практический комментарий к Банковскому кодексу республики Беларусь: в 2 кн. Кн. 2 / Д. А. Калимов, А. М. Ковалева и др. Мн.: Дикта, 2002. С. 476.

Последний экземпляр принятого к исполнению платежного поручения звращается плательщику. В качестве подтверждения приема в поле «Отмет и банка» на последнем экземпляре проставляются штамп банка, дата приема подпись ответственного исполнителя.

В случае отсутствия или недостаточности денежных средств на счете пла ельщика оплата платежных поручений производится по мере поступлени редств, в очередности, установленной законодательством. Допускается час ичная оплата платежных поручений. Свидетельством полной оплаты платеж ого поручения служит отметка банка о дате списания денежных средств о счета плательщика (при частичной оплате — дата последнего платеж поле «Списано со сч. плат.», заверенная подписью ответственного исполни еля и штампом банка в поле «Отметки банка».

Согласно п. 2.17 Положения Банка России № 2-П плательщик вправе от зать свое платежное поручение. Отозванные платежные поручения возвр аются плательщику.

Достоверным подтверждением факта оплаты, произведенной по платежн у поручению, является получение контрагентами выписки из банковско ета с указанием зачисленной суммы. Выписка представляется банком в ср , оговоренные договором банковского счета, на бумажном носителе, в т исле и в тех случаях, когда расчеты совершались в электронном формате.

Способы использования платежного поручения в целях обмана и злоупотреб ия доверием в целом можно разграничить на две основных группы:

первая — использование платежных поручений в качестве фиктивного ра тного документа, не имеющего реального наполнения денежными средствам

вторая — использование поддельного платежного поручения для хищен нежных средств в организации путем их перечисления со счета организаци другие счета.

спользование платежных поручений в качестве фиктивного расчетного документа, не имеющего реального наполнения денежными средствами

В случае использования платежных поручений в качестве фиктивного рас тного документа, не имеющего реального наполнения денежными средства , поддельное или подлинное, но не имеющее денежного наполнения пла жное поручение призвано создать у потерпевшего убежденность в том, что атеж осуществлен. Подлинное платежное поручение может быть выполнен имени фирмы-однодневки, учрежденной по утраченным документам. Така ирма открывает расчетный счет в банке с минимальным или нулевым остат м денежных средств. Нередко открытие счета сопровождается утверждения и некими действиями, призванными свидетельствовать об ожидаемом по плении в адрес клиента весомых сумм в оплату за якобы проведенные мас абные сделки и т. д. Возможности проверить реальное состояние счета трагента через банк клиент не имеет, поскольку названная информация, со сно ст. 26 Закона о банковской деятельности, составляет банковскую тайну.

Последующие действия преступников включают в себя заключение договора на приобретение партии товара с безналичной оплатой. Существенным обстоятельством, способствующим обману, является сложившаяся практика делового оборота, согласно которой товар отпускается по предъявлении последнего экземпляра платежного поручения с отметкой банка *о принятии расчетного документа к исполнению.*

Направляя банку поручение о перечислении денежных средств в качестве платежа за отпущенный товар и т. д., мошенники не имеют реального намерения платить. В качестве доказательства мнимого перечисления денежных средств они демонстрируют поставщику (получателю) упомянутый последний экземпляр документа с указанной выше отметкой банка.

В качестве другого варианта обмана преступники используют полностью поддельное платежное поручение, включая отметку банка о приеме к исполнению. Такая подделка в одних случаях может быть выполнена от имени реально существующей организации с ее подлинными реквизитами. В других случаях платежное поручение может содержать реквизиты несуществующей организации, но с подлинной отметкой банка о приеме к исполнению. Речь идет о фактах, когда банк (тоже введенный в заблуждение) открывает счет фиктивной фирме, не прошедшей даже формальной процедуры государственной регистрации.

В 2004 г., используя указанный способ обмана, группа мошенников похитила товары у восьми пермских фирм. При изготовлении поддельных платежных поручений мошенники указывали счет пермского банка, через который фирма-поставщик уже не раз получала деньги от клиентов. Бланки и логотипы они копировали с банковских сайтов, а штампы заказывали в частных гравер ных мастерских.

Товар получал по доверенности нанятый водитель, не осведомленный об истинном содержании операции.

Расчет преступников на то, что фирма, имеющая много клиентов и постоянно совершающая торговые сделки, пропустит отгрузку товара без предоплаты и уж тем более не станет звонить в указанный в платежном поручении банк и справляться о наличии счета клиента, оказался верным.

По данным правоохранительных органов, указанный способ обмана применяется примерно в 30% случаев мошенничества с использованием платежных поручений. Как правило, сумма хищения (чтобы не вызывать недоверия будущего потерпевшего) не выходит за пределы повседневных сделок предпринимателей-поставщиков и составляет от 30 до 70 тыс. руб. Однако в отдельных случаях ущерб может быть намного больше. Совершение такого обмана связано с предварительными действиями, предполагающими придание большей достоверности и убедительности намерениям мнимых «покупателей».

Преступники совершают первичную сделку на сравнительно небольшую сумму и аккуратно ее оплачивают. Оформляют платежные поручения в банке, через которые поставщик обычно ведет расчеты с другими клиентами. «Приучают»

отерпевшего к предложенной ими схеме расчетов, демонстрируют ее мнимые еимущества и надежность. Затем, войдя в доверие к продавцу, мошенники под м или иным предлогом (для облегчения и ускорения работы и т. д.) добиваются гласия потерпевшего на незначительное отступление от «формальных» пред исаний закона и правил совершения сделок. Завершающим этапом обмана яв ется «закупка» товара на крупную сумму, предъявление в качестве подтвержде я его оплаты копии поддельного платежного поручения. После этого «покупа ль» скрывается вместе с товаром. Нередко товар получает нанятый на это учай водитель, который не осведомлен о сути операции. Похищенные ценно и сгружаются в оговоренном месте, откуда впоследствии увозятся и сбываются заниженным ценам другими участниками преступления.

В случаях, когда товар получает непосредственный участник хищени оме поддельного платежного поручения могут предъявляться фальшивы спорт и доверенность на получение товара. Именно так действовала груп еступников, купивших мясо на Базарно-Карабулакском мясокомбинат Саратовской области.

10 ноября 2006 г. некая Р., представившись директором саратовской фирм Монолит», предложила директору названного мясокомбината продать ее фи 100 кг говядины. Сделка была заключена. На следующий день ООО «Моно т» уплатило за продукцию 20 тыс. руб. и получило говядину. Денежны едства прошли через банк и поступили на расчетный счет мясокомбинат кт платежа был подтвержден копией платежного поручения, переданной факсу. Через несколько дней после первой сделки Р. позвонила Д. и заяви что очень довольна сотрудничеством и готова приобрести 5 т мяс 1 млн руб. Она предложила бизнесмену следующий порядок расчетов ноября фирма переведет на счет мясокомбината 500 тыс. руб. Вторая поло ла суммы будет привезена на комбинат наличными после доставки продук в Саратов. Директор комбината с этим предложением согласился. Утро ноября на мясокомбинат приехал «КамАЗ». Р., позвонив Д., прислала факсу копию платежного поручения о перечислении 500 тыс. на счет ком ата. По указанию директора мясо было отгружено в полном объеме. Об был обнаружен после того, как Р. не появилась на мясокомбинате в ого енное время. Лишь после этого Д. решил проверить наличие подлинника тежного поручения в банке. Ответ был отрицательным, копия документа залась фальшивой. В ходе расследования уголовного дела, возбужденного ч. 3 ст. 159 УК РФ (Мошенничество, совершенное организованной груп в крупном размере) установлено, что ООО «Монолит» является фир -однодневкой, учрежденной по утраченному паспорту[1].

В случаях, когда мошенники обладают необходимой внутренней (инсай кой) информацией об осуществлении некоей организацией реальных

[1] Мошенники облапошили директора Базарно-Карабулакского мясокомбината // Саратовская областная газета (Саратов). 2006. 9 дек.

расчетов за приобретаемые товары с использованием платежных поручений, а также о реквизитах расчетных документов, обман может заключаться в изготовлении подделок реально оплаченных платежных поручений. Затем преступники, опережая подлинного плательщика, получают товары у поставщика по фиктивным платежным поручениям и доверенностям.

К описанным способам мошенничества примыкает использование в обманных целях платежных поручений, по которым денежные средства были перечислены, однако затем отозваны обратно до получения их контрагентом.

Например, в июне 1995 г. граждане Р., М. и Б., вступив между собой в сговор с целью похищения бюджетных средств, заключили с администрацией Мурманской области от лица учрежденных ими фирм эксклюзивные контракты на поставку областному комитету здравоохранения заграничного медоборудования и лекарств. После поступления бюджетных денег на счета их фирм, мошенники с целью маскировки преступных намерений перевели в феврале 1996 г. двум швейцарским и одной германской фирмам в качестве аванса за поставку медоборудования соответственно 300 тыс., 500 тыс. и 332 тыс. долл. Но, получив копии платежных поручений, через два дня отозвали платежи назад. Еще через несколько дней Разумовский с Блувштейном повторили эту комбинацию. А потом, собрав все ранее полученные копии платежных поручений и приложив к ним поддельное платежное поручение в Швейцарию на сумму более 1,8 млн долл., направили копии этих документов в администрацию Мурманской области в качестве подтверждения подготовки поставок. В действительности бюджетные деньги были переведены на счета учрежденной ими шведской компании «Разом скандинавиэн трейдинг АБ». Совершив хищение, мошенники скрылись за границей[1].

Отзыв платежных поручений, как способ обмана, может использоваться также для уклонения от ответственности за противоправные действия, выигрыша времени для проведения финансовых операций, препятствующих возврату похищенного имущества.

Так, бывший председатель совета директоров банка МЕНАТЕП некто Х. организовал приобретение принадлежащего Фонду имущества Мурманской области 20 пакета акций ОАО «Апатит» (г. Кировск Мурманской области), от имени подконтрольного ему АОЗТ «Волна». В связи с невыполнением АОЗТ «Волна» условий договора купли-продажи по внесению инвестиций и неперечислением до 1 сентября 1994 г. 168 млрд 951 млн неденоминированных рублей на специальный счет ОАО «Апатит» прокурор Мурманской области направил в Арбитражный суд Мурманской области исковое заявление о расторжении договора купли-продажи и возврате 20%-ного пакета акций Фонду имущества Мурманской области.

Намереваясь воспрепятствовать возврату акций их законному владельцу, Х. через подконтрольное ему лицо представил в Арбитражный суд Москвы

[1] Мошенники

атежные поручения № 20 от 10 августа 1995 г. на сумму 250 млрд неденом ированных рублей и № 22 от 11 августа 1995 г. на сумму 229 244 382 726 нед оминированных рублей, о перечислении указанных сумм со спецсчета АОЗ Волна» в банке МЕНАТЕП на расчетный счет ОАО «Апатит» в этом же бан качестве вложения инвестиций. С учетом указанных расчетных документ рбитражный суд Москвы своим решением от 16 августа 1995 г. в удовлетв ении иска прокурора Мурманской области отказал. Однако указанные п жи были фиктивными, так как в те же дни названные суммы были сно озвращены на указанный спецсчет АОЗТ «Волна».

Для уклонения от повторных исков о возврате имущества 20%-ный па ций ОАО «Апатит» под видом сделок купли-продажи от имени АОЗТ «Во а» был передан по частям в собственность шести подставных коммерческ рганизаций, учрежденных подконтрольными Ходорковскому оффшорны мпаниями. Уклониться от уголовной ответственности за мошенничест новные рассчитывали путем перевода совершенного хищения в категор битражных споров[1].

Использование поддельного платежного поручения для хищения денежных средст путем их перечисления со счета организации на другие счета

Для совершения обмана указанным способом от имени организации, кот й принадлежат похищаемые средства, в банк направляются поддельн латежные документы. В качестве основания для оплаты платежными поруч ями изготовляется фиктивный договор. Немаловажным является то обсто льство, что преступники нередко располагают инсайдерской информацие реквизитах расчетных счетов и некоторых элементах финансовой деятельно и организации, на которую направлено посягательство. Иногда преступле я совершают непосредственно бухгалтерские работники организации. Сп нные средства в одном случае могут быть переведены непосредствен счет лица, не осведомленного о подлинной сути операции, например, ба или организации-депозитария, поставщика товаров (услуг) и т. д. с цель лучения от них ценных бумаг или товаров. Для фактического получени нностей от неосведомленного посредника используются поддельные дове нности и паспорта.

В другом случае похищаемые средства списываются на счет специальн зданной фирмы-однодневки (лжекоммерческой организации), а затем об личиваются и присваиваются.

Иллюстрацией к первому варианту может служить факт хищения денежны едств со счета АООТ «Престус». Обслуживание банковского счета назван й организации согласно договору банковского счета от 3 января 1996 г. осу ствляло Ленинградское отделение одного из московских банков. 11 июня 6 г. в отделение банка было предъявлено платежное поручение от 11 июня

[1] Справка по уголовному делу № 18/41–03 // Коммерсантъ. 2003. № 198(2801). 29 окт.

1996 г. № 36, в соответствии с которым со счета АООТ «Престус» надлежало перечислить в обслуживающий банк 199 813 500 руб. на покупку облигаций государственного сберегательного займа по договору от 11 июня 1996 г. № 21411/20–96. В этот же день состоялись перевод денежных средств и получение облигаций неустановленным лицом по доверенности АООТ «Престус» от 11 июня 1996 г. № 26 и по утраченному паспорту.

Обнаружив списание денег со своего счета, АООТ «Престус» обратилось за экспертизой подлинности платежного поручения, договора купли-продажи облигаций и доверенности на их получение в Российский федеральный центр судебной экспертизы при Министерстве юстиции Российской Федерации. Согласно заключению Центра печати и подписи, выполненные на указанных документах, не принадлежали АООТ «Престус», его директору и главному бухгалтеру. В процессе проведенного расследования было установлено, что в период списания денежных средств директор и главный бухгалтер акционерного общества находились соответственно в командировке и в отпуске, поэтому платежного поручения, договора купли-продажи облигаций и доверенности на их получение они не подписывали.

Кроме того, из материалов дела следовало, что платежное поручение от 11 июня 1996 г. № 36 передано в банк неустановленным лицом, которое ранее не сдавало платежные документы от имени АООТ «Престус», а порядковый номер поручения значительно ниже предъявленных акционерным обществом к оплате в этот же период платежных документов. В ходе расследования уголовного дела, возбужденного по фактам подделки документов и хищения денежных средств АООТ «Престус», лицо, подлежащее привлечению в качестве обвиняемого, не было установлено[1].

Примером второго варианта являются действия некоего М., в апреле и мае 1997 г. временно исполнявшего обязанности бухгалтера ТОО «Валта». В указанный период М. изготовил и направил в филиал Инкомбанка за своей подписью и поддельной подписью первого лица ряд подложных платежных поручений, по которым с расчетного счета названной фирмы были списаны и похищены более 3,5 млрд руб.

Так, 28 апреля 1997 г. им было изготовлено и направлено в банк подложное платежное поручение № 97, по которому с расчетного счета ТОО «Валта» в филиале Инкомбанка по фиктивному основанию были перечислены на расчетный счет ЗАО ТФ «Тандем» 576 млн руб. 13 мая 1997 г. по изготовленному Мазуром платежному поручению № 98 с расчетного счета ТОО «Валта» в филиале Инкомбанка на расчетный счет ООО ФСК «ФК-Инвест» в отделении филиала Мосбизнесбанка были переведены 2 млрд 970 млн руб. по фиктивному договору № КФН/2350 о якобы предполагаемом финансировании ТОО «Валта» строительства жилого дома в Центральном административном округе Москвы.

[1] Постановление Президиума Высшего Арбитражного Суда Российской Федерации от 23 февраля 1999 г. № 6694/98.

Платежные поручения были скреплены оттисками поддельной печати. одлинная печать ТОО «Валта» до указанных событий была изъята органами лиции и находилась в распоряжении УЭП ГУВД г. Москвы. Все перечис нные выше денежные средства были впоследствии похищены. Сам М. по е совершения преступления скрылся[1].

Известен случай, когда филиал Инкомбанка перечислил по фальшивому атежному поручению (с поддельными подписью и печатью) со счета инсти га «Теплоэлектропроект» на счет фирмы-однодневки 400 тыс. долл. Эт ньги были похищены, а фирма исчезла. Аналогичным образом были пох ены около 200 млн руб. в «Мосбизнесбанке» и 1,5 млн долл. в «Российско циональном коммерческом банке».

Гражданское законодательство рассматривает списание банком денежн едств по платежному поручению с поддельными подписями и оттиском п ти как ненадлежащее совершение операций по счету. Согласно ст. 8 РФ, банк обязан возместить клиенту убытки, причиненные необоснова м списанием средств, в порядке и размерах, предусмотренных ст. 3 РФ. Как разъяснил Пленум Высшего Арбитражного Суда РФ в Постано нии от 19 апреля 1999 г. № 5 «О некоторых вопросах практики рассмотр я споров, связанных с заключением, исполнением и расторжением догов банковского счета», проверка полномочий лиц, которым предоставле во распоряжаться счетом, производится банком в порядке, определенно ковскими правилами и договором с клиентом. В случаях передачи плате документов в банк в письменной форме банк должен проверить по внеш признакам соответствие подписей уполномоченных лиц и печати на пе анном в банк документе образцам подписей и оттиска печати, содержа мся в переданной банку карточке.

Если иное не установлено договором, банк несет ответственность за по ствия неисполнения поручений, выданных неуполномоченными лицами, тех случаях, когда он, используя предусмотренные банковскими правила процедуры, не смог установить факта выдачи распоряжения неуполномо ными лицами.

Примером такого рода может служить судебное решение о возмещени тков, вызванных необоснованным списанием одним из московских бан со счета ООО «А» денежных средств в размере 8 690 797 руб. по поддель у платежному поручению от 4 марта 2002 г. № 815. В процессе уголовного следования по факту подделки документов и хищения денежных средств и получены заключения экспертиз о том, что подписи генерального ди ора ООО «А» и его главного бухгалтера на платежном поручении выпол ы не ими, а другими лицами, оттиск печати также сделан не печатью

Справка комиссии Государственной Думы Федерального Собрания Российской Федерации рьбе с коррупцией по результатам проверки материалов о хищении организованной группой енежных средств со счета ТОО «Валта» от 3 июня 2002 г. (www.nacbez.ru).

ООО «А». В рамках уголовного расследования была установлена и подложность доверенности на лицо, представившее в банк платежное поручение.

Согласно п. 3 ст. 401 ГК РФ, обстоятельством, освобождающим банк от ответственности в указанном случае, является воздействие непреодолимой силы, препятствующей исполнению обязательства по ведению счета.

По оценке суда противоправные действия третьих лиц к таковым не относятся. Следовательно, банк не принял всех мер к исключению возможности платежа по подложному документу и обязан возместить ООО «А» неправомерно списанные с его счета денежные средства[1].

В тех случаях, когда расчеты платежными поручениями ведутся в электронной форме, для изготовления поддельного платежного поручения может использоваться подлинный аналог электронной цифровой подписи, похищенный преступником либо доверенный ему.

Такого рода хищение денежных средств путем направления по электронной системе платежей «Клиент—Банк» подложного платежного поручения было совершено помощником главного бухгалтера одной из московских коммерческих организаций. Подготовка платежных поручений входила в круг обязанностей похитителя. Воспользовавшись компьютерной связью «Клиент—Банк» и дискетой с электронными подписями распорядителей кредитов, преступник при отсутствии соответствующего распоряжения владельца счета составил фиктивное платежное поручение и незаконно списал 3,2 млн долл. с валютного счета фирмы на заранее открытый по фиктивным документам валютный счет. В дальнейшем похищенные средства были переведены по подложным документам в один из коммерческих банков США.

В этом случае, благодаря своевременным и квалифицированным действиям сотрудников УЭП ГУВД Москвы и правоохранительных органов США, похищенные денежные средства были возвращены в Россию[2].

Использование поддельных платежных поручений для хищений денежных средств непосредственно у банка

Хищение денежных средств у банка с использованием поддельных платежных поручений совершают действующие или бывшие работники банка. В указанных целях могут использоваться поддельные платежные поручения как на бумажных носителях, так и их электронные аналоги.

Приемами хищения в названных случаях являются:

а) несанкционированное списание денежных средств плательщика на расчетный счет соучастника хищения.

В 1993 г., например, преступники списали со счетов Главного расчетно-кассового центра Главного управления Банка России (далее — ГРКЦ ГУ

[1] Федеральный арбитражный суд Московского округа. Дело № КГ-А 40/6121 от 22 июля 2004 г.

[2] Материалы Комитета по безопасности Ассоциации российских банков

Б РФ) по Москве деньги на сумму 68 млрд руб., осуществив несанкциониро-
ное «дописывание» платежных поручений в массив «операционного дн
пользу восьми коммерческих банков Москвы. Под проведенную электронную
оводку дополнительно в ГРКЦ ГУ ЦБ РФ были внедрены для дальнейшей
работки и рассылки по банкам фальшивые платежные поручения[1];

В июле 2005 г. хищение денежных средств из банка «Кедр» в Красноярске
вершил с использованием фиктивного платежного поручения программист
анского филиала банка. Незаконно проникнув в систему «Банк—Клиент»,
еступник перечислил 7,5 млн руб. в один из московских банков. Преступле-
ие было раскрыто службой безопасности банка «по горячим следам»[2].

б) несанкционированное зачисление вновь поступающих в банк средств
ательщика на расчетный счет соучастника хищения.

В августе 1995 г. из здания ГРКЦ ГУ ЦБ РФ по Москве были незаконно
несены подлинные платежные поручения, исходящие от расчетно-кассо-
х центров различных городов, заменены на поддельные с измененными
счетными счетами получателей и данными о назначении платежа, и внедре-
ы в систему расчетов. Денежные средства, поступившие по поддельным пла-
жным поручениям на счета соучастников преступления, были похищены[3].

Для изготовления поддельных платежных поручений на бумажных носите-
х фабрикуются поддельные оттиски печатей (с поддельных клише, путе-
анирования и т. п.). Возможны случаи использования подлинных печатей,
еменно попавших в руки преступников. Подделываются подписи уполно-
ченных лиц банка. Электронные же копии платежных поручений могут
ть заверены электронными аналогами подписей, носители которых вре-
нно вышли из законного владения либо похищены у уполномоченных лиц.

В качестве «промежуточного» получателя похищенных денег обычно вы-
упает физическое лицо, не осведомленное о подлинной сути готовящейся
ерации. Такие лица предоставляют свои документы для открытия счета
филиалах Сбербанка, получают поступившие на него деньги и передают
злоумышленникам. Действуют они за незначительное комиссионное воз-
граждение. В случае обнаружения причастности к хищению они утвержда-
, что поступившие на их счет суммы имели законное происхождение.

Предупреждение мошенничества при расчетах платежными поручениями

Предупреждение мошенничества в банке. В случаях передачи в банк платеж-
х документов на бумажном носителе следует проверить по внешним

[1] *Мельников Ю. Н.* Информационная безопасность в банке: Проблемы и рекомендации // ковские технологии. 1997. № 7. С. 18.

[2] Возбуждено уголовное дело по факту хищения из банка «Кедра» денежных средств // ИА пресс (Красноярск). 2005. 18 июля.

[3] Постановление Президиума Высшего Арбитражного Суда Российской Федерации от 24 де-ря 1996 г. № 3058/96.

признакам соответствие подписей уполномоченных лиц и печати на передан-
ном в банк документе образцам подписей и оттиска печати, содержащимся
в переданной банку карточке.

Проверить соответствие порядкового номера поступившего платежного поручения номерам предшествующих документов.

Перед списанием средств со счета клиента всеми возможными способами удостовериться в подлинности платежного поручения:

- установить канал поступления документа в банк (тщательно проверять и фиксировать данные лица, сдающего платежные поручения; обращать внимание на лиц, ранее не контактировавших с банком);
- проверить отсутствие внешних признаков подчисток и исправлений;
- проверить наличие на документе обязательных для платежного поручения реквизитов;
- сопоставить имеющиеся в платежном поручении реквизиты с реквизитами плательщика (банка-плательщика) и получателя (банка-получателя).

Проверить наличие основного договора, послужившего основанием для перевода денежных средств. Сопоставить содержание этих документов с содержанием платежного поручения. Наличие расхождений в содержании этих документов рассматривать как признак возможной подделки платежного поручения и основание для более глубокой проверки. В связи с тем что выявить признаки материального подлога трудно, следует получить в необходимых случаях прямое подтверждение факта выдачи платежного поручения от организации-плательщика.

Принять меры профилактического характера, препятствующие зачислению похищаемых средств на счета лжефирм и подставных лиц. С этой целью тщательно выполнять правила открытия расчетного (лицевого) счета. Внимательно изучать представленные учредительные и личные документы будущих владельцев счета.

Тщательно отслеживать и незамедлительно реагировать на случаи поступления неподтвержденных платежных поручений и попытки несанкционированного доступа к компьютерной информационной системе банка.

Предупреждение мошенничества в организации-плательщике. Установить ограниченный доступ сотрудников к работе с расчетными документами и информации о ведущихся и планируемых расчетах. Не допускать отклонений от порядка проведения операций, которые должны осуществляться только уполномоченными на то лицами и в строгом соответствии с определенными полномочиями и процедурой принятия решений.

Исключить возможность несанкционированного доступа неуполномоченных лиц к печатям и дискетам с электронными подписями распорядителей кредитов.

Предупреждение мошенничества в организации — получателе средств. Удостовериться в надежности и платежеспособности предполагаемого контрагента (по стандартной схеме). Проверить на соответствие фактическим данным

кие реквизиты предполагаемого контрагента, как наименование плательщи-
, номер его счета, ИНН; название и место нахождения банка-плательщика,
о БИК.

Проверить сведения о целях приобретения товара и механизме его даль-
йшего использования. Если, например, покупается мясо птицы для реали-
ции, выяснить, располагает ли организация штатом работников, торговыми
и перерабатывающими площадями, складами, холодильниками, транспор-
м.

При предъявлении расчетных документов проверить по внешним призна-
м их соответствие требованиям Положения Банка России № 2-П:

- наличие необходимых и отсутствие «избыточных», не предусмотренных Положением реквизитов. Правоохранительной практике известен случай разоблачения мошенника, предъявившего поставщику товаров последний экземпляр платежного поручения, скрепленного подписями уполномоченных лиц и печатью (реквизитов, которые проставляются только на первом экземпляре);
- отсутствие исправлений, помарок, подчисток и использования корректирующей жидкости;
- отсутствие внутренних несоответствий между платежным поручением и основным договором.

Тщательно проверить личные документы получателя товара и предъявляе
о этим лицом доверенность. Снять ксерокопию паспорта этого лица. Как
вило, мошенники используют утраченные или похищенные паспорта с пе-
леенной фотографией. Следы переклейки можно обнаружить при внима-
ьном осмотре, особенно при использовании лупы и источника ультрафио-
вого излучения (такие детекторы в виде авторучек продаются даже в ки-
ах печати).

Наиболее надежным способом защиты от обмана со стороны малоизвест-
о контрагента является заключение договора с условием предварительной
аты и отпуск товара после подтверждения банка о поступлении денег на
г получателя.

ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. В чем заключается отличие мошенничества под видом получения кредита от незаконного получения кредита?
2. Какие основные способы обмана и злоупотребления доверием применяются при совершении мошенничества под видом получения кредита и при незаконном получении кредита?
3. Какие действия следует выполнить для обеспечения безопасности кредитной операции?
4. Каковы основные способы хищения денежных средств банка с использованием пластиковых карт?
5. Какие меры организационного и технологического характера входят в программы предупреждения хищений с использованием пластиковых карт?
6. В чем заключаются основные способы обмана и злоупотребления доверием при расчетах по поддельному аккредитиву?
7. Какие действия следует предпринять с целью предупреждения потерь от мошенничества при расчетах по аккредитиву?
8. Какие способы фальсификации чеков и предъявления их к оплате применяют преступники?
9. Какие меры защиты должен предпринять банк для предупреждения хищений с использованием чека?
10. Каковы способы совершения хищений с использованием поддельного платежного поручения?
11. Какие действия должен выполнить банк для предупреждения хищений с использованием поддельного платежного поручения?

Глава 6

ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ И ИНОГО ИМУЩЕСТВА С ИСПОЛЬЗОВАНИЕМ ВЕКСЕЛЕЙ

- Правовая характеристика векселя
- Риски в сфере вексельного обращения
- Преступления против собственности, в которых вексель является предметом посягательства
- Преступления против собственности, в которых вексель является средством совершения преступления
- Меры предупреждения преступлений в сфере вексельного обращения

6.1. Правовая характеристика векселя

Действующее законодательство определяет *вексель* как ценную бумагу, удо-
веряющую с соблюдением установленной формы и обязательных реквизи
з имущественные права на получение денежных средств[1].

Основным источником регулирования вексельного оборота является По
жение о переводном и простом векселе, основанное на женевских вексель
х конвенциях 1930 г.[2] и введенное в действие постановлением ЦИК и СН
СР от 7 августа 1937 г. (далее — Положение). Действие названного Поло
ния на территории Российской Федерации подтверждено Федеральным за
ом от 11 марта 1997 г. № 48-ФЗ «О переводном и простом векселе» (да
— Закон о векселе).

Особенность вексельного законодательства состоит в том, что оно является
тко формализованной закрытой системой норм, регулирующих правоотно-
ния в указанной сфере, исходя исключительно из собственных «внутренних»
едписаний процессуального и материально-правового характера, не приме-
мых для регулирования других правоотношений.

Возможность изменения или отмены предписаний вексельного законода-
ьства другими формами права и применения законодательства по аналогии
лючается. В противоположность гражданскому законодательству, в век-
ьном праве действует принцип: запрещено все, что не разрешено. По этой
чине дефект формы векселя влечет за собой его недействительность без
едварительного признания этого факта судом[3].

---

[1] Статьи 142–143 ГК РФ.

[2] Конвенции, заключенные в Женеве 7 июня 1930 г.: «О единообразном законе о переводном
остом векселе»; «Конвенция, имеющая целью разрешение некоторых коллизий законов о пере-
ых и простых векселях»; «О гербовом сборе в отношении переводных и простых векселей».

[3] Подробнее о «дефекте формы векселя» см.: *Гудков Ф. А.* Вексель. Дефекты формы. (Мето-
выявления типичных ошибок). 2-е изд., исправ. и доп. М.: ЗАО ИПК «Интеркрим-пресс»,
. С. 13.

Гражданское право выступает в качестве дополнительного источника вексельного права. Нормы Гражданского кодекса РФ применительно к вексельному обороту используются прежде всего для рассмотрения обстоятельств возникновения (приобретения, утраты, восстановления) и передачи прав по векселю, решения вопросов об ответственности за неисполнение вексельных обязательств, признания полномочий лица на участие в вексельной сделке и др. Они действуют постольку, поскольку не противоречат закону о переводном и простом векселях[1].

Наиболее часто вексель используется в качестве инструмента *товарного кредита* (ст. 822 ГК РФ) и *коммерческого кредита* (ст. 823 ГК РФ) в сделках, связанных с авансом, предварительной оплатой, отсрочкой и рассрочкой оплаты товаров, работ или услуг. Форма вексельного кредита выгодна обеим сторонам. Заинтересованность кредитора (банка) объясняется тем, что деньги на время действия договора остаются в его распоряжении. Заемщик же получает вексельный кредит по уменьшенным процентным ставкам.

Исходя из ст. 815 ГК РФ вексель представляет собой документ, удостоверяющий ничем не обусловленное обязательство векселедателя (простой вексель) либо иного указанного в векселе плательщика (переводной вексель) выплатить по наступлении предусмотренного векселем срока полученные взаймы денежные суммы.

«Ничем не обусловленное обязательство» в вексельном праве отличается от обязательства гражданско-правового характера, в соответствии с которым обязанность одной стороны уплатить деньги другой стороне может быть обусловлена требованием совершить определенное действие, как то: передать имущество, выполнить работу и т. д.

Принципиальная разница между простым и переводным векселем заключается в следующем. Простой вексель представляет собой финансовый документ, содержащий прямое обязательство векселедателя уплатить оговоренную сумму приобретателю либо (по его приказу) любому другому лицу. В переводном же векселе выдавший его субъект предлагает третьему лицу (предприятию) уплатить указанную денежную сумму предъявителю векселя. Лицо, указанное в переводном векселе в качестве плательщика, может принять предложение об уплате (совершить акцепт) либо отказаться от него. Переводной вексель приобретает качества обязательства уплатить оговоренную сумму после совершения процедуры *акцептования* (согласия плательщика — *трассата* — на оплату). Векселя погашаются только в денежной форме.

В качестве векселедателей могут выступать юридические и физические лица. С 1992 г. выпуск векселей в России как банками, так и различными компаниями и местными администрациями приобрел взрывной характер. В отдельных случаях векселя крупных банков обеспечивались вексельным

---

[1] *Иоффе Л. Г.* Источники вексельного права // В мире права. 1999. № 1.

ручительством (авалем) Министерства финансов РФ. Наиболее ликвидны- считались векселя, выпускаемые нефтяным комплексом и энергосистема- . С 1995 г. «нефтяные» и «энергетические» векселя продаются на открытом нке как ценные бумаги[1].

Исходя из требований ст. 4 Закона о векселе переводной и простой векселя жны быть составлены только на бумаге (бумажном носителе).

Постановлением Правительства РФ от 26 сентября 1994 г. № 1094 «Об оформ- нии взаимной задолженности предприятий и организаций векселями единого разца и развития вексельного обращения» (в ред. Постановления Правительства 27 декабря 1995 г. № 1295) на территории Российской Федерации с 1 ноября 4 г. для использования в хозяйственном обороте введены единый образец бланка простого векселя и единый образец бланка переводного векселя.

Бланки указанных векселей изготавливаются типографией Гознака и по учению Министерства финансов РФ реализуются Главным управлением дерального казначейства коммерческим банкам через территориальные ор- ы Федерального казначейства для последующей реализации юридическим цам.

Следует иметь в виду, что образцы названных бланков носят рекоменда- ьный характер, а действие постановления не распространяется на векселя пускаемые коммерческими банками. Последние приобретают бланки ве- ей на предприятиях, способных изготовить их с достаточно высокой степе- защиты и имеющих лицензию. Технические требования к защищенност нков векселей утверждены Приказом Министерства финансов Росси февраля 2003 г. № 14н.

В соответствии с Федеральным законом от 8 августа 2001 г. № 128-Ф лицензировании отдельных видов деятельности» и Постановлением Пр ельства РФ от 11 ноября 2002 г. № 817 «Об утверждении Положения о л зировании деятельности по изготовлению защищенной от подделок пол фической продукции, в том числе бланков ценных бумаг, а также торгов анной продукцией», на 1 июля 2003 г. Минфин России предоставил 19 л зий на осуществление деятельности по изготовлению защищенной от по к полиграфической продукции, в том числе бланков ценных бумаг, а та торговли указанной продукцией.

В настоящее время правом на изготовление и торговлю бланками векселе дают: Московская печатная фабрика Объединения государственн приятий и организаций по производству государственных знаков — Об ения «Гознак» Министерства финансов Российской Федерации (госуда нное предприятие); Московская типография «Гознака» — государственн приятие; закрытое акционерное общество «Опцион» и другие предпр ы.

[1] Финансово-кредитный энциклопедический словарь / под общ. ред А. Г. Грязновой. нсы и статистика, 2002. С. 168.

Следует отметить, что законодательство не связывает действительность векселя с использованием специального бланка и расположением реквизитов по установленному образцу.

Для признания векселя действительным достаточно написать его на простом листе бумаги, однако документ должен быть составлен с соблюдением требований данного Положения о переводном и простом векселе и содержать все предусмотренные ст. 75 Положения реквизиты:

1) наименование «вексель», включенное в текст документа и выраженное на том языке, на котором этот документ составлен;
2) простое и ничем не обусловленное предложение уплатить определенную сумму;
3) наименование того, кто должен платить (плательщика);
4) указание срока платежа;
5) указание места, в котором должен быть совершен платеж;
6) наименование того, кому или по приказу кого платеж должен быть совершен;
7) указание даты и места составления векселя;
8) подпись того, кто выдает вексель (векселедателя).

6.2. Риски в сфере вексельного обращения

Использование в обороте векселей сопряжено с высокой степенью предпринимательского риска. Это объясняется рядом особенностей вексельного права.

1. Законодательство не устанавливает требований проверки и подтверждения обеспеченности векселя. Названная ценная бумага представляет собой передаваемое в упрощенном порядке абстрактное, формальное денежное обязательство, обеспечение которого вытекает исключительно из него самого. В связи с этим существует опасность приобретения так называемого пустого векселя.

2. Коммерческие организации имеют возможность приобретать права и принимать обязательства по векселям без каких-либо законодательно установленных ограничений. Поэтому проблемы кредитоспособности векселедателя и обращения его векселей являются в основном внутренним делом организации. Контроль за выдачей векселей кредитными организациями осуществляется опосредованно. Кредитные организации должны соблюдать установленные Банком России экономические нормативы, включающие обязательства по векселям, в том числе специальный норматив Н13, устанавливающий соотношение размера вексельных обязательств к величине капитала кредитной организации. Процесс же выдачи векселей некредитными организациями контролируется вовсе. Для них требования к кредитоспособности и выдаче векселей носят рекомендательный характер. В частности, коммерческим организациям, работающим в сфере торговой деятельности,

екомендуется при выдаче векселей обеспечить соблюдение показателей труктуры баланса, свидетельствующей об их платежеспособности.

3. Взыскание долгов по неоплаченным векселям через суд связано с пред ествующей иску процедурой протеста векселя. Упрощенный порядок взы кания долгов (безусловная вексельная сила), существовавший в стране в пе иод НЭПа, законодательством Российской Федерации не предусмотрен.

4. Под выдачей векселя понимается его выход из владения векселедателя ри любых обстоятельствах, в том числе против его воли (порок выдачи): при трате, ошибочной передаче, а также в результате хищения. Обстоятельства видетельствующие о пороке выдачи векселя, рассматриваются в рамках гра данского или уголовного права. При этом по обстоятельствам противопра ого выхода векселя из владения векселедателя отвечает лишь лицо, непо редственно к ним причастное.

В соответствии с п. 16 Положения о векселе лицо, которое приобрело вы ывший из владения (в том числе похищенный или утраченный) переводно ексель, рассматривается как законный векселедержатель. Оно обязано отдат ексель лишь в том случае, если приобрело его недобросовестно или же, при бретая его, совершило грубую неосторожность.

Обстоятельства противоправного приобретения векселя (так называемы орок, имевший место при выдаче) могут быть противопоставлены тольк епосредственному виновнику противоправных действий, но не последую им добросовестным приобретателям. Приобретатель векселя обладает пре умпцией, в соответствии с которой необходимость доказательства его не обросовестности, если это имело место, лежит на векселедателе или индос анте.

В соответствии с разъяснениями Пленума Верховного Суда РФ № 33, Пле ума высшего Арбитражного Суда РФ от 4 декабря 2000 г. № 14 приобрета ель считается недобросовестным, если он до или в момент приобретения нал о том, что вексель выбыл из владения собственника либо лица, уполно оченного распоряжаться векселем, помимо их воли. Грубая неосторожность риобретателя имеет место в том случае, когда приобретатель в силу сложив ихся условий оборота должен был знать о факте выбытия векселя из владе ия собственника, либо лица, уполномоченного распоряжаться векселем, по имо их воли (в частности, если вексель был приобретен после опубликова ия собственником в печати информации об утрате либо краже векселя, о чем риобретатель векселя по обстоятельствам дела не мог не знать, либо приоб етенный вексель имеет следы подчисток, видимых изменений текста и дру их подобных дефектов). При этом недобросовестность и грубая неосторож ость приобретателя доказываются в гражданско-правовом порядке лицом, редъявившим требование об изъятии векселя. Лицо же, обязанное по векселю, в случае предъявления требования об оплате векселя не вправе отказаться г исполнения со ссылкой на отсутствие основания обязательства либо его

недействительность, за исключением случаев, когда векселедержатель, приобретая вексель, действовал сознательно в ущерб должнику[1].

5. Векселедержатель, утративший вексель по тем или иным причинам, лишается вексельных прав, в том числе права на получение денег по этой ценной бумаге. Гражданско-правовой договор, послуживший основанием для установления вексельных отношений (об оплате векселем определенных действий: выполнения работ, передачи имущества и пр.), для вексельного права значения не имеет. В данном случае действует положение вексельного права: нет векселя — нет и прав кредитора.

Восстановление прав по утраченному векселю на предъявителя или признание векселя недействительным производится в порядке вызывного производства.

Однако в тех случаях, когда утраченный вексель был добросовестно приобретен до открытия вызывного производства, его законным собственником остается добросовестный приобретатель.

С невозможностью получить вексельную сумму с лица, ответственного по векселю в связи с непредъявлением векселя к платежу, столкнулось Таймырское региональное отделение Фонда социального страхования Российской Федерации (далее — отделение Фонда). Отделение Фонда 21 марта 1995 г. приобрело простой вексель № 531 номиналом 2 млрд руб. у Инновационного банка экономического сотрудничества, дополнительно оформив приобретение векселя договором. Обнаружив, что названный вексель утрачен при невыясненных обстоятельствах, отделение Фонда обратилось в Арбитражный суд Москвы с иском к Инновационному банку экономического сотрудничества о признании векселя № 531 утраченным, восстановлении права на утраченный вексель, *о взыскании 2 млрд руб. вексельной суммы и 1 млрд руб. годовых процентов* согласно договору на приобретение векселя.

Арбитражный суд Москвы Решением от 21 октября 1996 г. иск удовлетворил в сумме 2 млрд рублей, отказав во взыскании процентов. Постановлением апелляционной инстанции от 23 декабря 1996 г. решение было оставлено без изменения. В кассационном порядке законность и обоснованность решения и постановления не проверялись.

В дальнейшем, по протесту заместителя Председателя Высшего Арбитражного Суда РФ, состоявшиеся судебные акты были изменены. Президиум Высшего Арбитражного Суда РФ своим постановлением от 5 августа 1997 г. № 954/97 в иске о взыскании с ответчика 2 млрд руб. вексельной суммы отделению Фонда отказал. В обоснование данного решения были положены следующие доводы.

Согласно ст. 142 ГК РФ, ценной бумагой является документ, удостоверяющий с соблюдением установленной формы и обязательных реквизитов

[1] Постановление Пленума Верховного Суда РФ № 33, Пленума Высшего Арбитражного Суда РФ от 4 декабря 2000 г. № 14 «О некоторых вопросах практики рассмотрения споров, связанных с обращением векселей».

ущественные права, осуществление или передача которых возможны *толь-при его предъявлении.* Вексель относится к ценным бумагам и представляет бой письменный документ, содержащий простое и ничем не обусловленное язательство векселедателя (должника) уплатить определенную сумму денег определенный срок и в определенном месте векселедержателю или по его иказу. Поэтому для осуществления права требования платежа, выраженного векселе, *необходимо его предъявление, как это предусмотрено п. 38, 77 Поло-ения о переводном и простом векселе.*

Поскольку вексель не был предъявлен к платежу в связи с его утратой векселедержатель не представил доказательства о восстановлении его в пра- к по утраченной ценной бумаге, *оснований для взыскания вексельной суммы екселедателя не имеется.*

Довод Арбитражного суда Москвы о том, что требование отделения Фонда текает из обязательственных правоотношений и основано на договоре 21 марта 1995 г. № 1 о приобретении векселя, несостоятелен, так как со- асно ст. 815 ГК РФ в случаях, когда в соответствии с соглашением сторон емщиком выдан вексель, удостоверяющий ничем не обусловленное обяза- льство векселедателя (простой вексель) либо иного указанного в вексе- ателыцика (переводной вексель) выплатить по наступлении предусмотрен- го векселем срока полученные взаймы денежные суммы, отношения сторон векселю регулируются законом о переводном и простом векселе. С момен выдачи векселя нормы Гражданского кодекса РФ могут применяться к эти ношениям постольку, поскольку они не противоречат закону о переводно простом векселе.

6. Еще одна немаловажная проблема заключается в неосведомленности астников вексельных сделок о многочисленных особенностях вексельного ава. Это обстоятельство нередко используется недобросовестными партне- ми (и преступниками), которые умышленно нарушают обязательные требо- ния к юридическому оформлению векселя, приводящие к лишению его ксельной силы по причине «дефекта формы». Это дает им возможность от- аться от выплаты вексельной суммы на «законном» основании. Иски озмещении ущерба векселедержателя в гражданско-правовом порядке судом и наличии указанных обстоятельств не удовлетворяют.

Наряду со значительными предпринимательскими рисками для вексельного рынка характерно присутствие разнообразных рисков криминального ха- ктера. Причины привлекательности вексельного рынка для преступников лючаются в ряде особенностей вексельного права, предполагающих высо- й уровень взаимного доверия участников вексельных сделок (в том числе инцип презумпции добросовестности держателя похищенного либо под- ьного векселя), а также в отсутствии эффективного механизма контроля выдачей и обращением векселей и в определенных сложностях правовой щиты интересов добросовестных участников вексельных сделок.

Ежегодный рост «вексельных» преступлений в России составляет около 5%. Год от года повышаются уровень «квалификации» преступников и тяжесть последствий совершенных преступлений. По данным Следственного комитета при МВД России, за 11 месяцев 2007 г. у преступников изъято фальшивых и неликвидных векселей на сумму свыше 12 трлн руб. и 200 млн долл. Появление фальшивок зафиксировано в 23 регионах страны. МВД России отмечает, что мошенничество с векселями становится наиболее распространенным видом преступлений в кредитно-финансовой сфере.

Преступления в сфере вексельного обращения совершаются по двум основным направлениям. Первое — хищение подлинных векселей. Второе — подделка векселей и их использование в качестве средства совершения преступления.

6.3. Преступления против собственности, в которых вексель является предметом посягательства

По данным российских правоохранительных органов, в числе наиболее распространенных способов хищения векселей выделяются кража (ст. 158 УК РФ) и мошенничество (ст. 159 УК РФ). Вслед за ними идут присвоение и растрата (ст. 160 УК РФ), причиняющие порой весьма ощутимый ущерб собственникам ценных бумаг. Наряду с перечисленными выше способами тайных (относительно замаскированных) хищений правоохранительные органы фиксируют случаи совершения грабежей и разбоев с целью завладения векселями. В ноябре 2007 г. Свердловским областным судом осуждена группа преступников, совершивших 15 июля 2005 г. разбойное нападение и убийство директора ООО «Компания морепродукты» с целью завладения находившимися у погибшего векселями на сумму 20 млн руб. Похищенные векселя позднее были обналичены преступниками в различных банках на общую сумму12 млн руб.

К преступлениям второй группы относятся противоправные деяния в сфере экономической деятельности, описанные в главе 22 УК РФ. Это легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174); легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления (ст. 174.1); незаконное получение кредита (ст. 176); изготовление или сбыт поддельных денег или ценных бумаг (ст. 186).

Каждая из названных групп имеет свои специфические подвиды, объединяющиеся как на основе уголовно-правовой квалификации, так и по признакам криминалистической характеристики.

Хищение векселя путем кражи

Кража является преступлением, предусмотренным ст. 158 УК РФ. Часть 1 ст. 158 УК РФ определяет кражу как тайное хищение чужого имущества.

понятие имущества законодатель, наряду с товаро-материальными ценностями и деньгами, включает ценные бумаги, к числу которых отнесен вексель.

Под объективным признаком тайного хищения чужого имущества следует понимать скрытность преступного акта как от собственника, так и от других лиц.

Статья 158 УК РФ предусматривает три вида краж: простая — ч. 1 ст. 158 УК РФ; квалифицированная (ч. 2) и особо квалифицированная (ч. 3 и 4).

Наказание, предусмотренное ч. 1 ст. 158 УК РФ, может быть назначено в виде штрафа в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательных работ на срок до ста восьмидесяти часов, либо исправительных работ на срок от шести месяцев до одного года, либо ареста на срок от двух до четырех месяцев, либо лишения свободы на срок до двух лет.

Часть 2 ст. 158 УК РФ устанавливает повышенную ответственность за кражу, совершенную:

а) группой лиц по предварительному сговору;

б) с незаконным проникновением в жилище, помещение либо иное хранилище;

в) с причинением значительного ущерба гражданину;

г) из одежды, сумки или другой ручной клади, находившихся при потерпевшем.

Наказание, предусмотренное ч. 2 ст. 158 УК РФ, может быть назначено в виде штрафа в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательных работ на срок от ста восьмидесяти до двухсот сорока часов, либо исправительных работ на срок от одного года до двух лет, либо лишения свободы на срок до пяти лет.

Часть 3 ст. 158 УК РФ предусматривает ответственность за кражу, совершенную с незаконным проникновением в жилище, либо в крупном размере. Кража, совершенная указанным способом, наказывается штрафом в размере от 100 тыс. до 500 тыс. руб. или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо лишением свободы на срок от двух до шести лет со штрафом в размере до пятидесяти минимальных размеров оплаты труда, или в размере заработной платы или иного дохода осужденного за период до шести месяца, либо без такового.

Часть 4 ст. 158 УК РФ предусматривает ответственность за особо квалифицированную кражу, совершенную:

а) организованной группой;

б) в особо крупном размере.

Наказание, предусмотренное ч. 4 ст. 158 УК РФ, может быть назначено в виде лишения свободы на срок от пяти до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет, либо без такового.

Место кражи векселей. В большинстве случаев векселя похищаются в процессе хранения или обработки этих ценных бумаг в банках или иных организациях. Это может быть организация-векселедатель или векселедержатель, организация-посредник (депозитарий). В числе потерпевших от краж ценных бумаг, наряду со скромными коммерческими фирмами, не имеющими достаточных средств на обеспечение защиты собственных интересов, нередко оказываются органы власти, крупные банки с мощными службами безопасности.

Так, в марте 2003 г. 30 простых векселей по 1,5 млн руб. каждый похищены в одном из отделений Сбербанка России. В апреле 2004 г. 46 простых векселей на сумму 62 006 000 руб. исчезли из депозитарного хранилища биржи «Санкт-Петербург»[1]. В августе того же года было обнаружено хищение векселей на сумму 767 200 000 руб. в ООО КБ «Содбизнесбанк».

По данным АУВЕР, на начало декабря 2006 г., в розыске находились векселя номиналом от 15 000 руб. до 1 000 000 евро, похищенные у 34 субъектов, в числе которых государственные предприятия, субъекты Федерации, правоохранительные органы, предприниматели и банки.

От преступных посягательств на вексель не застрахованы и сами службы безопасности. В 1999 г. вексель номиналом в 1 000 000 руб. был похищен в одном из московских агентств безопасности. Известны случаи хищения векселей в правоохранительных органах[2].

Как показывает следственная и судебная практика, кражи векселей случаются *в процессе их перевозки* в специальных *транспортных средствах* и средствах общественного транспорта, а также в процессе *временного нахождения* векселей у ответственных за них лиц *в номерах гостиниц, квартирах и в некоторых других местах.*

Лица, похищающие векселя в организациях. Кражи векселей в кредитных и иных организациях совершаются:

а) сотрудниками организации;

б) сотрудниками организации в соучастии с посторонними лицами;

в) посторонними лицами, которые не являются сотрудниками организации.

В указанных выше случаях речь идет о сотрудниках организации, не обладающих никакими правомочиями в отношении похищаемого векселя, поскольку тайное изъятие векселя, вверенного виновному, следует квалифицировать как присвоение в соответствии со ст. 160 УК РФ.

Особенности краж векселей, совершаемых в банках и иных организациях. Выбор способа похищения документа в организации чаще всего определяется наличием тех или иных отступлений от правил хранения ценных бумаг, снижающих степень защищенности объекта посягательства.

---

[1] Материалы уголовного дела № 741 557, расследованного прокуратурой Василеостровского района Санкт-Петербурга.

[2] Ассоциация участников вексельного рынка // Информация о ценных бумагах, выбывших из законного оборота (www.auver.ru).

Подготовительные действия похитителей нередко направлены на выявле-ие устойчивых нарушений порядка хранения ценных бумаг с целью выбора ситуации, удобной для тайного завладения ими.

Похитители ищут возможность бесконтрольного пребывания в помеще-ии, где хранятся или обрабатываются ценные бумаги, пытаются получить свое пользование ключи от указанного помещения или сейфа. Заранее гото-ят тайники для краткосрочного хранения похищенного.

Указанные действия могут дополняться: подысканием соучастников пре-тупления; изготовлением, приисканием орудия совершения преступления; странением обстоятельств, препятствующих похищению. Например, рабо-ик одной из российских фирм Н., имея возможность бесконтрольного пр-ывания в помещении банка, где хранились ценные бумаги, обнаружил, ч-ответственный за них сотрудник периодически оставляет ключи от сей-письменном столе, а контроль за сохранностью ценных бумаг практичес-сутствует. Воспользовавшись этим, он похитил вексель номиналом бол-млн руб., который передал соучастникам для реализации. Факт кражи обн-жился лишь после того, как вексель был предъявлен к оплате добросовес-ым приобретателем.

Способы незаконного изъятия векселя. Установлено, что более половины п-щенных ценных бумаг в организациях изъято из запертых хранилищ, нах-вшихся в служебных кабинетах охраняемых помещений, с использовани-гатного ключа. Похитители использовали основной или запасной ключ-анившиеся в ненадлежащем месте. В ряде случаев ключи (или их дублик-) похищались у ответственного лица или присваивались при передаче хр-лица в пользование других работников. Не исключена также возможнос-хищения векселя вместе с сейфом. Именно таким способом 19 июля 2001-л украден из офиса векселедержателя — Негосударственного пенсионно-нда «К» в Москве вексель номиналом более 1 млн руб., выпущенный од-м из московских коммерческих банков.

Следующее место по распространенности занимает изъятие ценных бума-авленных на время вне сейфа в служебном кабинете. Похитители проник-в указанные помещения через незапертую дверь; либо применяют ключ-ычку и другие приспособления; иногда используют незакрытое окно.

Специфическую разновидность краж представляют собой случаи противо-авного изъятия ценных бумаг, не обеспеченных должной охраной, в про-се их перемещения в транспортных средствах (самолетах и поездах), время хранения в номерах и сейфах гостиниц и других местах проживания. азанные кражи могут иметь целью завладение конкретной ценной бумагой ть «заказными»). В таких случаях маршруты перемещения ценных бумаг анее отслеживаются, изучается поведение ответственного за них лица. оме того, вексель или другая ценная бумага может стать случайной «добы-» преступника, умысел которого был направлен на похищение имущества обще» (чемодан, портфель и т. д.).

Цели кражи векселей:

- сбыт векселя добросовестному (не осведомленному о дефекте выдачи) приобретателю;
- получение денежных средств путем предъявления похищенного векселя к оплате;
- лишение векселедержателя возможности предъявить ценную бумагу к оплате (с целью присвоения вексельной суммы векселедателем);
- использование векселя в целях подделки и совершения мошенничества.

Кражи векселей выявляются в связи с обнаружением специфических следов этого преступления и отсутствием векселя по месту хранения либо в связи с появлением векселя у другого владельца (в том числе в связи с предъявлением к оплате векселедателю). Нередко вексель исчезает из владения векселедержателя при невыясненных обстоятельствах. Такое событие рассматривается как утрата ценной бумаги.

Утрата векселя как признак возможного хищения ценной бумаги. В практике владельцев ценных бумаг имеют место случаи, когда вексель исчезает при невыясненных обстоятельствах. Отсутствие векселя по месту хранения в таких случаях предстает в качестве события утраты.

По данным АУВЕР, с ноября 2000 г. по декабрь 2006 г. официально заявлено об утрате при невыясненных обстоятельствах 248 векселей. Большинство ценных бумаг обладает весьма значительной номинальной стоимостью. Так, КБ «Газпромбанк» заявил об утрате векселя номиналом в 2 млн руб., выпущенного ОАО «Газпром» со сроком предъявления к платежу 26 июня 2002 г. А в 2005 г. векселедержателем ООО «Норд» был утрачен простой вексель АБ «Газпромбанк» серии ГПБ № 0197 224 на сумму 3 млн руб.

Утрата ценной бумаги в большинстве случаев представляет собой замаскированную кражу. О раскрытии краж векселей, ранее объявлявшихся утраченными, а также о появлении «утраченных» векселей в обращении периодически сообщается в специализированных информационных системах ФИС и АУВЕР в сети Интернет, а также на страницах периодической печати.

Всего, по данным АУВЕР, по состоянию на начало 2008 г. в розыске находилось более 300 похищенных и утраченных при невыясненных обстоятельствах векселей номиналом от 10 тыс. до 5 млн руб. В связи с этим особый интерес для лиц, изучающих факт исчезновения векселя при невыясненных обстоятельствах, представляют следующие возможные признаки умышленных действий преступника.

1. Отсутствие векселя в месте хранения, когда выход его из владения другим способом исключается.
2. Одновременное либо последовательное исчезновение нескольких ценных бумаг, а также бланков векселей, хранившихся в одном или разных местах (сейфах), либо использовавшихся в работе.
3. Исчезновение, наряду с утраченным векселем, денег, ценных предметов, личных вещей, хранившихся в сейфе или в служебном кабинете, где находился сейф.

4. Вывод из строя либо отключение защитной сигнализации помещения, котором хранилась ценная бумага.

5. Наличие обстоятельств, свидетельствующих о намерении похитителя зорганизовать работу организации либо отдельного лица, с целью сокрытия ледов другого преступления (исчезновение документа накануне аудиторской роверки, разбирательства по факту злоупотреблений отдельных лиц и т. п.).

6. Появление ценной бумаги в распоряжении других организаций.

Бланк векселя как предмет противоправных посягательств. Способы противоправного завладения бланком векселя по объективной стороне в большинстве случаев совпадают с кражей или присвоением ценной бумаги, однако ража бланка совершается для последующей подделки в мошеннических целях и поэтому в строго правовом смысле слова рассматривается как приготовление к мошенничеству (ст. 30, 159 УК РФ)[1].

Как правило, кражи бланков векселей первоначально обнаруживаются в виде события их утраты при невыясненных обстоятельствах. Такие события имеют место в организациях-векселедателях, а также на предприятиях, осуществляющих изготовление, хранение и рассылку бланков.

В декабре 1996 г., например, была обнаружена утрата 999 бланков простых векселей в Главном управлении федерального казначейства Министерства финансов РФ[2]. В феврале 1997 г. там же была выявлена утрата бланков переводных векселей общим количеством 1040 ед.[3]

Факты утраты и похищения бланков у векселедателей также довольно распространенное явление. Об этом можно судить по периодически появляющимся сообщениям в разделе «Информация о ценных бумагах, выбывших з законного оборота» на странице АУВЕР в Интернете.

О том, что утраченные бланки были похищены, как правило, становится известным в связи с их обнаружением у другого владельца (в том числе в связи с попыткой реализации или оконченной реализацией поддельной ценной маги, выполненной с использованием похищенного бланка).

Похищения аннулированных векселей и бланков векселей. Определенное совпадение по цели с кражами бланков имеют случаи похищения (утраты) аннулированных (оплаченных и переоформленных) векселей. К примеру, 12 февраля 2002 г. один из московских банков обнаружил утрату 54 оплаченных и ранее векселей. Такие векселя, попадая в руки преступников, могут использоваться в мошеннических операциях, виды которых будут рассмотрены ниже. В случаях похищения указанные ценные бумаги тайно изымаются из массивов соответствующих архивных документов либо утаиваются в процессе уничтожения по истечении срока хранения.

[1] В целях удобства описания таких действий далее будет использоваться «юридически неюгий» термин «кража бланков векселей».

[2] Информационное письмо Министерства финансов РФ от 6 декабря 1996 г. № 03-А5–10/65 б аннулировании бланков простых веселей».

[3] Письмо Министерства финансов РФ от 4 февраля 1997 г. № 03-А5–10/11.

Как правило, меры по защите аннулированных векселей от хищений заметно уступают по надежности мерам обеспечения сохранности неоплаченных ценных бумаг. Именно на это обстоятельство и рассчитывают похитители в указанных случаях. Особенность похищения документов, подлежащих уничтожению, заключается в трудности выявления указанных фактов.

Следы кражи ценной бумаги (векселя). Умышленные посягательства на кражу с криминалистической точки зрения характеризуются наличием специфических материальных следов в месте хранения векселя.

Ими являются:

- следы несанкционированного отпирания сейфа — трасы нештатного ключа или отмычки, металлические опилки на деталях и коробе замка;
- нарушение целостности печати либо следы ее временного удаления (с последующим восстановлением) путем срезания, отделения от корпуса хранилища после замораживания, выворачивания проушин, крепящих приспособление для опечатывания;
- следы использования запасного ключа, хранящегося в установленном месте (вскрытие пакета или пенала одним из способов);
- следы повреждения корпуса сейфа — взлом, отжим, разрезание;
- следы рук и одежды на корпусе сейфа, а также на документах и предметах, оставшихся после похищения в хранилище, в том числе частицы кожи и следы крови на острых кромках;
- следы извлечения документа через проем поврежденного хранилища;
- следы проникновения и пребывания постороннего в помещении, где обнаружено отсутствие ценной бумаги;
- вывод из строя или отключение защитной сигнализации;
- признаки отпирания двери помещения нештатным ключом или отмычкой, отжима двери или ригеля замка, запирание двери необычным способом (например, запирание одного из нескольких замков двери, который обычно не использовался либо наоборот — оставление одного из замков незапертым);
- признаки проникновения в помещение через окно либо каким-нибудь другим способом;
- следы рук, ног постороннего в помещении, выброшенные или оброненные им предметы.

Характерные материальные следы в ходе преодоления защитных средств, вскрытия сейфа остаются на самом похитителе и его одежде. К ним относятся ссадины, царапины, опилки, микрочастицы краски, металла и т. п. Кроме того, на похищенном векселе, в случае его последующего обнаружения, могут быть выявлены отпечатки пальцев похитителя.

Воспрепятствование расследованию кражи. Способы воспрепятствования расследованию кражи векселя, совершенной лицами, посторонними по отношению к организации — потерпевшему, не имеют принципиальных отличий от противодействия расследованию других видов краж. Это могут быть

одробно описанные в учебниках криминалистики сокрытие похищенного, ничтожение следов, маскировка внешнего вида похитителя, создание ложных следов и т. д.[1]

Среди способов воспрепятствования расследованию кражи векселя, совершаемой сотрудниками организации следует отметить:

- сокрытие факта кражи путем использования приспособления, позволяющего виновному извлекать векселя из хранилищ без их взлома (штатные и поддельные ключи от хранилищ, отмычки, поддельные печати для опечатывания и т. д.);
- сокрытие факта отсутствия похищенного векселя путем его подмены качественно изготовленной копией, подлинным векселем из другого массива документов либо аннулированным векселем;
- создание ложного алиби путем фальсификации времени и обстоятельств выхода векселя из законного владения;
- сокрытие своего участия в краже ценной бумаги путем сообщения ложной информации, свидетельствующей об утере векселя, ошибочных передаче другому лицу или засылке по почте ответственным лицом.

Хищение векселя путем присвоения

Правовая характеристика присвоения. Присвоение и растрата — две самостоятельные формы хищения чужого имущества. Ответственность за них установлена ст. 160 УК РФ. Далее исходя из практической целесообразности будет рассматриваться лишь одна из названных форм, а именно хищение векселя путем присвоения.

Статья 160 УК РФ предусматривает три вида присвоения: простая (ч. 1), квалифицированная (ч. 2) и особо квалифицированная (ч. 3 и 4).

Наказание, предусмотренное ч. 1 ст. 160 УК РФ, может быть назначено в виде штрафа в размере до 120 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательных работ на срок до 120 ч, либо исправительных работ на срок до шести месяцев, либо лишения свободы на срок до двух лет.

Часть 2 ст. 160 УК РФ устанавливает повышенную ответственность за присвоение, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину.

Перечисленные деяния наказываются штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо лишением свободы на срок до пяти лет.

[1] Криминалистика: учеб. для вузов / под ред. проф. А. Ф. Волынского. М.: Закон и право; ЮНИТИ-Дана, 2000. С. 239–250.

Часть 3 ст. 160 УК РФ устанавливает признаки особо квалифицированного состава присвоения, к которым относятся: совершение деяния лицом с использованием своего служебного положения, а равно в крупном размере.

Перечисленные в ч. 3 ст. 160 УК РФ деяния могут повлечь наказание в виде штрафа в размере от 100 тыс. до 500 тыс. руб. или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо лишением свободы на срок от двух до шести лет со штрафом в размере до десяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного месяца, либо без такового.

Часть 4 ст. 160 УК РФ устанавливает признаки особо квалифицированных составов присвоения, к которым относятся деяния, предусмотренные частями первой, второй или третьей названной статьи, совершенные организованной группой либо в особо крупном размере.

Перечисленные деяния наказываются лишением свободы на срок от пяти до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет, либо без такового.

Основным признаком, отличающим указанную форму хищения от кражи, является отношение субъекта преступления к похищаемому имуществу (векселю). При присвоении имущество не только вверено виновному, находится в его правомерном владении, но похититель наделен относительно этого имущества определенными правомочиями. При краже же субъект либо вообще не имеет никакого отношения к похищаемому имуществу, либо получает лишь доступ к нему для выполнения чисто технических, производственных функций, которые, однако, не порождают на его стороне никаких правомочий по владению, пользованию, распоряжению или ответственной охране.

Субъектом присвоения могут быть как должностные, так и недолжностные работники различных организаций, в том числе и коммерческих структур, достигшие 16-летнего возраста. Субъектом данного преступления может быть и иной гражданин, получивший определенные правомочия в отношении векселя.

Присвоение признается оконченным с момента изъятия векселя из имущества собственника и одновременного присоединения к имуществу похитителя с целью распорядиться им как своим собственным. Последующие действия виновного, относящиеся к неправомерному использованию присвоенного векселя, лежат за пределами состава преступления.

Основным отличием присвоения векселя от кражи с криминалистической точки зрения является отсутствие следов преодоления средств физической защиты места его хранения.

Субъект преступления имеет официально разрешенный доступ к названной ценной бумаге и необходимости вскрывать хранилище путем взлома,

спользования специальных приспособлений и т. п. не имеет (за исключени-
и случаев инсценировки кражи).

Цели присвоения векселя не отличаются от целей кражи. Мотивом, как при краже, является корысть.

Обстоятельства, при которых выявляется присвоение векселя. Присвоение ;кселя выявляется в связи:

- с отсутствием названной ценной бумаги по месту хранения по невыяс-ненным обстоятельствам (в этом случае событие первоначально пред-стает в виде утраты векселя);
- с обнаружением следов инсценировки кражи векселя;
- с обнаружением векселя у другого владельца (в том числе при предъяв-лении к оплате).

Следы присвоения векселя могут представлять собой материальное или ид-ьное отражение любого из элементов имевшего место события присвоени-кселя. Однако в большинстве случаев они оставляются преимущественно лью воспрепятствования расследованию.

Воспрепятствование расследованию присвоения векселя осуществляется виде:

- утаивания факта отсутствия ценной бумаги в активной либо пассивной форме. К числу активных способов утаивания относятся: подмена век-селя качественно изготовленной копией, подлинным векселем из дру-гого массива документов либо аннулированным векселем. Пассивным способом утаивания является умолчание о факте отсутствия векселя;
- уничтожения документов, связанных с движением векселя;
- фальсификации обстоятельств выхода векселя из законного владения: заведомо ложные показания; создание ложных следов и иных доказа-тельств; внесение исправлений в учетные документы, фиксирующие движение векселей;
- создания ложного алиби путем фальсификации времени и обстоя-тельств выхода векселя из законного владения;
- сокрытия своего участия в краже ценной бумаги путем сообщения ложной информации, свидетельствующей об утере векселя, его ошибочной пере-даче другому лицу, ошибочной засылке по почте ответственным лицом.

Хищение векселя путем мошенничества

В отличие от кражи, потерпевший «добровольно» передает либо выдает сель мошеннику под влиянием обмана.

Основные способы обмана и злоупотребления доверием, которые применяются мошеннического завладения векселем, включают в себя:

- подмену подлинного векселя на поддельный в процессе купли-продажи ценной бумаги, предъявления векселя к оплате либо иных действий, связанных с временным выходом векселя из владения потерпевшего;

- завладение векселем под видом его покупки, с использованием под-дельных документов об оплате;
- завладение векселем в обмен на несуществующие товары, неоказанные услуги;
- завладение векселем путем обманного получения ценной бумаги под предлогом его необходимости для процедуры подготовки к заключению будущей сделки;
- завладение ранее проданным векселем под видом восстановления права на утраченную ценную бумагу.

Рассмотрим названные способы подробнее.

Подмена подлинного векселя на поддельный в процессе купли-продажи ценной бумаги предполагает подготовительные действия мошенников в виде изготов-ления высококачественной копии подлинной ценной бумаги. Копия может быть снята до того, как вексель стал собственностью продавца, либо уже во время нахождения ценной бумаги у векселедателя. В последнем случае в качестве соучастников мошенничества выступают так называемые инсайде-ры — сотрудники организации — держателя векселя. Следующий этап совер-шения преступления предполагает ведение «переговоров» (возможно, неодно-кратных) об условиях сделки, ее цене и т. д., во время которых и совершается акт подмены. Подмена подлинных ценных бумаг на фальшивые с такими же реквизитами была использована мошенниками для хищения двух простых векселей ОАО «Газпром» номинальной стоимостью 3 млн руб. каждый у одно-го из банков Ростова-на-Дону. Ценные бумаги были похищены некими «пред-ставителями» фиктивной фирмы ОАО «Ц-И» в процессе очередного этапа пе-реговоров о заключении сделки купли-продажи векселей 26 февраля 2001 г. Убытков от этого хищения банку удалось избежать лишь за счет обнаружения подделки в день совершения преступления и умелых и безотлагательных дей-ствий по блокированию описанных ценных бумаг[1].

Подмена подлинного векселя на поддельный в процессе предъявления векселя к оплате векселедателю. Приготовление к совершению преступления включа-ет в себя действия, призванные вызвать доверие к мошеннику и заинтересо-вать векселедателя выгодными условиями финансового сотрудничества.

С этими целями преступник неоднократно совершает вексельные операции с векселедателем и аккуратно выполняет свою часть обязательств, прямо или косвенно демонстрируя заботу о своей деловой репутации. Сделки заключа-ются на весьма привлекательных для векселедателя условиях. Приобретя в очередной раз вексель на весьма значительную сумму, похититель (имея в своем распоряжении подлинник) изготавливает высококачественную копию ценной бумаги. В процессе приготовления подыскиваются возможные соучаст-ники преступления. Их роль может заключаться в изготовлении подделки, в участии противодействию расследованию тем или иным путем.

[1] Дело № Ф08–215/2003 Арбитражного суда Ростовской области.

На следующем этапе преступных действий мошенник в оговоренный срок предъявляет поддельный вексель вместо подлинного к оплате векселедателю. Плательщик, как правило, оплачивает ценную бумагу без тщательной проверки подлинности векселя. Недостатку внимания с его стороны способствуют: мнимое узнавание «собственного» векселя; подтверждение факта его выдачи и предстоящей оплаты внутренними учетными документами (реестром) организации-векселедателя; «хорошо» знакомый контрагент — первый векселедержатель.

Не исключено использование в указанной мошеннической схеме и сразу двух документов — подлинника и подделки. В этом случае первоначально будет предъявлен к оплате подлинный вексель. После проверки его подлинности ценная бумага под заранее продуманным предлогом на короткое время передается в руки мошенника, который производит ее подмену на поддельную практически в присутствии плательщика по векселю.

Одновременно с предъявлением поддельного векселя к оплате векселедателю мошенник продает подлинный вексель другому лицу, которое затем также предъявляет его к оплате. Не исключается, что это лицо осведомлено о мошеннических действиях предыдущего собственника векселя и действует в сговоре с ним. В случае отказа векселедателя оплатить вексель последний собственник ценной бумаги обращается с иском в арбитражный суд, который обязывает векселедателя выплатить вексельную сумму.

Противодействие расследованию мошенничества со стороны лица, предъявившего к оплате подделку, может заключаться в маскировке субъекта преступления (использование фальшивого паспорта) либо в его сокрытии. Не исключена ситуация получения вексельной суммы по доверенности субъектом с поддельным паспортом. В таком случае установление подлинных виновников преступления еще более затрудняется.

Следует помнить, что передача (даже кратковременная) ценной бумаги другим лицам после принятия ее к оплате недопустима. Если же такая передача имела место, процедуру проверки подлинности векселя следует проводить заново в полном объеме.

К числу трудностей расследования следует отнести установленный правилами вексельного обращения запрет на задержание плательщиком подложного или утраченного векселя в случае его предъявления к оплате. Такой вексель должен быть возвращен предъявившему его лицу. В противном случае нарушается право обладателя подделки на регрессный иск в отношении лиц, поставивших на документе свои подлинные подписи. О факте предъявления поддельного векселя плательщик должен поставить в известность органы внутренних дел.

Характерной особенностью ситуаций подобного рода является нежелание правоохранительных органов разбираться в сложных механизмах вексельных взаимоотношений и стремление направить разбирательство в русло арбитражного процесса, не имеющего эффективных механизмов борьбы с мошенниками.

Подмена подлинного векселя на поддельный в процессе выдачи ценной бумаги. Наряду с подменой векселя в процессе предъявления к оплате мошеннические действия указанного рода могут иметь место и при выдаче векселя.

На этапе подготовки к совершению преступления мошенники заранее изготавливают поддельный вексель. В процессе выдачи подлинный вексель подменяется на бумагу, имеющую признаки подделки. Фальсификация обнаруживается в процессе предъявления векселя к оплате. Смысл подмены заключается в заранее задуманном отказе от уплаты по векселю. Подмена подлинного векселя на фальшивый может иметь место и при передаче векселя по индоссаменту новому владельцу.

Случай подмены подлинника векселя имел место в сделке, совершенной между Санкт-Петербургским акционерным коммерческим банком «Таврический» (далее — банк «Таврический») и ОАО «МВЦ «Северсталь». Названный банк 20 февраля 1998 г. приобрел у ОАО «МВЦ «Северсталь» вексель № 027 602 и затем продал его одной из коммерческих организаций. В дальнейшем вексель использовался для расчетов рядом юридических лиц, однако 6 апреля 1998 г. был изъят по постановлению следователя в связи с возбужденным уголовным делом по факту сбыта в открытом акционерном обществе «Северсталь» поддельных векселей названной организации. При этом подлинный вексель ОАО «МВЦ «Северсталь» № 027 602, согласно показаниям свидетелей и документальным данным, с 16 февраля 1998 г. до момента выявления подделки банку «Таврический» не выдавался и находился в кассе ЗАО «Северсталь-Инвест». Лица, виновные в выдаче банку подделки взамен подлинника векселя, не были установлены[1].

Подлог при совершении мошеннических действий по указанной схеме в большинстве случаев заключается в неподлинности подписей. То есть ценная бумага, даже если она содержит все другие установленные вексельным правом реквизиты, оказывается подписанной не тем лицом, от имени которого выполняется подпись. Такие случаи квалифицируются как подлог подписи, делающий вексель недействительным.

Маскировочные действия преступников направлены на то, чтобы личность субъекта, выполнившего подпись, не была установлена.

Другие способы мошенничества, заключающиеся в умышленном лишении выданного векселя законной силы, будут рассмотрены ниже.

Завладение векселем под видом его покупки с использованием поддельных документов об оплате. Хищение под видом покупки, как правило, совершается в ситуациях, когда вексель находится на ответственном хранении вне пределов головной организации-векселедателя: в филиале организации либо в депозитарии. Такая форма хранения векселя может быть выбрана как по инициативе векселедателя, так и по предложению мошенников.

---

[1] Постановление Президиума Высшего Арбитражного Суда РФ от 1 июня 1999 г. № 8595/98.

Подготовительный этап указанного способа завладения векселем включает себя учреждение лжепредпринимательской организации (лжефирмы), как правило, по поддельному либо утраченному паспорту. Не исключается привлечение в качестве учредителей организации реальных лиц с подлинными документами и адресами. Обычно указанные лица не осведомлены о подлинной цели создания организации. С мошенниками их связывает получение разового или периодического вознаграждения (заработной платы). В качестве руководителя лжефирмы выступает участник преступной группы, использующий поддельный паспорт.

В число подготовительных действий входят открытие расчетного счета лжефирмы в одном из банков и сбор информации о владельцах высоколиквидных векселей. Одновременно распространяются тщательно продуманные «сведения» о готовности «фирмы» приобрести векселя на весьма выгодных для продавца условиях.

Не исключено вовлечение для участия в сделке «втемную» банков и иных организаций с хорошей деловой репутацией. В указанных случаях банк либо иная организация привлекается в качестве агента по покупке векселей, посредника, представителя интересов «покупателя». Включение в мошенническую схему солидной организации призвано «увести в тень» инициатора «покупки» и отвлечь продавца от выполнения необходимых проверочных действий в отношении непосредственного «покупателя».

Необходимым условием реализации преступного замысла является выведение похищаемых векселей из непосредственного владения векселедателя в распоряжение третьей организации — банка-депонента либо филиала банка-векселедателя.

Другим элементом описываемой схемы мошенничества может быть внедрение преступников в технологическую цепочку продажи векселя (в том числе подключение к линиям связи продавца) с целью использования поддельных документов об оплате покупки, передачи ложных подтверждений по факсу и телефону.

В процессе подготовки к «покупке» векселей мошенники заключают договор и таким образом завладевают образцами бланков, печати и подписей уполномоченных лиц. После перевода векселей в банк-депозитарий (или филиал) под благовидным предлогом откладывают на некоторый срок завершение сделки (иногда задержка оплаты может быть оговорена заранее под предлогом перевода денежных средств из других регионов). Одновременно изготавливаются поддельные документы об оплате векселей, которые мошенники предъявляют организации-депозитарию, и завладевают ценными бумагами.

По аналогичной схеме совершаются хищения векселей, переданных по той или иной причине на ответственное хранение в филиал или представительство выпустившего их банка.

Отношения между банком-векселедателем и мошенниками не обязательно завершаются моментом преступного завладения векселями. Поскольку для

реализации ценных бумаг необходимо определенное время, преступники могут продолжать контакты с потерпевшим некоторое время с целью маскировки совершенного преступления. Известен случай, когда мошенник в целях усыпления бдительности банка-векселедателя приезжал в офис этой кредитной организации и продолжал некоторое время звонить (по мобильному телефону), жалуясь на непредвиденную задержку с переводом денег. Тем временем похищенные векселя были перепроданы по заниженным ценам добросовестным приобретателям. Пропажа векселей была обнаружена лишь после того, как банк-депозитарий прислал уведомление о выполнении поручения о выдаче векселей и закрытии счета.

Эффективным средством предупреждения подобных случаев служит обычная проверка (по стандартной схеме) фирмы-приобретателя и лиц, выступающих от ее имени. Практика свидетельствует, что минимальные усилия в этом направлении позволяют выявить весьма подозрительные обстоятельства сделки и избежать возможных нежелательных последствий ее совершения.

Кроме того, следует обращать внимание на характерные признаки, присущие любому мошенничеству. В их число входит соответствующая психологическая обработка потерпевших и других причастных лиц, вовлеченных в мошенническую операцию без раскрытия подлинной сути происходящего (с использованием «втемную»). Указанная обработка включает в себя создание представления о хорошей деловой репутации и высоких экономических показателях деятельности лжефирмы, о необычной привлекательности предлагаемой сделки.

Кроме того, мошенники, как правило, вводят в схему сделки жесткие ограничения по времени принятия решений контрагентами, по требованиям обеспечения конфиденциальности сделки и т. п. Указанные условия создают своего рода психологический стресс и сужают возможность проведения полноценной проверки и принятия взвешенных решений.

С другой стороны, поведение неосведомленных посредников и участников сделки формируется при помощи различных положительных стимулов. Чаще всего в их роли выступает реальное или обещанное вознаграждение «за оперативность» и т. д. лицам, участвующим в подготовке и оформлении сделки.

Совершению подобного рода мошенничества способствуют просчеты в организации технологии и отсутствии должного контроля за этапами совершения сделки; утечка конфиденциальной информации о процедуре оформления и продажи векселей (не исключается наличие информатора из числа сотрудников организации-векселедателя); использование незащищенных каналов связи; халатность сотрудников организации-векселедателя, не выполняющих в полном объеме требований процедуры выдачи векселя.

В частности, сотрудник филиала одного из московских банков в аналогичном случае выдал вексель без получения, предусмотренного регламентом дублирующего распоряжения о выдаче векселя. Кроме того, на основании междугороднего телефонного разговора с женщиной, которая представилась сотрудницей

ексельного центра банка, он задержал отправление в головную контору кви-анции о выдаче векселя.

Завладение векселем в обмен на несуществующие товары. В указанных случаях шенники создают фирму-«однодневку» и подыскивают организации, способ-ые выдать ликвидные векселя. Затем заключают договор на поставку продук-ии, пользующейся повышенным спросом, на привлекательных для векселедате-я условиях. После получения ценной бумаги договор поставки (оказания услуг) жет быть частично выполнен или не выполнен вовсе. Векселя обналичивают, и вырученная от их продажи сумма присваивается мошенниками.

Директор ООО «Гуманитарно-промышленный фонд» обязался поставить ООО «Стимул» по договору купли-продажи 5 тыс. т сырой нефти. В качестве платы поставки «Стимул» обязался передать фонду восемь векселей финансового управления Саратовской области на общую сумму 21 млн руб. Эти векселя хранились в депозитарии КБ «Российский кредит». По условию договора предполагалось, что они будут переданы после выполнения поставки на основании нотариальной доверенности представителю фонда Т. Зная данные условия хранения и другие необходимые сведения по сделке, Г. подделал нотариальную доверенность на имя Т., получил векселя в депозитарии, реализовал их добросовестному приобретателю — коммерческой структуре, получил взамен облигации государственного сберегательного займа на сумму 17 млн руб. и скрылся[1].

Завладение векселем путем обманного получения ценной бумаги под предлогом его необходимости для процедуры подготовки к заключению будущей сделки. Эта схема мошенничества рассчитана на неосведомленность потерпевшего относительно особенностей вексельного права и мер безопасности в процессе выдачи векселя (или совершения аваля). В частности о том, что вексель, будучи выданным даже при обстоятельствах, которые характеризуются как «порок выдачи» (обман, принуждение, кража и т. п.), считается собственностью его владельца. Обстоятельства приобретения векселя (или совершения аваля) лежат за пределами вексельного права. Обязанность же доказывания незаконности завладения векселем в рамках гражданского права лежит на векселедателе, поскольку в данном случае применяется принцип гражданского права — движимая вещь является собственностью владельца, пока не доказано обратное.

Механизм преступлений подобного рода включает в себя обычный набор подготовительных действий: создание лжекоммерческой или общественной (благотворительной) организации, психологическую обработку потерпевших, демонстрацию признаков высокой деловой репутации лжефирмы и экономической привлекательности предлагаемой сделки. Нередки случаи предварительной обработки «втемную» деловых партнеров будущего потерпевшего. В таких случаях партнеры, зная о финансовых проблемах векселедателя, сообщают ему о возможности «поправить дела», и как им кажется, по собственной

[1] Уголовное дело № 011 699, расследованное РУВД ЦАО г. Москвы.

инициативе, указывают на мошенническую фирму, готовую выдать кредит либо оказать другие услуги.

Лжефирма, после обращения к ней будущего потерпевшего, оговаривает условия будущего «договора», проводит в процессе переговоров встречи в респектабельных «офисах» либо ресторанах.

Ключевым этапом схемы является завладение векселем потерпевшего до заключения предполагаемого договора. Делается это под различными предлогами. При этом вексель может быть оформлен как полностью, так и частично (однако мошенники настоятельно просят проставить на нем печать и подписи уполномоченных лиц). Недостающие реквизиты заполняются преступниками после получения документа в свое распоряжение.

Показательным примером подобного рода обмана является описанный в периодической печати случай с АОЗТ «Энергетическая компания», произошедший летом 1996 г. Названная компания, нуждаясь в открытии кредитной линии, подыскивала для этого соответствующий банк. По рекомендации одного из деловых партнеров генеральный директор АОЗТ обратился к зарубежному «инвестору» — английской компании Amadeus Ltd., зарегистрированной в Лондоне. Руководитель Amadeus Ltd. некто Климов потребовал в качестве обязательных условий будущей сделки предоставить ему «прототип» договора займа и бланка простого векселя на сумму кредита в 2 млн долл. с авалем одного из российских банков. При этом Климов настаивал, чтобы документы были подписаны уполномоченными лицами и скреплены печатью. Такие несуразные условия заключения сделки он объяснял мерами по обеспечению безопасности активов возглавляемой им компании.

Руководство АОЗТ «Энергетическая компания» согласилось с требованиями Климова. Вексель (почему-то получивший качество прототипа) с указанием суммы, подписями и печатью был авалирован банком «Линд». При этом из соображений безопасности на «прототипе векселя» не были проставлены время и место его составления. Такие меры предосторожности после консультаций с юристами были признаны руководством АОЗТ достаточными. Выполнению требований Климова не помешал и тот факт, что понятие «прототип векселя» в вексельном праве отсутствует. Показательно, что термин «прототип векселя» в текст описанного документа внесен не был. «Прототип векселя» был отправлен в Лондон.

После этого компания Amadeus Ltd., заполнив недостающие реквизиты, продала вексель за 1,8 млн долл. одному из российских банков и была ликвидирована. Каких-либо денежных средств в рамках договора кредитования «Энергетическая компания» не получила.

Показательно, что готовясь к совершению вексельной сделки на весьма значительную сумму с неизвестным ранее партнером, «Энергетическая компания» не приняла в отношении Amadeus Ltd. простейших мер проверочного характера.

Схема завладения векселем обманным путем под предлогом подготовки к заключению предполагаемой сделки весьма популярна среди отечественных

и иностранных мошенников. Попытки преступлений подобного рода периодически предпринимаются с конца девяностых годов по наши дни. К примеру, начиная с 1996 г. по настоящее время руководители многих регионов России получают предложения о выделении крупных кредитов в долларах США под минимальный процент. До 2000 г. предложения исходили от американской компании International Financial Communications Inc. (INFINCO), генеральный директор В. Швахман и генеральный директор по России и странам СНГ В. Кобзарь, и Международного благотворительного христианского фонда (МБХФ) (президент В. Кобзарь), имеющих на территории России разветвленную сеть представительств. Руководители более 50 субъектов Российской Федерации получили от указанных лиц сообщения о возможности открытия регионам кредитной линии на несколько десятков миллиардов долларов США сроком от 10 до 30 лет с возможной пролонгацией и с процентной ставкой не более 7% годовых. Предложения были высказаны в ходе личных встреч представителей INFINCO и МБХФ с ответственными чиновниками администрации регионов.

Для получения кредита предлагалось организовать компанию-кредитополучатель, которая выпускает векселя номиналом в 500 млн долл. США без процентной ставки и передает их по договору в трастовое управление МБХФ на срок до 10 лет. Обеспечением векселей должны стать залоговые документы на имущество и другие активы, которые должны быть депонированы в банке компании в пользу кредитодателя. Далее предлагалось направить зарубежным «партнерам» заявку на кредит с приложением векселей на сумму предполагаемого кредита. Фактически речь шла о выдаче векселя будущему «кредитору» до получения кредита. В предложение было включено обязательство не размещать получаемые векселя на вторичном рынке ценных бумаг и не передавать их третьим лицам.

Расчет мошенников строился на безусловности денежного обязательства по векселю, о которой уже говорилось выше. То есть на обязанности векселедателя платить по выданному векселю независимо от того, был предоставлен кредит или нет.

Несомненно, с требованием оплаты по таким векселям в дальнейшем обратились бы третьи лица, которые купили бы их на вторичном рынке ценных бумаг. Обязательство инициаторов аферы не выходить на указанный рынок и не передавать вексель третьим лицам, как известно, правовой силы не имеет. Однако в описанном выше случае руководители некоторых регионов проявили разумную настороженность. По их просьбе ФСБ России провела соответствующую проверку, о результатах которой проинформировала всех заинтересованных, а заодно и средства массовой информации. Было установлено, что МБХФ создан в начале 1990-х годов сторонниками секты «Истинные христиане веры евангельской» (пятидесятники), имеет представительство в Москве. Денежные средства на счетах фонда отсутствуют. Имели место факты предъявления представителями фонда к оплате поддельных векселей Сбербанка России (преступный умысел доказать не удалось). Президент фонда Кобзарь В. И. — гражданин России, осужденный в свое время на 11 лет лишения

свободы за грабеж, хищение государственного имущества в особо крупных размерах и другие преступления.

Завладение ранее проданным векселем под видом восстановления права на утраченную ценную бумагу. Указанный способ обмана применяется в отношении лиц (юридических и физических), не желающих по тем или иным причинам, чтобы покупка ими векселя попала в поле зрения контролирующих, налоговых или правоохранительных органов. Они могут преследовать цель уклонения от налогов, легализации (отмывания) доходов, полученных преступным путем, и т. д. Таким лицам мошенники предлагают приобрести так называемый забалансовый вексель (то есть вексель, выданный без соблюдения правил оформления его выдачи). Напомним, что легальная выдача векселя сопровождается заключением договора о заключении гражданско-правовой сделки с использованием векселей, записью в регистре бухгалтерского учета, записью в специальном реестре с указанием серии и номера векселя, даты его составления, срока платежа, суммы векселя, вида и величины дохода по векселю, наименования получателя платежа (первого векселедержателя).

Кроме того, при выдаче векселя составляется акт приема-передачи этой ценной бумаги, в котором указываются наименование документа; дата составления; содержание хозяйственной операции; реквизиты векселя, ссылка на договор, наименование должностей лиц, ответственных за совершение хозяйственной операции и правильность ее оформления, личные подписи и их расшифровки. Акт с приложением к нему копии векселя является основанием для отражения в бухгалтерском учете.

Аналогичный порядок установлен для документального оформления переводных векселей, принятых к акцепту.

Покупка же «забалансового» векселя осуществляется, что называется из рук в руки. Для придания видимости надежности сделки вексель предварительно проверяется у векселедателя. Оплата покупки производится денежными средствами в наличной форме. Какие-либо документы, подтверждающие факт приобретения ценной бумаги, у покупателя отсутствуют.

После передачи векселя покупателю мошенники немедленно обращаются в суд с исковым заявлением о признании векселя утраченным и о восстановлении прав по этой ценной бумаге. При этом нередко выясняется, что лицо, продавшее вексель, никакого отношения к «векселедателю» не имеет.

6.4. Преступления против собственности, в которых вексель является средством совершения преступления

Мошенничество при выдаче векселей

Способ обмана при выдаче векселя заключается в том, что взамен ценной бумаги приобретателю выдается документ, плата по которому изначально не предусматривается. В преступных целях используется интеллектуальный

одлог либо иной умышленный дефект формы векселя, т. е. заранее задуман-ые нарушения правил выдачи векселя, лишающие ценную бумагу вексель-ой силы.

Под интеллектуальным подлогом принято понимать составление докумен-а, содержащего заведомо ложные сведения, имеющие юридическое значени-ля подтверждения взаимных обязательств между сторонами в области граж-анского права. При этом по форме документ правилен, однако изложенны-нем сведения не соответствуют действительности. Интеллектуальный под-ог устанавливается на основе логического анализа содержания документ-его реквизитов путем установления их несоответствия известным факта-ожным, применительно к описываемой ситуации, является запись в вексе-обязуюсь уплатить».

Выдача необеспеченных векселей. Наиболее распространенным видом м-енничества указанного вида в вексельной сфере является выдача просто-екселя без намерения его оплатить. «Векселедатель» в большинстве случа-росто не располагает средствами для оплаты по векселю и изначаль-е имеет намерения его оплатить. Для создания видимости надежности свое-рганизации и высокой ликвидности ценных бумаг мошенники нередко и-ользуют названия зарегистрированных ими лжекоммерческих организаци-озвучные с известными фирмами.

В октябре 2005 г. на рынке ценных бумаг появились векселя ЗАО ИФ-Норильский никель», созвучного с названием известной группы ГМК «Но-ильский никель», но не имеющего к последней никакого отношения. В мо-еннических целях использовались также необеспеченные векселя фир-ы-«однодневки» «Алмазы Якутии», которую потерпевшие связывали по ас-оциации с компанией «Алмазы Саха»[1].

Выдачей необеспеченных векселей без намерения их оплатить нередко решат» организации, не способные удовлетворить требования кредиторов о денежным обязательствам из-за банкротства. Так, в 2006 г. в Москве отме-лись неоднократные попытки сбыта векселей ряда кредитных организаций, оторые вскоре лишились лицензий на осуществление банковских операций. есьма поучительной для банковского сообщества оказалась крупнейшая век-льная афера, совершенная под вывеской упоминавшегося выше агропро-ышленного холдинга «Русагрокапитал».

Эта организация выпустила на фондовый рынок необеспеченные векселя общую сумму, эквивалентную 50 млн долл.

В 2004 г. руководство «Русагрокапитала» отказалось гасить собственные кселя, мотивируя отказ «сложным финансовым положением» в холдинге. ержатели векселей получили неофициальные предложения «Русагрокапита-» реструктуризировать выплаты по ценным бумагам на сроки от трех до пя- лет.

[1] Прикинулись «Норникелем» // РБК daily. 2006. № 27.

К моменту получения писем ряд векселей был опротестован, а некоторые держатели ценных бумаг имели на руках исполнительные листы. Однако деньги по ним получить не удалось. С целью уклонения от уголовного преследования К. и ряд руководителей, входивших в холдинг региональных организаций, попытались «перевести» рассмотрение аферы в сферу гражданско-правовых отношений. Так, самарское ЗАО «Мукомольный завод № 1» и ЗАО «Самарский мукомольный завод № 2» выпустили необеспеченные вексельные обязательства на общую сумму свыше 2,6 млрд руб. ОАО «Новочеркасский комбинат хлебопродуктов» и ОАО «РомузЪ» выдали вексельные обязательства на общую сумму свыше 2,4 млрд руб. После предъявления векселей к оплате руководители организаций-векселедателей объявили о несостоятельности заводов и комбината, обратились с соответствующими заявлениями в арбитражные суды.

Уголовные дела по ч. 3 ст. 159 (мошенничество) УК РФ по обвинению главы сельскохозяйственного холдинга К. и подчиненных ему региональных руководителей были возбуждены лишь после обращения Ассоциации российских банков в Государственную думу и проведения парламентских слушаний[1].

Приобретение необеспеченных векселей не всегда является результатом заблуждения обманутого покупателя. Известно немало фактов, когда организации, в том числе кредитные, умышленно приобретают такие векселя в обмен на реальные ценности. Речь идет о специально создаваемых ситуациях умышленного банкротства, когда руководство организации попросту разворовывает средства акционеров и вкладчиков.

Вывод активов кредитной организации производится по незамысловатой схеме: недобросовестные руководители банков реализуют высоколиквидные ценные бумаги, а на вырученные денежные средства приобретают неликвидные ценные бумаги, в частности векселя фирм-«однодневок». Затем эти фирмы исчезают вместе с бывшими активами банков[2].

Дополнительные способы маскировки необеспеченности векселя. В отдельных случаях мошенники, убеждая приобретателя векселя в надежности выданной ими ценной бумаги, ссылаются на внесенную в вексель запись, согласно которой векселедатель поручает обслуживающему его банку производить платежи по выданным им векселям за счет средств на его расчетном счете. Из содержания указанной записи следует, что платеж должен быть произведен

[1] Материалы Комитета по безопасности Ассоциации российских банков; материалы уголовного дела № 196 872, расследованного УВД ЦАО г. Москвы; материалы проверки ОБЭП Ржевского ОВД по сообщениям о преступлении КУП № 2700 от 21 июля 2004 г., КУП № 2780 от 3 июля 2004 г., КУП № 2781 от 3 августа 2004 г.

[2] За 2006–2008 гг. процедурам отзыва лицензии с последующим банкротством подверглись более 100 банков. По данным Агентства по страхованию вкладов, причина утраты активов банков-банкротов в 80% случаев заключается в их преднамеренном выводе (хищении), замаскированном путем фальсификации финансовой отчетности. На обстоятельства, связанные с банковскими рисками, приходится лишь около 20% случаев.

банке по месту нахождения расчетного счета векселедателя. При этом банк случае необходимости подтверждает свою готовность выполнить поручение. Недостаточно искушенный в вексельном и финансовом праве приобретатель екселя полагает, что банк таким образом берет на себя и обязательства об оп-ате векселя.

Когда же векселедержатель при наступлении срока платежа обращается указанный банк с требованием об оплате векселя, то узнает, что ценная бу-ага оплате не подлежит в связи с отсутствием средств на расчетном счете екселедателя, а сам банк никаких обязательств по векселю не несет. Дело том, что банк, на который векселедатель возлагает обязанность платить о векселю, не является лицом, несущим в силу ст. 47 Положения о простом переводном векселе ответственность за оплату векселя перед векселедержа-елем. Такую ответственность несет сам векселедатель, назначивший уполно-оченное лицо для платежа.

Прямое указание векселедателем на банк (либо иную организацию), как а плательщика (а не посредника в оплате) по векселю, также не является га-антией будущей оплаты ценной бумаги. Такое указание подлежит выполне-ию лишь в тех случаях, когда предполагаемый плательщик акцептует ценную умагу. В случае отказа в акцепте банк точно так же, как и в описанном выше лучае, не несет никакой ответственности перед векселедержателем. Все пре-ензии по оплате векселя следует адресовать к векселедателю.

Выдача векселя с заведомым дефектом формы. Дефект формы векселя, со-ласно ст. 76 Положения о простом и переводном векселе, означает отсутствие акого-либо из обязательных реквизитов (обозначений) векселя, что лишает енную бумагу силы простого векселя. Перечень обязательных реквизитов екселя содержится в ст. 75 Положения о простом и переводном векселе, их числе:

1) наименование «вексель», включенное в самый текст и выраженное том языке, на котором этот документ составлен;
2) простое и ничем не обусловленное обещание уплатить определенную мму;
3) указание срока платежа;
4) указание места, в котором должен быть совершен платеж;
5) наименование того, кому или по приказу кого платеж должен быть со-ршен;
6) указание даты и места составления векселя;
7) подпись того, кто выдает документ (векселедателя).

При этом наличие реквизитов оценивается не только по формальному исутствию, но и по содержательному признаку (например, по признаку длинности подписи).

Применяя в целях обмана умышленный дефект формы векселя, мошенни-и пользуются недостатками правовой подготовки и делового опыта у добро-вестных участников вексельного обращения. Эти обстоятельства позволяют

мошенникам применять изощренные формы обмана потерпевших под видом «ошибок» при оформлении векселя, влекущих его недействительность, либо существенно уменьшающих размеры обязательств векселедателя. Отличить в данном случае обман от случайной ошибки совсем нетрудно, однако приобретатели векселей не всегда распознают упомянутые выше умышленные нарушения процедуры оформления ценных бумаг. Это позволяет преступникам отказываться от исполнения обязательств и маскировать мошеннические действия путем придания им видимости гражданско-правового деликта.

Самым достоверным признаком обмана в указанных случаях служит отказ от исполнения предусмотренных векселем обязательств. При добросовестном же заблуждении обязанного по векселю лица каких-либо правовых препятствий для исполнения обязательств не имеется.

Подписание векселя неуполномоченным лицом. Наиболее распространенными видами дефекта формы векселя (и способами уклонения от исполнения обязательств по векселю), как показывает практика, является подписание векселя неуполномоченным лицом.

Согласно требованиям вексельного законодательства, векселедатель должен подписать вексель собственноручно либо выдать доверенность на подписание названной ценной бумаги другому лицу. В последнем случае подпись сопровождается припиской «по доверенности».

Подписание векселя от имени организации-векселедателя требует полномочий, специально оговоренных в уставе или положении. Аналогичные требования установлены и к подписи организации авалиста (вексельного поручителя). Подпись лица, не имеющего соответствующих полномочий либо вышедшего за их пределы (например, за пределы определенной уставом банка суммы, которую ему разрешено авалировать без согласования), не влечет каких-либо обязательств со стороны организации, от имени которой подписана ценная бумага. В таком случае, согласно ст. 8 Положения о векселях, «каждый, кто подписал переводный вексель в качестве представителя лица, от имени которого он не был уполномочен действовать, *сам обязан по векселю*». То есть данное лицо отвечает по вексельным обязательствам как частное лицо в пределах собственного имущественного положения. Вероятность же того, что частное лицо способно возместить многомиллионные суммы обязательств, данных от имени организации, практически отсутствует. Кроме того, граждане, подписавшие подобные ценные бумаги, нередко просто скрываются от векселеприобретателей и судебных органов.

Иногда в качестве неуполномоченного лица выступает руководитель организации, превысивший пределы отведенных ему полномочий.

ОАО «Ш» обратилось в суд с иском о признании недействительными двух векселей на сумму 2 млн руб., подписанных руководителем организации без одобрения общего собрания акционеров. Иск основывался на положениях ст. 78 и 79 Закона об акционерных обществах. Решение об одобрении крупной сделки, предметом которой является имущество, стоимость которого

составляет более 50% балансовой стоимости активов общества, принимается общим собранием акционеров большинством в три четверти голосов акционеров — владельцев голосующих акций, принимающих участие в общем собрании акционеров. В ходе рассмотрения иска судом было установлено, что на момент совершения сделки купли-продажи векселей сумма активов баланса общества составляла 989 тыс. руб., поэтому для одобрения этой сделки требовалось решение общего собрания акционеров[1].

Отказы от платы по векселям в связи с подписанием ценных бумаг неуполномоченным лицом — явление постоянное. Данные АУВЕР свидетельствуют, что лишь за период с марта 2000 г. по март 2003 г., по указанному основанию не были оплачены 152 векселя.

В частности, Российская самолетостроительная корпорация «МиГ» выдала 31 января 2001 г. ЗАО «Росавиаспецкомплект» 13 простых векселей номиналом 5 млн руб. каждый со сроком предъявления к платежу «по предъявлении», но не ранее 1 декабря 2001 г. Однако еще до предъявления этих ценных бумаг к оплате 23 июля 2002 г. органами прокуратуры в ходе расследования уголовного дела было установлено, что на указанных векселях стоят подписи лиц, не правомочных выдавать векселя от имени предприятия.

Другой векселедатель — «Аэрофлот — российские авиалинии» 3 июля 2001 г. проинформировал заинтересованных, что не несет обязательств по оплате выданных в 1999 г. от имени указанной организации 14 векселей, номиналом более 3 млн руб. каждый, поскольку эти ценные бумаги были подписаны сотрудницей К., не имевшей на это полномочий.

Отказ от уплаты по векселю может являться правомерной попыткой защиты организации-векселедателя от последствий мошеннических действий ее отдельных работников. Однако практике известны другие случаи, когда организация-векселедатель делала ставку на будущий отказ от выпущенных ею векселей как на самостоятельное направление своей финансовой политики.

В. А. Белов, например, описывает случай обнаружения следователем служебной записки начальника юридического отдела банка, адресованной его президенту. Этот «юрист» предлагал для обеспечения возможности «правомерного» отказа банка от оплаты выданных им векселей умышленно подписывать их лицами, не наделенными соответствующими полномочиями. На записке была собственноручная резолюция президента банка: «Согласен. Подобрать лиц для подписания»[2].

Подписание векселя с отступлением от способа воспроизведения подписи

Дефект подписи векселя может выразиться не только в подписании документа неуполномоченным лицом, но и в способе воспроизведения подписи.

[1] Постановление ФАС Уральского округа от 5 ноября 2002 г. по делу № Ф09–2697/02-ГК.

[2] *Белов В. А.* Вексельные преступления // Законодательство. 1997. № 5. С. 8.

Согласно правилам выдачи векселя (а также совершения аваля) подпись лица, уполномоченного от имени векселедателя, должна быть выполнена чернильной, шариковой или капиллярной ручкой, а также фломастером черного или темно-синего цвета. При этом использование карандаша или факсимильного штемпеля не допускается. Нарушение этих требований признается судебной практикой достаточным основанием для отказа от платы по векселю. В частности, в одном из случаев при рассмотрении спора о взыскании суммы по векселю с авалиста было установлено, что подпись лица, подписавшего вексель от имени юридического лица — векселедателя, была воспроизведена посредством штемпеля.

Авалист в обоснование своего отказа платить указывал на дефект формы векселя, который должен был содержать собственноручную подпись уполномоченного лица, поскольку иные способы оформления документа вексельным правом исключены.

Векселедержатель, ссылаясь на п. 2 ст. 160 ГК РФ, считал вексель надлежаще оформленным. Напомним, что названная норма указывает, что «использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон».

Тем не менее, Арбитражный суд в данном случае признал наличие дефекта формы векселя и освободил авалиста от ответственности на основании ст. 32 Положения о переводном и простом векселе. При этом суд указал, что в нормативном порядке иной, кроме собственноручного, способ оформления подписи на векселе не установлен[1].

Выдача векселя с обязательством выплаты вексельной суммы при наступлении определенных условий. Весьма распространенным видом дефекта формы векселя является включение в данный документ записей, связывающих выплату вексельной суммы какими бы то ни было условиями. Такие записи противоречат природе простого векселя, который в соответствии со ст. 75 Положения должен содержать простое и ничем не обусловленное обещание уплатить определенную сумму.

Судебными инстанциями, в частности, был установлен факт дефекта формы векселя, вызванный включением в него условия о наступлении срока платежа по истечении 20 дней с момента поступления денежных средств на расчетный счет векселедателя. Суд отметил, что «Включение в вексель указания, связывающего обязанность оплаты с наступлением события, относительно которого не известно, наступит ли оно, свидетельствует об условном характере

[1] Обзор практики разрешения споров, связанных с использованием векселя в хозяйственном обороте. Приложение к информационному письму Президиума Высшего Арбитражного Суда РФ от 25 июля 1997 г. № 18.

обязательства. Кроме того, Положение исключает возможность ук
ков по векселю способами иными, нежели установлено ст. 33
Следовательно такой документ не может быть признан имеющим
ля ввиду дефекта формы».

К числу условий, ограничивающих выплату по векселю и пот
щих документ вексельной силы, относятся не редкие на прак
включения в вексель условий о погашении задолженности в
форме.

В частности, ЗАО «Межрегиональный инвестиционно-финанс
тут» посредством индоссамента приобрело простой вексель № 42
санный ОАО «КамАЗ» 6 февраля 1997 г., со сроком платежа по пр
но не ранее 7 марта 1997 г., по которому подлежало оплате 500 м
ловием: продукцией ОАО «КамАЗ».

Данное условие было включено в текст бланка векселя и рас
ред подписью векселедателя. Предъявленный в установленный ср
спорный вексель не был оплачен векселедателем по мотиву отс
стороны обязательства уплатить денежную сумму, так как докум
специальную оговорку о поставке продукции ОАО «КамАЗ» на с
ную в векселе.

Президиум Высшего Арбитражного Суда РФ своим постано
знал отказ от уплаты по векселю денежной суммы обоснован
что пометка об оплате векселя продукцией ОАО «КамАЗ» удост
нежное обязательство, а обязательство по передаче данной прод
му, указанную в векселе. При таких условиях документ, предст
цом и названный им векселем, следует рассматривать как долг
ное обязательство, а правоотношения сторон в этом случае
нормами гражданского права[1].

В числе других недобросовестных уловок, делающих векс
тельным, встречаются: передача действительного векселя лицу
непрерывного ряда индоссаментов, по этой причине приобр
бумаги не может рассматриваться законным векселедержател
осуществлять права по векселю; заведомо неправильное вы
сей о посредничестве, об акцепте, об авале; недействительны
обязательства векселедателя, зафиксированные не в самом век
хотя бы и связанных с ним, документах.

Умышленная дефектность оформления векселя может выр
документа от имени филиала организации, который таким пр
Вексель может быть выдан от имени банка, лишенного лице
вершения банковских операций. Злоумышленники соверш
логичные «ошибки».

[1] Постановление Президиума Высшего Арбитражного Суда РФ от 6 ап

...Мошенничество с использованием фальшивых векселей

...: *характеристика изготовления и сбыта фальшивых векселей.* Изго-
...дельного векселя или его сбыт рассматриваются как преступле-
...экономической деятельности, предусмотренное ст. 186 (Изготов-
...быт поддельных денег или ценных бумаг) УК РФ. Принадлеж-
...к ценным бумагам установлена ст. 143 ГК РФ. К ценным бумагам
...и с названной статьей относятся: государственная облигация, об-
...сель, чек, депозитный и сберегательный сертификаты, банковская
...я книжка на предъявителя, коносамент, акция, приватизацион-
...бумаги и другие документы, которые законами о ценных бумагах
...ленном ими порядке отнесены к числу ценных бумаг[1].

...товлением поддельных денег или ценных бумаг понимается
...либо полная подделка, обеспечивающая их существенное сход-
...нными денежными знаками или ценными бумагами по форме,
...м параметрам[2].

...дельных денег или ценных бумаг заключается в их непосредст-
...льзовании для любых расчетных операций, а равно в их передаче
...возмездно или безвозмездно.

... предусмотренные п. 1 ст. 186 УК РФ, наказываются лишением
...срок от пяти до восьми лет со штрафом в размере до одного мил-
..., или в размере заработной платы или иного дохода осужденного
... пяти лет, либо без такового.

...ирующие (отягчающие) признаки данного преступления преду-
...2 ст. 186 УК РФ (те же деяния, совершенные в крупном размере)
... УК РФ (деяния, предусмотренные частями первой или второй
...атьи, совершенные организованной группой).

...е по п. 2 ст. 186 УК РФ может быть назначено в виде лишения
... срок от семи до двенадцати лет со штрафом в размере до одного
...блей или в размере заработной платы или иного дохода осужден-
...од до пяти лет, либо без такового. Деяния, предусмотренные п. 3
...Ф, наказываются лишением свободы на срок от восьми до пятна-
... штрафом в размере до одного миллиона рублей или в размере за-
...аты или иного дохода осужденного за период до пяти лет, либо

...*сти изготовления поддельного векселя.* Изготовление поддельных
...алее — подделка векселей) относится к числу преступлений,

...телей поддельных денежных знаков, а также ценных бумаг в судебной и следст-
...е нередко объединяют общим понятием — фальшивомонетчики.
... изготовления и сбыта денежных купюр и ценных бумаг, явно несоответствующих
...едует квалифицировать как мошенничество (п. 3 Постановления Пленума Верхов-
... от 28 апреля 1994 г. «О судебной практике по делам об изготовлении или сбыте
...ег или ценных бумаг»).

которым свойственны высокая степень организации участников, наличие них специфических знаний и навыков в области химии, полиграфии, имитации почерка, а также технического оснащения.

Указанные преступления, как правило, совершаются устойчивыми и сплоченными группами соучастников, каждый из которых выполняет заранее определенную ему роль. Практика показывает, что такие группы действуют в течение продолжительного времени. Размеры наживы, получаемой ими в результате каждого конкретного эпизода преступной деятельности, могут быть весьма высоки. Судебной практике известны преступления, в которых фигурировали фальшивые векселя Сберегательного Банка РФ номиналом в 1 млн руб., векселя Инкомбанка номиналом в 1 млрд (неденоминированных) руб. векселя, изготовленные на фальшивых бланках единого образца, номиналом 4 млрд (неденоминированных) руб. и др.[1]

Крупные размеры наживы, получаемой в результате сбыта поддельных векселей, позволяют фальшивомонетчикам использовать для достижения новых преступных целей весомые материальные ресурсы, организовывать многоходовые подготовительные операции, вовлекать в преступную деятельность соучастников из числа персонала коммерческих и государственных организаций.

Изготовление поддельных векселей (а также их сбыт) — преступление широко распространенное как по количеству преступных проявлений, так и по их географии. Факты сбыта подделок продолжаются и поныне в Москве и Московской области, во многих городах европейской части России, Кавказа и Сибири. По оценке специалистов, распространенность указанных преступлений сравнима с печально памятной эпидемией поддельных авизо. Однако в отличие от последних, поток вексельных подделок на убыль не идет.

По данным Комитета по безопасности Ассоциации российских банков в течение 2002–2006 гг. имело место более полусотни преступных посягательств на интересы банков, в которых фигурировали поддельные векселя номиналом от 30 млн до 50 млн руб. К сожалению, не все случаи мошенничества удалось вовремя выявить и предотвратить.

В феврале 2003 г. в Новосибирске вынесен приговор группе местных фальшивомонетчиков, подделывавших и сбывавших векселя Сбербанка России конце 1990-х годов. В ходе расследования установлены факты сбыта указанных векселей в Южно-Сахалинске, Красноярске, Алтайском крае, Новосибирской области, Челябинске, Москве и Самаре. Общая сумма установленного судом ущерба составила 20 млн руб.[2]

В 2006 г. Следственная часть Главного управления МВД РФ по Уральскому федеральному округу закончила расследование уголовного дела по факту

[1] *Масич А.* Экспертиза ценных бумаг — барьер на пути подделок // Депозитариум. 2000. № 1(20).

[2] «Вексельное дело» закрыто // Российская газета. 2003. № 26 (3140). 11 февр.

хищения денежных средств у Свердловской железной дороги с использованием поддельных векселей на сумму более 44 млн руб.

Согласно учетам АУВЕР на вексельном рынке устойчиво обращаются поддельные векселя ряда организаций, в том числе банков. Наиболее привлекательными для подделки по причине высокой ликвидности являются векселя Сбербанка России[1].

Приготовление к подделке векселей. Названный этап преступной деятельности включает в себя создание организованной преступной группы, приобретение необходимых технических средств, сбор информации о субъектах, от имени которых будут изготовлены векселя, и лицах, которым планируется сбыть подделки. Разрабатываются и реализуются планы завладения образцами бланков, документов, подписей должностных лиц и печатей организаций, выпускающих ценные бумаги. Устанавливаются неслужебные, а порой и преступные отношения с персоналом организаций-векселедателей и покупателей векселей. Иногда преступные организации внедряют в банк своих представителей, которые впоследствии снабжают их образцами документов и информацией об особенностях банковских технологий. Ведется психологическая подготовка сотрудников организаций, которым предполагается сбыть фальшивки. С этой целью преступники обналичивают в этих организациях подлинные векселя небольших номиналов.

На этом этапе планируются способы противодействия расследованию преступлений. Учреждается фиктивная (лжекоммерческая) организация, от имени которой предполагается осуществить сбыт подделок, приобретаются подельные паспорта для ее «руководителей» и «представителей».

Нередки случаи создания групп «силового» прикрытия и иных способов защиты на случай разоблачения лиц, сбывающих подделки. Так, например, при попытке сбыть поддельный вексель в одном из уральских городов участник упомянутой выше группы новосибирских фальшивомонетчиков был разоблачен и задержан службой безопасности компании. Однако «страховавшие» его соучастники уплатили компании крупную денежную сумму и он был отпущен без каких бы то ни было последствий.

Виды подделок векселя. Статья 147 ГК РФ проводит разграничение между двумя подвидами указанных противоправных действий: *подлогом и подделкой* ценных бумаг. Согласно абз. 2 п. 2 ст. 147 ГК РФ владелец ценной бумаги, обнаруживший *подлог или подделку* ценной бумаги, вправе предъявить лицу, передавшему ему бумагу, требование о надлежащем исполнении обязательства, удостоверенного ценной бумагой.

В гражданском праве и криминалистике к числу поддельных ценных бумаг относят документы, сфабрикованные полностью от имени векселедателя. Под

[1] В начале 2008 г. Сбербанк России обнаружил в обращении очередную серию подделок Сбербанка России ВМ (всего 25 бумаг с реквизитами векселя номиналом 10 000 000 каждая), якобы выданных Ханты-Мансийским отделением 1791 Западно-Сибирского банка Сбербанка России.

подложной ценной бумагой понимают выпущенный в оборот подлинный документ, в который незаконно внесены изменения.

Указанная классификация не имеет практического смысла для уголовно-правовой квалификации деяний, предусмотренных ст. 186 УК РФ, поскольку названная статья объединяет понятием «подделка» оба способа совершения преступления.

В то же время разграничение подделки и подлога представляет практический интерес для выявления и предупреждения указанных разновидностей преступления способами и средствами криминалистики, оперативно-розыскной и частной детективной деятельности.

Рассмотрим названные выше способы подделки ценных бумаг подробнее.

Изготовление подделки векселя (в криминалистическом понимании этого термина) предполагает применение копировальной техники либо типографского оборудования. Некоторые экземпляры фальшивок настолько приближены по качеству к подлиннику, что эксперты относят к числу «суперподделок». Они, по описанию эксперта Банка России А. Масича, изготовлены на бумаге с водяными знаками и снабжены защитными волокнами, имеется микротекст, выполненный с хорошим качеством. На оборотной стороне присутствуют люминесцирующие изображения оранжевого орнамента и бесцветного круга. Для нанесения всех изображений на фальшивых бланках использовались те же способы полиграфической печати (офсетный и высокий), что и при изготовлении подлинных[1]. Кроме того, преступники подделывают подписи векселедателя и оттиски его печати.

Подлог векселя связан с внесением в содержание подлинной ценной бумаги несоответствующих действительности записей, меняющих номинал векселя (в сторону увеличения), его серию и номер (во избежание проверки по стоп-листу) и другие реквизиты. В частности, могут быть изменены номера служебных телефонов организации, указанные в первоначальном тексте. В этом случае они заменяются на номера телефонов, по которым на вопросы о подлинности векселей отвечают члены преступной группы.

К примеру, группа фальшивомонетчиков, разоблаченная в Москве в 2006 г., покупала векселя Сбербанка России и других банков, имеющие небольшую номинальную стоимость. Члены группы, владеющие соответствующими познаниями и навыками, смывали специальным химическим составом реквизиты векселя (отдельные цифры номера и номинальную стоимость), восстанавливали путем дорисовки поврежденную защитную сетку и наносили новые записи, многократно завышая стоимость векселя. Качество дорисовки защитной сетки было настолько высоким, что сделать однозначный вывод о подделке векселя не представлялось возможным даже с использованием мощного микроскопа.

[1] *Масич А.* Экспертиза ценных бумаг — барьер на пути подделок // Депозитариум. 2000. № 1.

Подлог может заключаться во внесении в вексель не соответствующих действительности записей об индоссаменте, акцепте и авале.

Для подлога могут использоваться подлинные бланки векселей, в которые вносятся заведомо ложные сведения об их выдаче и векселедержателях, проставляются оттиски поддельных печатей. Для совершения преступлений используются погашенные векселя, которые похищаются в организациях сообщниками фальшивомонетчиков. Порой преступники изготавливают подделки, используя лишь реквизиты погашенных векселей.

В 2006 г. на вексельном рынке появился поддельный вексель ОАО «Росельхозбанк» серии 056 Д № 07947 номиналом в 1 110 000 руб. с выпуском 20 сентября 2004 г. и погашением 19 августа 2006 г., реквизиты которого представляли своеобразный гибрид серий, номеров и номиналов двух выданных ранее и уже погашенных векселей этого банка. Первый из них — серии 056 Д № 07947 имел номинал 1 022 400 руб., второй — серии 056 Д № 07946 — 1 110 000 руб.

Нередко подделки отличаются весьма высоким качеством изготовления, и выявить их без экспертного исследования практически невозможно. Доказательством этому может служить случай, когда фальшивые векселя Инкомбанка предъявлялись ему к оплате и признавались им подлинными. А лица, от имени которых эти векселя были подписаны, не смогли отличить поддельные подписи от собственных[1].

Обстоятельства, при которых выявляются подделки векселей:

- *при попытке сбыта* (предъявления к оплате) — в марте—апреле 2003 г. были выявлены в Москве два поддельных векселя ЗАО «Газпромбанк» номиналом в 500 тыс. руб. каждый и два поддельных векселя Сбербанка России номиналом по 50 тыс. руб. В г. Самаре был предъявлен к оплате поддельный вексель Сбербанка России на сумму 148 142 руб.;
- *в результате оперативно-розыскной деятельности*, осуществляемой правоохранительными органами в целях предупреждения преступлений в финансовой сфере;
- *в результате внутренних проверок в организациях*, осуществляющих выдачу и приобретение ценных бумаг, а также депозитарную и посредническую деятельность с ними (поддельные векселя были обнаружены, в частности, в ходе внутреннего расследования деятельности ООО КБ «ДИАМ-Банк», проводившегося правопреемником названного банка КБ «Новая экономическая позиция»);
- *в результате проверок правоохранительных, надзорных и контролирующих органов.*

Сбыт поддельных векселей является органической частью общего преступного замысла фальшивомонетчиков. Как правило, механизм сбыта разрабатывается преступниками одновременно с планами изготовления подделок. Он

[1] *Масич А.* Экспертиза ценных бумаг — барьер на пути подделок // Депозитариум. 2000. № 1.

ключает в себя подбор участников преступления, распределение преступных олей, поиск возможных покупателей фальшивки, их психологическую обра-отку с целью создания впечатления о выгодности и надежности сделки, спо-обы предъявления к оплате, получения и обналичивания денежных средств, пособы маскировки участников преступных акций и уклонения от ответст-енности за ее совершение. В число участников сбыта могут вовлекаться лица з персонала банков и других организаций.

На этапе приготовления к сбыту подделок учреждается лжекоммерческая рганизация. Чаще всего она создается по поддельным документам либо а подставных лиц, не имеющих представления о ее подлинном предназначе-ии. Участники сбыта обзаводятся поддельными паспортами (которые перио-ически меняют).

Классической иллюстрацией к механизму сбыта фальшивок может слу-ить случай реализации поддельных векселей Сбербанка России в Хабаровск реступной группой, упоминавшейся выше.

В конце января 1998 г. к директору хабаровского филиала ВостокБизнес-анка С. с предложением приобрести десять векселей Сбербанка России об-тился некто Б., выступавший под видом ответственного сотрудника совме-ного предприятия. Он действовал под чужой фамилией по поддельному спорту. Б. объяснил, что предприятие получило векселя в Москве в оплату выполненные услуги.

Психологическая обработка директора включала в себя обещание «щедро благодарить» его в случае покупки векселей самим банком или уплатить орошие комиссионные» за посредничество в продаже этих ценных бумаг угому покупателю.

Для проверки подлинности векселей Б. представил в филиал ВостокБизнес-Банка ксерокопию одного из документов, на обороте которой имелись но-ера предлагаемых к реализации всех десяти ценных бумаг. По результатам роверки реквизитов фальшивок, в 439 Центральном отделении Хабаровского анка СБ России был получен ответ о том, что 9 векселей являются доброка-ественными ценными бумагами, а один — блокирован к оплате. Подлин-ость каждого из 9 «доброкачественных векселей», предъявленных затем экспертизу, была проверена оператором 439 отделения Сбербанка Хабаров-а Щ. По результатам проверки, каждая из «ценных бумаг» получила офици-ьную справку о доброкачественности. После этого фальшивки общей номи-альной стоимостью 7,16 млрд (неденоминированных) руб. были переданы анку по агентскому договору для хранения и реализации. Дальнейшее уча-ие банка в их сбыте создавало дополнительный эффект надежности «цен-ых бумаг».

Впоследствии «ВостокБизнесБанк» продал указанные выше подделки ха-ровскому представительству коммерческого банка «Дземги» за 6,7 млрд руб. ырученные от продажи подделок деньги по указанию Б. были перечислены

«Кроун» в республике Науру (Центральная Океания) и фирмы «Трент-Бизнес» в латвийском АКБ «Айзкрауклес».

Факт подделки векселей был обнаружен после передачи их на хранение в Хабаровский банк Сбербанка России от КБ «Дземги». На момент выявления подозрительных признаков они уже находились в банковском архиве. Подделки были исполнены на высоком профессиональном уровне, однако не обладали некоторыми тайными метками, присущими подлинным векселям.

Следует отметить, что причастность банков к продаже поддельных векселей — не редкость. При обнаружении подделки продавший ее банк, как правило, утверждает, что его действия объясняются добросовестным заблуждением. Естественно, что в случае возникновения арбитражного спора обязанность доказывания умышленной продажи фальшивки лежит на ее приобретателе.

В августе 2002 г., например, АКБ «Диалог-Оптим» обвинил «Доверительный инвестиционный банк» (ДИБ) в том, что последний, будучи осведомленным о недоброкачественности ценной бумаги, продал ему фальшивый вексель банка «Менатеп СПб». АКБ «Диалог-Оптим» потребовал от ДИБ возмещения ущерба, однако тот выполнить это требование отказался, заявив, что не видит своей вины и считает, что действовал добросовестно и в соответствии с условиями договора и обычаями делового оборота[1].

Попытки взыскать ущерб от покупки подделки через арбитражный суд связаны с определенными трудностями. Во-первых, истцу предстоит доказать заведомую осведомленность ответчика о недействительности векселя. Во-вторых, в случае, если будет установлено, что поддельный вексель умышленно приобретался и сбывался с использованием возможностей банка его сотрудником по собственной инициативе, то ответственность за причиненный вред должен нести не банк, а указанное лицо. Вполне понятно, что реальное возмещение ущерба в полном объеме за счет имущества частного лица, учитывая размеры вексельных сумм, становится в таких случаях проблематичным.

Об особенностях рассмотрения исков о возмещении ущерба, возникшего в результате приобретения поддельного векселя, свидетельствует следующее.

В апреле 1998 г. Товарищество с ограниченной ответственностью «Бизнес-Консульт» обратилось в Арбитражный суд Санкт-Петербурга и Ленинградской области с иском к Санкт-Петербургскому акционерному коммерческому банку «Таврический» (далее — банк «Таврический») о применении последствий ничтожной сделки купли-продажи поддельного векселя серии А № 027 602 по договору от 3 апреля 1998 г. № 48/ВТ, о взыскании с банка 336 242 руб., из которых 238 500 руб. — денежные средства ТОО «Бизнес-Консульт» и ТОО «Аксон», указанного в исковом заявлении в качестве соистца, 9920 руб. — договорная неустойка и 93 822 руб. — убытки, предъявленные ТОО «Аксон».

Решением от 19 июня 1998 г. в удовлетворении иска было отказано. Арбит-ажный суд исходил из того, что представленные истцом доказательства ie позволяют установить вину банка в изготовлении и сбыте поддельных век-елей. Президиум Высшего Арбитражного Суда РФ своим постановлением т 1 июня 1999 г. № 8595/98 направил дело на новое рассмотрение, указав, что ля правильного разрешения спора необходимо выяснить, знали ли работни-и банка о том, что вексель поддельный[1].

В число приемов маскировки, применяемых при сбыте поддельного векс-я, входит его предварительное введение в оборот между «дружественны-труктурами (банками, коммерческими организациями). Такой способ реал-ации позволяет придать векселю видимость надежной ценной бумаги, по-уюшейся спросом, а в случае выявления подделки дает дополнительную во-ожность противодействия в установлении истины следствием и суде-В указанном случае число субъектов, возможно причастных к подделке, з-ительно расширяется, возникают дополнительные трудности в установлен-омента введения фальшивки в обращение.

Довольно распространенным способом сбыта подделок является приоб-ение на них товарных ценностей с их последующей продажей по снижен-енам.

Как способ реализации поддельных векселей, следует рассматривать и-ользование подделок в виде залога при получении кредита и при иных ра-етах в случаях, предусмотренных гражданским правом. Пакеты поддельн-екселей могут быть проданы мошенниками, выступающими под видом би-евых брокеров.

Субъекты, участвующие в изготовлении и сбыте поддельных векселей. Обоб-ение практики правоохранительных и судебных органов позволяет соста-ить весьма обширный и разнообразный по социальным признакам перечень иц, участвующих в изготовлении и сбыте поддельных векселей.

В числе таких лиц были выявлены представители коммерческих организ-ий и весьма известных банковских структур, чиновники государственных уч-еждений, силовых ведомств и правоохранительных органов, специалисты области полиграфии, химии, компьютерного оборудования, а также члены езаконных вооруженных бандитских формирований.

Некоторые из разоблаченных преступных сообществ, занимавшихся под-елкой и сбытом фальшивых векселей, имели межрегиональный и даже меж-ународный характер. В них участвовали граждане Англии, Германии, США, Прибалтийских республик. Нередко члены таких преступных сообществ были езнакомы друг с другом, а их деятельность координировалась из одного цен-ра непосредственно организаторами преступных акций.

В ряде случаев преступники используют для прикрытия изготовления сбыта подделок возможности организаций, в которых они занимают

[1] Постановление Президиума Высшего Арбитражного Суда РФ от 1 июня 1999 г. № 8595/98.

определенное (порой высокое должностное положение), либо покровительство высоких государственных чиновников.

Наглядным примером такого рода является Территориально-отраслевой финансовый энергетический союз (далее — ТО ФЭС), созданный при содействии бывших руководителей Минтопэнерго России. Ответственные лица этой организации наладили выпуск необеспеченных векселей номиналом на сумму 28 трлн неденоминированных руб. (часть указанных векселей затем была объявлена поддельными, хотя была отпечатана в той же типографии, что и «подлинные»). Затем, пользуясь «рекомендациями» чиновников Минтопэнерго России, ТО ФЭС разместил векселя по указанному в них номиналу на подведомственных министерству предприятиях, получив взамен своих «ценных бумаг» реальное имущество[1]. Известны случаи, когда подделки изготавливались в типографиях силовых и иных структур, научных учреждений и сбывались при содействии государственных чиновников и депутатов Государственной думы.

Непременным «субъектом» вексельных преступлений являются юридические лица, организации, специально созданные для совершения и маскировки преступных деяний. Без использования реквизитов и банковских счетов таких организаций сбыт поддельных векселей, получение и обналичивание преступной наживы во многих случаях были бы невозможны.

6.5. Меры предупреждения преступлений в сфере вексельного обращения

Общие требования к построению системы безопасности в сфере вексельного обращения в банке (организации) векселедателе

Защита от преступных посягательств, объектом которых является вексель, а также от его использования в качестве средства совершения преступления должна строиться в виде системы мер правового, организационного, технологического, криминалистического и сыскного характера.

В основу системы следует положить внутренний нормативный акт организации, регламентирующий порядок выпуска, хранения, выдачи и принятия к оплате векселей. Такой акт, изданный в форме положения, регламента, инструкции или приказа, должен полностью соответствовать положениям вексельного права. Его требования должны быть направлены на защиту сотрудников от просчетов правового характера.

Как и в других сферах банковской деятельности, важнейшим показателем системы безопасности является надежность персонала участка вексельного обращения. Лица, работающие с векселями, тщательно отбираются и проверяются. Они принимают обязательство не разглашать сведения о технологии

[1] *Гамза В. А., Ткачук И. Б.* Безопасность комерческого анка: учеб.-практ. пособие. М.: Изд-ль Шумилова И. И., 2000. С. 36–37.

і других особенностях вексельных операций. Эти сотрудники должны посто-інно совершенствовать уровень своих профессиональных знаний.

В качестве документа, наиболее детально и всесторонне регламентирующе-о деятельность системы защиты сферы вексельного обращения, можно на-вать Положение о простых векселях Сбербанка России, утвержденное поста-влением правления Сбербанка России от 27 августа 1998 г. № 431-р. Однако наличие системы само по себе не гарантирует от просчетов в выявлении і пресечении преступных посягательств. Практика свидетельствует о том, что Сбербанк России ежегодно несет убытки от действий вексельных мошенни-ков. Причина этого, по оценке специалистов Сбербанка России, заключается в недостатках подготовки персонала (прежде всего сотрудников филиаль-ной сети) и отсутствия достаточного опыта действий в соответствующих си-туациях.

Меры организационного характера включают в себя:

- *создание единой информационной системы* (далее — ИС) данных о состав-ленных, выданных, погашенных, утраченных, похищенных, подделан-ных векселях. ИС представляет собой сочетание электронной базы дан-ных и массива документов на бумажных носителях. В число бумажных носителей включаются ксерокопии векселей (выданных, погашенных, похищенных, утраченных, поддельных), а также договоров купли-про-дажи векселей и иных документов, сопровождающих оборот векселя;
- *особый порядок хранения векселя и бланков векселей.* Бланки векселей хра-нятся в специально отведенном помещении. В случае подготовки к со-ставлению и выдаче векселя они выдаются уполномоченному сотрудни-ку на период операционного дня. Неиспользованные бланки и состав-ленный, но не выданный вексель по окончании операционного дня возвращаются в хранилище. В течение операционного дня бланки век-селя и составленные векселя хранятся в сейфе ответственного сотруд-ника. Оплаченный (погашенный) вексель хранится в бухгалтерии и пе-редается в архив с соблюдением специального порядка защиты от утра-ты и хищения;
- *разграничение полномочий сотрудников, участвующих в вексельном обра-щении.* Участие в процедуре составления, выдачи, хранения и принятия к оплате векселя нескольких работников организации существенно снижает риск неправомерных действий со стороны вероятного зло-умышленника. Механизм разграничения полномочий реализуется по-средством участия в выдаче векселя:
  а) лица, выдающего бланк ценной бумаги;
  б) лиц, визирующих договор о купле-продаже векселя;
  в) руководителя и главного бухгалтера, подписывающих вексель;
  г) лица, ответственного за хранение печати, оттиск которой выполня-ется на векселе, и некоторых других лиц;
- *защиту информации о неиспользованных бланках.* Согласно правилам за-щиты вексельного обращения сотрудникам банка категорически запре-щается копировать бланки векселей. Эта мера направлена на предупре-ждение подделок векселя;
- *индивидуализацию ответственности работников, участвующих в выдаче векселя*, в сочетании с комиссионным порядком проверки соблюдения установленного порядка работы с векселями и их бланками. Работник удостоверяет своей подписью факт участия в процедуре проверки доку-ментов при выдаче векселя (расписывается на ксерокопии доверенно-сти, предъявленной первым векселедержателем). При предъявлении векселя к оплате работник расписывается на оборотной стороне векселя с указанием своих должности и фамилии.

Комиссионный порядок устанавливается для процедуры выдачи чистых бланков векселей в начале операционного дня, проверки правильности их расхода и сдачи в кладовую в конце рабочего дня.

Меры технологического характера включают в себя:

- *описание процедуры составления и условий выдачи векселя.* Наиболее су-щественным элементом технологии является предписание, согласно ко-торому вексель выдается векселеприобретателю только после поступления на счет банка полного объема денежных средств, указанного в договоре. Технология выдачи векселя предписывает выполнение соответствующих мер идентификации лица, получающего вексель в качестве первого век-селедержателя. Эта мера призвана предупредить случаи получения оп-лаченного векселя неуполномоченным лицом;
- *порядок документирования прохождения векселем процедур подготовки* к составлению и выдаче, документирование фактов его выдачи или по-гашения. Процедура выдачи векселя и передачи его на хранение в кла-довую отражаются в операционном дневнике. Факт принятия векселя к оплате документируется путем выполнения подписи на оборотной стороне векселя и отражением в операционном дневнике. Операция по-гашения векселя также показывается в операционном дневнике. Де-тальное отражение этих процедур в соответствующих учетах банка име-ет целью предотвратить возможные злоупотребления со стороны работ-ников банка, а также необоснованное обвинение в них со стороны векселедержателя;
- *содержание проверочных процедур при подготовке к оплате векселя.* В чис-ле первых действий работника при предъявлении векселя к оплате сто-ит проверка реквизитов предъявленной бумаги по соответствующей ба-зе данных векселей, находящихся в обороте, а также погашенных и за-прещенных к оплате (утраченных, похищенных, подделанных). В число проверочных процедур входят действия работника, предусмотренные методическими указаниями по определению подлинности ценных бу-маг;

- *процедуру, направленную на предотвращение повторного использования* погашенного векселя. На лицевой стороне погашенного векселя выполняется надпись «Принят к оплате». В качестве дополнительной меры защиты от повторного использования векселя допустимо внесение в бланк броских физических дефектов, например вырезать часть буквы из слова «вексель» в заголовке;
- *порядок работы с предъявленными неплатежными векселями.* Имеет целью предупредить дальнейшее возможное обращение предъявленных неплатежных документов. Учитывается особенность норм вексельного права, запрещающих изымать неплатежный документ у предъявившего его лица. Если экспертизой установлен факт подделки векселя и его недействительности, уполномоченный работник на лицевой стороне поддельного документа выполняет запись «Вексель неплатежный», проставляет штамп с наименованием банка, ставит дату и подпись. Кроме того, с поддельного векселя снимается ксерокопия, которая заверяется печатью банка и подписью работника. Лицо, предъявившее неплатежный документ, должно сделать на ксерокопии надпись: «Бумага с реквизитами векселя (серия и номер) получена. Подпись, фамилия, имя, отчество, дата».

Обязанность выполнения дальнейших действий с копией подделки, в частности обращения с заявлением в правоохранительные органы, возлагается на службу безопасности.

Меры криминалистического характера включают в себя действия, направленные на упреждающую защиту ценной бумаги путем выполнения так называемых вексельных меток (скрытых либо зашифрованных признаков подлинности документа), а также экспертизу документов, предъявленных к оплате.

Экспертиза проводится сотрудниками банка либо сторонних организаций, том числе правоохранительных органов и органов юстиции (по договору). случаях, вызывающих подозрение в подделке документа, сотрудник банка согласия клиента направляет вексель на экспертизу. На этот предмет к клиенту выдается соответствующая квитанция. В соответствии с правилами делового оборота срок экспертизы не должен превышать двух рабочих дней.

Эффективной мерой защиты организации векселедателя является периодическое проведение внутренних ревизий с обязательным выполнением всех требований по специально разработанной методике. Своевременное обнаружение хищения (утраты) векселя во многих случаях позволяет его собственнику избежать материального ущерба от противоправных и ошибочных действий.

Меры предупреждения вредных последствий хищения векселей

В случае кражи либо исчезновения векселя при невыясненных обстоятельствах потерпевший, независимо от факта возбуждения уголовного дела,

должен принять неотложные меры к восстановлению своих прав по утраченной ценной бумаге в порядке гражданского судопроизводства: подать заявление в суд о признании векселя недействительным и о восстановлении прав по нему. Это даст собственнику похищенного (утраченного) векселя возможность предотвратить возможные операции с похищенным (утраченным) векселем и восстановить ущерб независимо от успехов расследования.

Восстановление прав по утраченному векселю на предъявителя или признание векселя недействительным производится в порядке вызывного производства, предусмотренного ст. 294–301 Гражданского процессуального кодекса РФ (ГПК РФ).

После принятия заявления судья выносит определение о запрещении выдавшему документ лицу производить по документу платежи или выдачи и направляет копию определения лицу, выдавшему документ, регистратору.

Этим же определением на заявителя возлагается обязанность опубликовать за свой счет в местном периодическом печатном издании сведения:

- о факте обращения в суд в связи с утратой документа и наименование суда;
- собственное наименование заявителя, его место жительства или место нахождения;
- реквизиты векселя;
- предложение лицу, у которого возможно находится утраченный документ, обратиться в течение трех месяцев со дня опубликования в суд с заявлением о своих правах на этот документ.

Второй этап начинается после обращения нового владельца векселя в суд либо по истечении установленного срока такого обращения.

В случае если вероятный новый держатель утраченного документа заявит о своих правах на вексель до истечения трех месяцев, суд разъясняет заявителю его право предъявить в общем порядке иск к держателю документа об истребовании этого документа, а держателю документа его право взыскать с заявителя убытки, причиненные принятыми запретительными мерами.

Если же заявление от нового держателя векселя в указанный срок не поступило, суд принимает решение о признании векселя недействительным и восстанавливает права по утраченной ценной бумаге на предъявителя или ордерной ценной бумаге. Это решение суда является основанием для выдачи заявителю нового документа взамен признанного недействительным.

Меры защиты от конкретных видов посягательств на вексель или использования векселя в преступных целях

Меры защиты векселя от хищения путем кражи. Организация системы защиты ценных бумаг (векселя) от хищения в форме кражи предполагает в первую очередь хранение и обработку векселей в технически укрепленном помещении, оборудованном специальными средствами защиты и сигнализации.

Речь идет о технико-криминалистических средствах, применение которых затрудняет или исключает возможность совершения преступного посягательства либо создает благоприятные условия для розыска и разоблачения преступника.

К числу первых относятся запирающие устройства, средства охранной сигнализации, предназначенные для обнаружения несанкционированного проникновения на объект и оповещения службы охраны о появлении и нарастании угроз такого проникновения.

Вторая группа средств включает в себя технологические видеокамеры, позволяющие фиксировать действия преступника на месте преступления; различного рода ловушки и устройства дистанционной беспроводной передачи тревожного сигнала.

В числе ловушек, выпускаемых отечественными изготовителями, наибольшее распространение получили магнитоконтактные, пиротехнические изделия «Кукла» и «Миникредит», предназначенные для предотвращения краж из сейфов и иных хранилищ, а также для облегчения розыска и задержания преступника.

Ловушки маскируются под стандартную пачку банкнот или ценных бумаг. При попытке их изъятия с места установки происходит выброс несмываемой краски и облака слезоточивого газа.

Устройство дистанционной тревожной сигнализации «Радиокнопка», замаскированное указанным выше способом, в случае кражи обеспечивает выдачу защищенного от помех кодированного сигнала тревоги независимо от действий персонала[1].

Наряду с техническими средствами защиты реализуются меры организационного характера, направленные на исключение доступа посторонних в помещение, где хранятся и обрабатываются векселя; на предупреждение фактов оставления ценных бумаг вне сейфа, хранилища (даже на короткое время); а исключение возможности использования посторонним лицом дубликата или подделки ключа, а также штатного ключа, оставленного в ненадлежащем месте (в ящике стола, в «укромном месте»). Устанавливается запрет на несанкционированный вынос векселя за пределы организации даже на короткое время.

Специальные меры предосторожности следует предпринимать для обеспечения санкционированного перемещения векселя за пределами организации.

Наиболее надежным способом доставки представляется использование возможностей подразделений инкассации или фельдсвязи.

Меры защиты векселя от хищения путем присвоения. Специфика этих мер защиты определяется особенностями субъекта преступления. При совершении

[1] Указанные изделия разрабатывает и внедряет Научно-исследовательский центр «Охрана» ЗО МВД России. Подробнее см.: *Крахмалев А. К.* Безопасность учреждений кредитно-финансовой системы. Технические средства охранной сигнализации // Банковское дело. 2003. № 5. 37–39.

преступления ценная бумага вверена виновному и находится в его правомерном владении вплоть до похищения. По этой причине применение мер физической и технической защиты векселя от возможного присвоения смысла не имеет.

Основные меры предупреждения преступления заключаются в тщательном отборе персонала, организации эффективной системы внутреннего учета векселей, систематической проверке соблюдения правил обращения и хранения векселей, эффективной деятельности служб внутреннего контроля и безопасности.

Внутренний учет операций с векселями должен своевременно, полно и всесторонне отражать все совершаемые организацией действия с векселями, влекущие за собой возникновение, изменение или прекращение вексельных обязательств (в том числе совершение акцептов и авалей). Учет ведется на бумажных носителях либо в электронной (компьютерной) форме (возможно одновременное использование обеих форм) методом сплошного документирования. Имеющиеся в обороте векселя учитываются в денежном и количественном выражении во взаимосвязи с документами бухгалтерского учета, имеющими прямое либо опосредствованное отношение к вексельным операциям (договоры о приобретении векселей, акты приема-передачи, документы об оплате векселей и т. д.). Порядок учета выданных и погашенных векселей и построение аналитического учета об их обороте в организациях регламентирован письмом Министерства финансов России от 31 октября 1994 г. № 142.

Организация внутреннего учета должна предоставлять возможность незамедлительной внеплановой проверки количества векселей, находящихся в сфере финансово-хозяйственной деятельности организации, обязательных реквизитов каждого из них, а также документов, сопровождающих возникновение, изменение и прекращение обязательств по векселю. Плановую проверку наличия векселей и выполнения денежных обязательств по ним следует проводить не реже 1 раза в месяц.

Надлежащая постановка документального учета и контроля над движением векселей является действенным средством предупреждения их возможного присвоения либо своевременного раскрытия хищения. Проведение проверок не следует ограничивать сличением соответствия документальных данных с фактическим наличием векселей. Учитывая применяющиеся преступниками способы маскировки противоправных действий, необходимо периодически дополнять процедуру формального контроля проверкой подлинности имеющихся в распоряжении организации векселей (в том числе с применением средств криминалистической техники). Это позволит выявить возможную подмену векселя, специально изготовленную подделку.

Показателен факт обнаружения девяти поддельных векселей Сбербанка России, приобретенных КБ «Дземги» на вексельном рынке на сумму 6,7 млрд руб. Векселя некоторое время после приобретения хранились в «Дземги». Их подделка была обнаружена лишь в момент передачи на хранение в Хабаровский

банк Сбербанка России. Подделки были исполнены на высоком профессиональном уровне, однако не обладали некоторыми тайными метками, присущими подлинным векселям[1].

Меры защиты векселя от хищения путем мошенничества. Основным условием предупреждения хищений векселей путем мошенничества является проверка добросовестности и надежности предполагаемых контрагентов. Свидетельством наличия указанных качеств служит положительная деловая репутация контрагента, зафиксированная в его кредитной истории, истории его финансовых взаимоотношений с кредитными организациями и другими участниками имевших место сделок. В то же время факты неплатежа или неакцепта по векселям со стороны предполагаемого контрагента, информация о его причастности к продаже поддельных векселей либо векселей с иными дефектами, делающими ценную бумагу недействительной, служат признаком повышенной степени риска будущего партнерства с таким участником сделки. Сведения о фактах указанного рода публикуются на интернет-сайте АУВЕР (доступны для всех интересующихся). О финансовых конфликтах подобного рода периодически сообщают средства массовой информации, дают информационные сообщения судебные органы.

Наиболее предпочтительным вариантом подтверждения надежности потенциального участника сделки являются соответствующая информация банков, рекомендации других контрагентов и компаньонов.

Проверка вероятного партнера по сделке относится к общим требованиям обеспечения безопасности для всех видов вексельных операций. Не является исключением и сделка по продаже векселя предполагаемому партнеру, которая на первый взгляд может показаться менее опасной, чем покупка векселя.

Не следует упускать из виду, что, заявляя о намерении приобрести вексель, предполагаемый «покупатель» на самом деле может планировать его похищение тем или иным способом. В случае реализации такого намерения у потерпевшего, который не выполнил необходимых проверочных мер, порой не остается и минимально необходимых сведений для расследования.

Такая ситуация сложилась при похищении векселей у банка «Европа». Некто Борисов, представившийся генеральным директором фирмы «Юнайт» Никулиным, договорился о том, что банк «Европа» продаст названной фирме векселей общей номинальной стоимостью 30 млрд (неденоминированных) руб. В соответствии с условиями сделки векселя были депонированы в другом банке. Затем, пользуясь поддельным паспортом на имя Никулина, поддельной доверенностью банка «Европа» на получение векселей и поддельными платежными документами, Борисов обманным путем получил векселя из депозитария, реализовал их по заниженным ценам и скрылся.

[1] *Тимофеева И.* Аферисты, воры, взяточники повышают квалификацию // Вечерний Новосибирск. 2001.

В ходе расследования было установлено, что какие-либо действия по проверке будущего «покупателя» векселей банк «Европа» в период подготовки сделки не предпринимал. Названная выше фирма «Юнайт» была учреждена на имя подставного лица. Какие-либо денежные средства на ее счету отсутствовали. По юридическому адресу фирма никогда не находилась и почтового адреса не имела. Паспорт на имя Никулина на самом деле принадлежал лицу без определенного места жительства, а деловые контакты с банком Никулин-Борисов поддерживал лишь по радиотелефону.

Следует отметить, что вероятность банка ошибиться в подлинных намерениях клиента была бы значительно ниже в случае получения от Борисова стандартного набора сведений о фирме, которую он представлял, и выполнении элементарных действий по их проверке.

Минимально необходимый объем информации о клиенте банк имеет возможность получить при помощи анкеты, которая должна входить в пакет документов, приложенных к заявлению об открытии счета. Такая анкета разрабатывается каждым банком самостоятельно, но в целом их содержание совпадает. Лицу, выразившему желание заключить договор открытия счета либо совершить иную сделку с банком, предлагается ответить на вопросы анкеты о полном названии организации, ее юридическом адресе, фактическом местонахождении конторы (офиса), номере телефона, месте и дате регистрации, регистрационном номере, основном виде деятельности, наличии расчетного и ссудного счетов в других банках и их номерах. Кроме того, сообщаются сведения о руководителях организации, прилагаются нотариально заверенные выписки из Устава (Положения об организации), подтверждающие право конкретных лиц заключать сделку, а также карточки с образцами их подписей и оттиска печати. Расширенный вариант анкеты должен содержать вопросы о партнерах компании и их адресах.

При подготовке сделки с зарубежным партнером следует также проверить наличие этой компании в реестре страны регистрации. В большинстве стран данные этих реестров открыты. Они включают в себя сведения об организациях, их собственниках и лицах из высшего управленческого звена. В реестрах также содержится перечень фирм, исключенных из реестра на основаниях, порочащих их репутацию.

Следует отметить, что приведенные выше сведения о возможном контрагенте может получить в процессе подготовки к заключению договора не только банк, но и любой другой субъект, участник вексельной (и любой другой) сделки. Какие-либо запреты и ограничения со стороны закона либо стандартов профессиональной этики на этот счет отсутствуют. Более того, глубокое знание законопослушности, надежности и деловой репутации партнера всемерно поощряется в отечественном и зарубежном деловом мире. Решение о совершении сделки банк (либо другой участник сделки) принимает после проверки достоверности ответов на вопросы анкеты.

В зависимости от степени «прозрачности» ситуации проверка может ограничиться сопоставлением полученных от клиента (контрагента) сведений с данными открытых источников информации либо продолжиться путем сбора информации в рамках Закона о частной детективной деятельности.

Меры предупреждения мошенничества в форме подмены подлинного векселя на поддельный в процессе предъявления к оплате. Речь идет о случаях подмены подлинной ценной бумаги в процессе заключения «сделки» либо иных действий, связанных с временным выходом векселя из владения потерпевшим. Чаще всего подмена имеет место во время процедуры предъявления векселя к оплате векселедателю.

В целях защиты от подмены плательщик по векселю должен получить от предъявителя векселя следующие документы:

- паспорт;
- реестр векселей в двух экземплярах;
- акт приема-передачи в двух экземплярах;
- доверенность векселедержателя, за исключением случаев, когда предъявителем векселя является физическое лицо — владелец векселя или лицо, которое действует от имени юридического лица без доверенности. Предъявитель векселя предоставляет устав, нотариально заверенную карточку с образцами подписей распорядителей финансов и оттиска печати организации (векселедержателя).

Плательщик по векселю должен истребовать от предъявителя вексель. Предъявитель бумаги совершает на оборотной стороне векселя надпись: «Вексель предъявлен к оплате. Подпись и дата». Если векселедержатель — физическое лицо, на оборотной стороне реестра на основании предъявленного им паспорта указываются его паспортные данные (серия, номер, кем и когда выдан паспорт, место регистрации).

Факт принятия векселя к оплате заверяется путем нанесения на оборот бланка подписи принявшего работника и даты.

В некредитных организациях в качестве меры противодействия подмене векселя возможно помещение его после проверки в опечатанный конверт, заверенный подписями участвующих в сделке (и присутствующих при ней) лиц.

В качестве приема, затрудняющего подмену векселя непосредственно в процессе обмена документами, плательщик может воспользоваться предоставленным ему правом проставления на ценной бумаге отметки об имевшем место факте предъявления векселя к оплате.

Еще одним эффективным и малозатратным способом противодействия предъявлению подделки к оплате векселедателю является так называемое крапление векселя — включение в ценную бумагу своеобразных признаков, скрытых от посторонних (вексельная метка). Суть приема разрабатывается самим векселедателем (возможно с помощью специалистов в области криминалистики или средств защиты) и известна ограниченному кругу лиц. Отсутствие

«крапления» на предъявляемом документе служит верным признаком его подделки.

Меры предупреждения завладения векселем под видом его покупки с использованием поддельных документов об оплате. В число средств предупреждения указанного вида мошенничества входят:

- тщательная проверка надежности и платежеспособности приобретателя векселя;
- выявление подозрительных обстоятельств предполагаемой сделки, в число которых входят необычная экономическая привлекательность, ограничения времени на принятие решений, необычные условия по обеспечению конфиденциальности;
- внедрение защитной системы приема-передачи ценных бумаг и порядка проверки подлинности распоряжений и сообщений;
- использование для оформления векселей специальных бланков договоров и печати, которые не применяются в других случаях;
- максимальное ограничение круга сотрудников организации, посвященных в технологию оформления купли-продажи векселей;
- установление запрета на участие в составлении документов работников, не имеющих отношения к этому виду деятельности;
- использование для пересылки важных финансовых документов защищенных каналов связи;
- организация защиты информации о технологии совершаемых сделок с векселями.

Меры предупреждения мошенничества в форме подмены подлинного векселя на поддельный в процессе выдачи ценной бумаги. В данном случае речь идет о случаях, когда подлинный вексель подменяется в процессе выдачи на бумагу, имеющую явные или замаскированные признаки подделки. Впоследствии это позволяет мошенникам отказаться от уплаты по векселю.

Суть подделки может заключаться в умышленном искажении реквизитов и формы бланка векселя. Поддельный документ может содержать недостоверные данные о векселедателе, подпись от имени векселедателя может быть выполнена другим лицом, заверена печатью другой организации и проч.

Для избежания обмана приобретатель должен выполнить ряд действий предупредительного характера. В частности, проверить вексель на возможное наличие дефектов его формы и содержания. Следует обратить внимание на подлинность подписей и оттиска печати. Анализ на подлинность проводится путем сличения подписей и оттиска печати на векселе с их эталонными образцами. При выдаче векселя физическим лицом необходимо удостовериться в личности субъекта, подписывающего вексель. В число проверочных действий входит установление соответствия наименования векселедателя в документе его официальному наименованию, зафиксированному в учредительных документах.

В случаях, когда вексель после его проверки выходил из рук приобретателя оть на короткое время, проверку следует повторить с целью обнаружения озможного изменения первоначального текста и реквизитов ценной бумаги.

Меры предупреждения завладения векселем в обмен на несуществующие товары, невыполненные работы и неоказанные услуги. Первоочередной мерой предуреждения обмана в указанных случаях является проверка надежности и добросовестности предполагаемого контрагента. В этих целях следует как минимум ыполнить следующие действия:

- проверить подлинность сведений и документов, удостоверяющих право организации на поставку товаров или оказание услуг, о которых идет речь;
- проверить подлинность документов, удостоверяющих личность руководителя или представителя организации, наличие у них соответствующих полномочий на заключение сделки;
- получить сведения, подтверждающие реальное существование организации — приобретателя векселя;
- установить, соответствует ли предполагаемая сделка законодательству и уставным документам приобретателя;
- получить сведения, подтверждающие наличие у организации-приобретателя реальных возможностей поставки товаров или оказания услуг (наличие товаров, складских помещений, производственных мощностей и проч.).
- провести оценку юридической и фактической значимости документов, устанавливающих обязательства приобретателя векселя; в частности, проверить их точное соответствие нормам гражданского законодательства, наличие возможных признаков материального и интеллектуального подлога.

Особое внимание следует обращать на такую распространенную форму обмана, как обещание выплатить взамен полученного векселя определенные суммы в бюджеты различных уровней в погашение задолженности векселедателя.

Меры предупреждения обманного получения векселя под предлогом временной передачи ценной бумаги для подготовки к заключению будущей сделки. При разработке мер предупреждения указанной формы обмана следует исходить из содержания вексельного права, согласно которому вексель считается собственностью лица, у которого он находится (пока не доказано обратное). Не меняет положения и факт передачи векселя недобросовестному приобретателю по ошибке или вследствие заблуждения.

При учете сказанного, векселедатель при заключении сделок должен руководствоваться заранее разработанными правилами выдачи векселя. Указанные правила должны предусматривать меры по проверке будущего векселеприобретателя, а также документы, которые могут быть выданы вероятному контрагенту для оформления будущей сделки.

К последним относятся документы, подтверждающие факт создания и функционирования организации-векселедателя на законном основании, а также обеспеченность обязательств векселедателя по выдаваемым им ценным бумагам.

Сам же вексель должен храниться в сейфе векселедателя. Выдача векселя, даже не оформленного полностью, в том числе временная, до завершения сделки не допускается.

Меры предупреждения обманного завладения ранее проданным векселем под видом восстановления права на утраченную ценную бумагу. Напомним, что указанный способ обмана применяется в расчете на то, что векселеприобретатель не желает огласки факта приобретения векселя. По этой причине покупка векселя осуществляется без отражения совершенной сделки в соответствующих документах и подтверждения факта оплаты ценной бумаги.

Лучшим способом избежать обмана в указанных случаях является строгое соблюдение процедуры приобретения векселя, которая включает в себя составление договора о заключении гражданско-правовой сделки с использованием векселей, запись в регистре бухгалтерского учета, запись в специальном реестре с указанием серии и номера векселя, даты его составления, срока платежа, суммы векселя, вида и величины дохода по векселю, наименования получателя платежа (первого векселедержателя).

Кроме того, при выдаче векселя следует составить акт приема-передачи этой ценной бумаги, в котором указываются наименование документа; дата составления; содержание хозяйственной операции; реквизиты векселя, ссылка на договор, наименование должностей лиц, ответственных за совершение хозяйственной операции и правильность ее оформления, личные подписи и их расшифровка.

Меры предупреждения мошенничества в форме выдачи необеспеченных векселей. При разработке указанных мер следует учитывать, что вексельное законодательство не связывает право коммерческих организаций приобретать и выдавать векселя с фактической платежеспособностью участников вексельных отношений. Выдача и акцепт векселей могут быть обеспеченными или не имеющими дополнительного (кроме вексельного обещания) обеспечения. Государственный контроль за выдачей векселей некредитными организациями отсутствует. Поэтому лица, приобретающие векселя, должны оценить степень риска невозврата вексельной суммы самостоятельно.

Основанием для принятия решения о приобретении векселя должны стать результаты оценки платежеспособности векселедателя, обеспеченности организации собственными оборотными средствами для ведения хозяйственной деятельности и погашения срочных обязательств. Показатели указанных элементов баланса характеризуют состояние финансовой устойчивости организации-векселедателя.

Дополнительным признаком обеспеченности векселя является депонирование денежных средств или иных активов в размере вексельной суммы

депонирующей организации, а также гарантии Правительства или субъектов оссийской Федерации.

В случае депонирования активов в договоре с депонирующей организацией должно присутствовать указание на обеспечение использования имущества ля выполнения обязательств по векселю.

Положительная оценка финансовой устойчивости векселедателя не отменяет необходимости изучения его законопослушности, добросовестности деловой репутации вероятного партнера. Окончательное решение о приобретении векселя следует принимать на основе совокупности всех названных ыше показателей.

Меры защиты от приобретения векселя, выданного с заведомым дефектом ормы и реквизитов ценной бумаги. Для того чтобы избежать обмана в виде заедомого дефекта формы и реквизитов при оформлении покупки векселя, риобретатель ценной бумаги должен внимательно отнестись к проверке:

- наличия обязательных реквизитов векселя, предусмотренных ст. 1 и ст. 75 Положения о переводном и простом векселе;
- соблюдения правил написания реквизитов в соответствия с требованиями к написанию реквизитов, предъявляемыми Положением;
- соответствия формы бланка векселя Положению .

Следует учесть недопустимость в тексте векселя любых исправлений, в том исле заверенных.

Как дефект формы следует рассматривать отклонения от следующих требований ст. 1 Положения к реквизитам векселя:

- обязательство (для простых векселей) и предложение (для переводных векселей) уплатить не должно быть связано каким-либо условием (должно быть безусловным); любая оговорка к предложению или обязательству об уплате или любое условие, определяющее возможность наступления оплаты векселя, будут лишать данный документ вексельной силы;
- сумма уплаты по векселю (вексельная сумма) должна быть указана точно и не содержать разночтений в прописных и цифровых выражениях;
- указание на место составления векселя должно соответствовать полному (без сокращений) официальному наименованию пункта в соответствии с административно-территориальным делением;
- дата составления векселя обозначается согласно действующему в России календарному исчислению (число, месяц, год). При этом число обозначается цифрами, месяц указывается прописью, а год пишется полностью цифрами с добавлением после них слова «года»;
- плательщик по векселю (юридическое лицо) обозначается указанием полного собственного наименования и места нахождения в соответствии с его учредительными документами;
- плательщик по векселю (физическое лицо) указывает в векселе паспортные данные и место фактического проживания;

- срок платежа по векселю должен соответствовать одному из следующих четырех способов обозначения:
  1) по предъявлении;
  2) во столько-то времени от предъявления (через указанное число дней, месяцев или лет от даты предъявления);
  3) столько-то времени от составления (ради большей четкости вместо данного рекомендуется использовать нижеследующий способ);
  4) на определенный день;
- место платежа следует называть с указанием точного адреса и средств связи; векселедатель может дать дополнительное обязательство оплатить вексель в ином (помимо основного места платежа) месте, оформив это обязательство отметкой на вексельном бланке, однако следует учитывать, что протест векселя может быть совершен только по основному месту платежа;.
- наименование того, кому или по приказу кого должен быть совершен платеж должно включать полное название юридического лица в соответствии с его уставными и регистрационными документами; данные о физических лицах должны содержать фамилию, имя, отчество и сведения о паспорте;
- подпись векселедателя должна быть собственноручной либо выполненной другим лицом по доверенности на право совершения подписи. В последнем случае подпись сопровождается указанием: «По доверенности». Использование факсимильного штемпеля при подписании векселя не допускается;
- сведения о должностном лице, подписавшем вексель, должны включать в себя его фамилию, имя, отчество и должность, а также основание полномочий (Устав, доверенность и проч.). С целью предупреждения возможных ссылок на дефект подписи при выдаче векселя приобретатель указанной ценной бумаги должен тщательно следить за выполнением следующих условий оформления сделки. Если векселедатель является юридическим лицом, подпись на векселе должна скрепляться печатью организации-векселедателя с четко видимым текстом (во избежание использования печати другой организации). Рядом с подписью должны быть указанны фамилия, имя, отчество и должность подписавшего, а также основание полномочий (Устав, доверенность и проч.). Желательно наличие подписи главного бухгалтера организации. В случае подписания векселя по доверенности, доверенность (или ее нотариально заверенную копию) следует прилагать к векселю;
- отметка о предъявлении векселя к платежу (в случае срока платежа «во столько-то времени от предъявления») выполняется по требованию векселедержателя плательщиком и заверяется его подписью;
- векселедержатель должен обратить особое внимание на наличие в век-

«Подлежит акцепту не ранее (указанной даты)». Эти оговорки являются условием выплаты вексельных сумм. В случае их невыполнения векселедержатель лишится своих прав по причине неакцепта или неплатежа. Акцепт должен содержать указание на дату его совершения;

- переводный вексель, выданный в нескольких экземплярах, должен содержать номер экземпляра, в противном случае каждый экземпляр будет рассматриваться как самостоятельный вексель. Номер включается в формулировку указания об оплате, а также в заголовок векселя Prima, secunda, tertia (т. е. первый, второй и третий экземпляры);
- записи о дополнительных (вневексельных) обязательствах, касающихся формы погашения ценной бумаги, в тексте векселя не допускаются. Указанные обязательства при желании держателя векселя могут быть даны в отдельном документе в соответствии с требованиями, установленными гражданским законодательством;
- текст векселя может содержать записи о залоге (закладе) имущества в качестве дополнительного обязательства погашения платежа. При этом договор залога (заклада) составляется отдельно, а его реквизиты указываются в соответствующей записи в тексте векселя.

Меры предупреждения от приобретения поддельного векселя. Состоят из действий общепредупредительного характера и процедуры непосредственной проверки подлинности ценной бумаги.

Первые включают в себя защиту информации об особенностях применяемых технологий при заключении вексельных сделок; тщательный подбор сотрудников, участвующих в заключении вексельных сделок, систематический контроль за соблюдением ими установленных полномочий, процедуры принятия решений и порядка оформления сделок.

Признаки подозрительности предполагаемой сделки могут быть выявлены в ходе стандартной проверки надежности и добросовестности партнера, а также в результате анализа его поведения. Как элементы подозрительного поведения субъекта, желающего сбыть поддельный вексель, следует рассматривать установление им неслужебных отношений с персоналом, моменты психологической обработки сотрудников с целью создания у них отношения личной заинтересованности в заключении сделки (обещание комиссионных и иных видов благодарности), настойчивая демонстрация экономической привлекательности предлагаемой сделки.

Процедуры непосредственной проверки подлинности векселей проводятся в случаях:

- предъявления векселя к оплате;
- заключения сделки с использованием векселя (в том числе с использованием ценной бумаги в виде залога и при иных расчетах);
- приема векселя на депозитарное хранение;
- при передаче векселей организации-правопреемнику;

- при плановых внутренних проверках ценных бумаг, находящихся на хранении (в том числе архивном) в организациях, осуществляющих выдачу и приобретение ценных бумаг, а также депозитарную и посредническую деятельность с ними.

Непосредственная проверка векселя имеет целью выявление возможных признаков подделки (изготовление полностью фальсифицированного документа) или подлога (неправомерного изменения первоначального текста и реквизитов ценной бумаги).

Названная процедура включает в себя следующие действия:

- сличение реквизитов ценной бумаги с перечнем поддельных векселей (стоп-листом), информация о которых содержится на WEB-странице АУВЕР в сети Internet, а также в информационных письмах Банка России;
- осмотр ценной бумаги с целью обнаружения внешних признаков подделки или неправомерного изменения первоначального текста. В случаях, вызывающих сомнение в подлинности векселя, заинтересованное лицо имеет возможность обратиться за помощью к квалифицированным специалистам в соответствующие структуры, созданные кредитными организациями, Банком России, а также в экспертные подразделения МВД России и Гознака;
- сличение подписей и оттисков печати на векселе с заведомо подлинными образцами;
- фактическую проверку реквизитов и содержательной стороны текста векселя. Следует учесть, что номер векселя может быть изменен с целью избежать идентификации ценной бумаги по стоп-листу, а указанный в векселе номер телефона временно абонирован соучастниками мошенников, которые дают соответствующие «подтверждения» на телефонные запросы;
- непосредственное обращение к организации, выдавшей вексель (включая посещение офиса), с целью сверки содержания и реквизитов векселя с данными реестра, подтверждения подлинности имеющихся в документе подписей.

Предупреждение вредных последствий в случае порока выдачи векселя

В случае выхода векселя из владения держателя против его воли — кражи либо другого способа противоправного изъятия векселя у векселедержателя, а также в случае его исчезновения при невыясненных обстоятельствах законный держатель ценной бумаги, независимо от факта возбуждения уголовного дела, должен принять неотложные меры к восстановлению своих прав по утраченной ценной бумаге в порядке гражданского судопроизводства. В первую очередь следует обратиться в суд с заявлением о признании векселя недействительным и о восстановлении [illegible] собственнику похищенного

(утраченного) векселя возможность предотвратить возможные операции с векселем со стороны третьих лиц и восстановить убытки, независимо от успеха расследования.

Восстановление прав по утраченному векселю на предъявителя или признание векселя недействительным осуществляется в порядке вызывного производства, предусмотренного ст. 294–301 ГПК РФ. На первом этапе, после принятия заявления судья выносит определение о запрещении выдавшему документ лицу производить по векселю платежи или выдачи и направляет копию определения лицу, выдавшему документ, регистратору.

Этим же определением на заявителя возлагается обязанность опубликовать за свой счет в местном периодическом печатном издании следующие сведения:

- о факте обращения в суд в связи с утратой документа и наименование суда;
- собственное наименование заявителя, его место жительства или место нахождения;
- реквизиты векселя;
- предложение лицу, у которого, возможно, находится утраченный документ, обратиться в течение трех месяцев со дня опубликования в суд с заявлением о своих правах на этот документ.

Второй этап начинается в случае обращения нового владельца векселя в суд либо по истечении установленного срока такого обращения. Если вероятный новый держатель утраченного документа заявит о своих правах на вексель до истечения трех месяцев, суд разъясняет заявителю его право предъявить в общем порядке иск к держателю документа о его истребовании, а держателю документа — его право взыскать с заявителя убытки, причиненные принятыми запретительными мерами.

В тех случаях, когда заявление от нового держателя векселя в 3-месячный срок не поступило, суд принимает решение о признании векселя недействительным и восстанавливает права по утраченной ценной бумаге на предъявителя или ордерной ценной бумаге. Решение суда служит основанием для выдачи заявителю нового документа взамен признанного недействительным.

ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. В чем заключаются особенности вексельного законодательства?
2. Как вексельное законодательство соотносится с другими формами права?
3. В чем состоит различие между простым и переводным векселем?
4. Какие реквизиты должен содержать вексель. Что означает дефект формы векселя?
5. Какими особенностями вексельного права объясняются высокие риски в вексельном обороте?
6. Какими способами и для каких целей совершаются хищения векселей?
7. Какие способы обмана применяются при выдаче векселей?
8. Какие особенности характеризуют обман с использованием фальшивых векселей?
9. Перечислите виды мер предупреждения преступлений в сфере вексельного обращения.

Глава 7

ЗАЩИТА ОТ ПРЕСТУПЛЕНИЙ, ПОСЯГАЮЩИХ НА ПОРЯДОК ФУНКЦИОНИРОВАНИЯ БАНКА

- Злоупотребление полномочиями
- Коммерческий подкуп
- Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну
- Противоправные посягательства в сфере компьютерного обеспечения деятельности банка
- Противоправные посягательства на кадровое обеспечение банка
- Противоправные посягательства на нематериальные активы банка

7.1. Злоупотребление полномочиями

Обязательным условием нормального функционирования (управления деятельностью) банка является точное и добросовестное исполнение его сотрудниками требований федерального законодательства и других нормативных актов, определяющих политику и регулирующих деятельность банка. При этом следует иметь в виду, что наряду с постановлениями Правительства РФ, указаниями Банка России, иными регулятивными требованиями, устанавливающими стандарты деятельности и нормы профессиональной этики, определенное значение для организации работы банка имеют локальные (внутренние) нормативные акты.

В число названных актов входят документы двух видов. Первые — регламентируют лимитную и учетную политику банка, предписывают процедуры принятия соответствующих решений и выполнения банковских операций (определяют политику банка при проведении операций по размещению и привлечению средств; устанавливают порядок проведения операций на финансовых рынках, порядок открытия и обслуживания счетов клиентов). Вторые — наделяют работников банка определенными функциями и полномочиями (правом принятия решений о заключении договоров, разрешением на доступ к осуществлению операций в программном обеспечении, а также к базам данных компьютерных системах и др.). Указанные функции и полномочия могут быть изложены в уставе банка, должностных инструкциях либо положениях. Допускается их изложение в одном документе[1].

К сожалению, практика свидетельствует о том, что уровень ответственности лиц, выполняющих управленческие функции в коммерческих организациях, в том числе в банках, за последствия принимаемых решений, за сохранность

[1] Перечень внутренних документов, которые должны быть приняты соответствующими органами руководства банка, определен Положением Банка России от 16 декабря 2003 г. № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах».

эффективность использования имущества, а также за результаты финансово-хозяйственной деятельности остается низким.

Причина указанного положения в основном заключается в недостаточной компетентности управленцев. Однако в ряде случаев ущерб интересам коммерческих организаций (банка) причиняется в результате преступных посягательств со стороны указанных лиц. С точки зрения уголовного права такие деяния рассматриваются как злоупотребление полномочиями (ст. 201 УК РФ).

В соответствии с названной статьей, основанием для наступления уголовной ответственности является использование лицом, выполняющим управленческие функции в коммерческой или иной организации, своих полномочий вопреки законным интересам этой организации и в целях извлечения выгод и преимуществ для себя или других лиц либо нанесения вреда другим лицам, если это деяние повлекло причинение существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

Исходя из содержания статьи указанное деяние признается преступным при наличии следующих обязательных условий.

1. Лицо, совершающее деяние, формально действует в пределах своей служебной компетенции, однако фактически деяние совершается вопреки целям и задачам, принципам и правилам деятельности банка, определенным в нормативных правовых актах и учредительных документах.

2. Совершенное деяние должно причинить существенный вред правам и законным интересам граждан, организаций, общества или государства. Понятие существенного вреда является оценочным и рассматривается применительно к конкретным обстоятельствам преступления. Существенный вред может выражаться в форме прямого материального ущерба, упущенной материальной выгоды либо ущерба нематериальным благам банка (деловой репутации, деловым связям).

3. Наличие прямой связи между неправомерными действиями субъекта и наступившим существенным вредом.

Максимальное наказание, предусмотренное ч. 1 ст. 201 УК РФ, — лишение свободы на срок до трех лет.

Часть вторая названной статьи предусматривает наступление «тяжких последствий». Это понятие также является оценочным. Правоприменительная практика относит к тяжким последствиям экономическое банкротство организации, разорение акционеров и т. п. Максимальное наказание, которое может быть назначено виновному в совершении указанных деяний, — лишение свободы на срок до пяти лет.

Злоупотребления полномочиями могут совершаться в форме заключения заведомо невыгодного для банка договора, вступления в коммерческие отношения с фирмами-банкротами либо с мошенническими лжефирмами; в форме кредитования заведомо несостоятельных партнеров; незаконной передачи информации ограниченного распространения третьим лицам; в виде

использования реквизитов банка для совершения физическим лицом от имени банка лжебанковских операций (выдачи кредита под залог и др.).

Примером злоупотребления полномочиями могут служить действия бывшего управляющего пермским филиалом банка ВТБ К. Действуя вопреки установленным в банке правилам, К. принимал решения о выдаче займов заведомо неплатежеспособным компаниям, к тому же не имевшим вторичных источников погашения долга (залога). Преступная деятельность К. продолжалась с 2001 г. по 2005 г. и причинила банку ущерб в размере 190 млн руб.[1]

Субъектом преступления, предусмотренного ст. 201 УК РФ, может быть лицо, постоянно, временно либо по специальному полномочию выполняющее организационно-распорядительные (найм, организация труда и т. д.) или административно-хозяйственные (управление имуществом, заключение договоров и т. д.) обязанности.

При совершении указанного преступления лицо сознательно использует управленческие полномочия вопреки интересам своей организации, нарушает служебный долг с целью извлечения выгод (имущественного характера) и преимуществ (неимущественного характера) для себя или для других лиц. Деяние может совершаться также с целью причинения вреда другим лицам.

Уникальным по дерзости и простоте фактом злоупотребления полномочиями явились действия и. о. руководителя Хунзахского отделения Дагестанского филиала Сбербанка России Г., который приказал своим подчиненным оформить вклад на сумму 60 млн руб. на имя своего знакомого без фактического внесения денежных средств. Затем указанная сумма была получена наличными и предана фонду «Имам Шамиль». В ходе последующего расследования сотрудницы филиала в своих объяснительных записках утверждали, что в процессе оформления сделок на них оказывалось неприкрытое давление: в случае их отказа оформить операции по вкладу и последующему снятию денег Г. обещал всех уволить. Сам Г. и его знакомый утверждали на следствии, что денежная сумма была фактически внесена в банк[2].

Особенностью ст. 201 УК РФ является содержание п. 2 в примечании к ней, в соответствии с которым законодатель отказывается от принципа публичности при осуществлении уголовного преследования за деяния, предусмотренные указанной статьей и другими статьями главы 23 УК РФ в тех случаях, когда вред причинен исключительно коммерческой организации. Уголовное дело в названных ситуациях может быть возбуждено только по заявлению той организации или с ее согласия.

Меры предупреждения злоупотреблений осуществляются в первую очередь в форме административного и финансового контроля.

Задача административного контроля заключается в предупреждении отклонений от порядка проведения операций, которые должны осуществляться

[1] Банкир 5 лет грабил собственный банк // DENGI 59.ru (15 марта 2008 г.).

[2] *Герасимов А.* «Имам Шамиль» украл $ 2 млн. // Коммерсантъ. 2003. № 7/П. 20 янв.

только уполномоченными на то лицами и в строгом соответствии с определенными банком полномочиями и процедурами принятия решений.

Финансовый контроль должен предупреждать возможные отступления от принятой и закрепленной документами политики банка применительно к разным видам финансовых услуг и их адекватного отражения в учете и отчетности.

Указанные виды контроля должны с достаточной надежностью удостоверить, что доступ сотрудников к имуществу банка, к осуществлению операций по счетам клиентов и кредиторов допускается только в строгом соответствии с надлежащим образом удостоверенными полномочиями, а сами операции отражаются в учете в соответствии с установленными Банком России требованиями, реально отражают состояние активов и пассивов банка и обеспечивают составление установленных форм отчетности.

Названные меры предупреждения ущерба от противоправных либо некомпетентных действий работников банка представляют определенную систему, в реализации которой принимает участие и служба безопасности банка. Работа в указанном направлении начинается с контроля за подбором и расстановкой кадров с целью ограждения банка от лиц с сомнительной деловой и общественной репутацией, а также недостаточно компетентных лиц. Проверяется содержание заключенного с работником трудового соглашения (контракта) и наличие документа (служебной инструкции), четко регламентирующего должностные обязанности сотрудника до того, как он непосредственно приступил к исполнению служебных обязанностей.

В процессе исполнения работником возложенных на него обязанностей службой внутреннего контроля отслеживается эффективность и работоспособность систем, контролирующих соблюдение работником установленных правил совершения банковских операций и иных операций, осуществляемых банком на уровне банка и соответствующего структурного подразделения, надежность процедур и механизмов, исключающих выход работника за пределы установленного ему объема и состава банковских операций, соответствие условий осуществляемых работником сделок и операций общей политике привлечения или размещения ресурсов банка.

Кроме того, служба внутреннего контроля проверяет корректность ведения работником первичной документации; проведение в полном объеме установленных в банке процедур сверки, согласования и визирования, а также соблюдение процедуры формирования на базе документов балансовых данных.

Подробные рекомендации по осуществлению указанных мер службой внутреннего контроля содержатся в Положении Банка России № 242-П.

В обеспечении надежности функционирования систем банка путем предупреждения и выявления возможных нарушений установленного порядка, наряду со службой внутреннего контроля, участвует служба безопасности (служба защиты интересов) банка. В этих целях она принимает меры к обнаружению информации о возможных нарушениях порядка проведения отдельных

и соблюдения финансовой политики банка, о действиях сотрудников банка, выходящих за пределы установленных полномочий. Однако, в отличие от службы внутреннего контроля, пользующейся для получения необходимых сведений методами административного и финансового контроля, служба безопасности использует методы частного сыска и криминалистики.

По каждому выявленному факту злоупотребления полномочиями банку следует провести внутреннюю проверку (разбирательство) силами служб внутреннего контроля и безопасности банка, а его результаты зафиксировать в соответствующих документах.

Собранные документы должны содержать ответы на следующие вопросы: кто из служащих совершил правонарушение; какими документами установлены функциональные обязанности и полномочия виновного; в каких учредительных и иных документах содержатся сведения о целях, задачах и направлениях деятельности организации (банка); в чем именно заключается злоупотребление полномочиями; каков примерный объем причиненного вреда.

Желательно также приобщить к материалам проверки документы, подтверждающие факт злоупотребления (например, бухгалтерские записи, в том числе черновые), вид и размеры причиненного ущерба (заключение специалиста-бухгалтера), а также указывающие на местонахождение похищенных материальных ценностей, денежных счетов.

Собранные в результате внутренней проверки (разбирательства) материалы и документы потребуются для решения вопроса о наказании виновного и компенсации причиненного им ущерба.

В случае, если банком в лице его исполнительного органа (либо собрания акционеров, когда деяние совершил руководитель) будет принято решение о направлении заявления в правоохранительные органы для решения вопроса о возбуждении уголовного дела, материалы проверки следует приложить к заявлению.

Не исключено, однако, что потерпевшая ущерб коммерческая организация (банк) откажется от намерения привлечь виновного к уголовной ответственности. В основе такого решения может лежать опасение причинить вред деловой репутации банка и т. п. В таком случае эти материалы могут быть использованы в качестве основания для принятии решения о прекращении трудового договора с виновным в связи с утратой доверия к нему со стороны работодателя в соответствии с п. 7 ст. 81 ТК РФ. Решение о прекращении трудового договора по указанному основанию обладает значительным карательным и профилактическим эффектом, поскольку (в соответствии со ст. 16 Закона о банковской деятельности) уволенный лишается права занимать в течение двух последующих лет должности руководителя исполнительных органов и главного бухгалтера кредитной организации.

Кроме того, не следует упускать из виду, что перед банком, наряду с решением вопроса о персональной ответственности лица, злоупотребившего полномочиями, может стоять задача компенсировать потери, причиненные заведомо

невыгодным договором (сделкой) и другими действиями виновного. Одним из путей ее решения является обращение в суд с гражданско-правовым иском о признании договора недействительным по основаниям, предусмотренным ст. 173 ГК РФ (недействительность сделки юридического лица, выходящей за пределы его правоспособности), ст. 174 ГК РФ (последствия ограничения полномочий на совершение сделки) или ст. 179 ГК РФ (недействительность сделки, совершенной под влиянием обмана, насилия, угрозы, злонамеренного соглашения представителя одной стороны с другой стороной или стечения тяжелых обстоятельств).

В указанных случаях материалы, полученные в результате внутренней проверки (разбирательства), могут быть использованы в качестве судебных доказательств. Следует учесть, однако, что для признания сделки недействительной по основаниям ст. 174 ГК РФ и ст. 179 ГК РФ необходимо, кроме фактов, подтверждающих противоправный умысел уполномоченного работника банка, собрать сведения, соответственно, о недобросовестности или злонамеренности третьего лица.

Следует отметить, что лица, злоупотребляющие полномочиями, предвидя возможность обнаружения их противоправных действий, нередко заранее предпринимают меры, направленные на уклонение от уголовной и иной ответственности.

Реализуется этот замысел в форме различных действий в виде маскировки фактов совершения заведомо убыточных сделок, утаивания, уничтожения либо фальсификации относящихся к ним документов. Преступный умысел может маскироваться мнимой ошибкой, якобы допущенной при правовом оформлении сделки, либо в процессе экономических расчетов. Нередко виновные утверждают, что при совершении сделок за пределы своих функциональных обязанностей и полномочий не выходили.

Указанным способам уклонения от ответственности способствуют недостатки в делопроизводстве организации, нечетко составленные документы, регламентирующие порядок принятия решений и совершения операций (либо их отсутствие), а также недостатки документов, устанавливающих функции полномочия работников управленческого звена.

Риск понести убытки от указанных преступных действий (в банковском деле риски указанного вида принято именовать рисками, вызываемыми последствиями неправомерных или некомпетентных решений отдельных работников) может быть существенно снижен путем осуществления ряда предупредительных мер, которые осуществляют служба внутреннего контроля, юридическая служба и служба безопасности банка.

В основу указанных мер входит проверка наличия документов, регулирующих деятельность банка (определяющих процедуры принятия решений, распределение функций и полномочий между подразделениями и сотрудниками банка и т. п.). Особое внимание следует обратить на наличие должностных инструкций для всех штатных должностей в банке.

7.2. Коммерческий подкуп

Коммерческий подкуп — явление весьма распространенное во всех странах с рыночной экономикой и во многих случаях имеет интернациональный характер. Так, в январе 2000 г. в Швейцарии было проведено расследование дел о подкупе сотрудников двух крупнейших банков страны UBS и Credit Suisse. Тринадцать человек из 8 стран — Германии, Франции, Великобритании, Голландии, Австрии, Италии, США и Израиля — обвинялись в незаконном получении сведений о счетах клиентов указанных банков. Обвинение предъявлено семи банковским служащим и четырем швейцарским частным детективам, которых подкупали иностранцы для получения нужных им сведений. По данным швейцарских правоохранительных органов суммы, затраченные на подкуп виновных, составляли до 65 тыс. долл. за запрос.

Особенность этого вида деяний заключается в стремлении лица, совершающего подкуп, заинтересовать сотрудника банка, выполняющего управленческие функции, получением различного рода личных выгод и мнимой безобидностью (безнаказанностью) действий, которые ему предлагается выполнить.

Действия лиц, участвующих в коммерческом подкупе, посягают на нормальное управление банком. При этом указанное преступление не является самоцелью. Лицо, осуществляющее подкуп, как правило, добивается совершения в его интересах других действий, наносящих ущерб интересам банка или конкурента. Наиболее распространенными в банковской практике являются попытки коммерческого подкупа за нарушение установленного порядка кредитования, которое выражается в установлении льготных процентных ставок либо освобождении от взимания процентов; в выдаче несоответствующей действительности заключения о возможности физического или юридического лица погасить задолженность; в предоставление кредита без определения конкретной цели либо с превышением предельно допустимых размеров для одного заемщика; выдачу кредита под фиктивную цель.

Нередко коммерческий подкуп совершается в целях получения необоснованных банковских гарантий либо информации, составляющей банковскую или коммерческую тайну. Целью подкупа могут быть также не соответствующие установленному порядку решения в сфере кадрового обеспечения банка, а также в любых других сферах управления банком.

Непосредственным объектом коммерческого подкупа является точное и добросовестное исполнение сотрудниками коммерческой организации своих служебных обязанностей в соответствии с требованиями федерального законодательства, иных нормативных актов, а также внутренних документов, определяющих политику и регулирующих деятельность банка.

Отечественная судебная практика по уголовным делам о коммерческом подкупе по существу делает первые шаги, так как в УК РСФСР 1960 г. этот состав преступления отсутствовал. Он появился лишь в УК РФ 1996 г., однако

определенный опыт в выявлении, предупреждении и расследовании дел указанной категории уже накоплен.

В марте 1999 г. органами МВД России по ст. 204 УК РФ привлечен к уголовной ответственности председатель правления Волжского социального банка К. Ему предъявлено обвинение в том, что он выдавал клиентам крупные кредиты в обмен на денежное вознаграждение. В частности, К. негласно оказывал содействие одному из крупнейших заемщиков банка — самарской фирме «Пилот». В течение 1997–1998 гг. эта фирма имела в ВСБ открытую кредитную линию и получила от банка в общей сложности более 10 млрд руб. кредитов. По данным следствия в благодарность за эту услугу руководство фирмы ежемесячно передавало К. в качестве вознаграждения несколько десятков тысяч долларов. Правоохранительными органами действия банкира и клиентов квалифицированы как коммерческий подкуп[1].

В настоящее время определенное распространение получили попытки коммерческого подкупа лиц, ответственных за подготовку договоров потребительского кредитования.

В 2007 г., например, к уголовной ответственности по ст. 204 УК РФ привлечен эксперт одного из банков Амурской области, оформлявший кредитные договоры на заведомо неплатежеспособных заемщиков. За свои противоправные действия работник банка получал от организатора преступной деятельности вознаграждение в размере половины выданных банком денежных сумм[2].

Согласно материалам опросов представителей российских коммерческих банков, попытки подкупа в отношении сотрудников банков получили в отечественной практике широкое распространение. По данным МВД России, количество уголовных дел, возбужденных по фактам коммерческого подкупа, в стране в 2005 г. составило 2178, в 2006 г. — 1751, в 2007 г. — 1786.

Учитывая высокую латентность этого вида преступлений, следует полагать, что их фактическое количество значительно выше названных статистических показателей.

Негативные последствия коммерческого подкупа не исчерпываются материальным ущербом для банка и его добросовестных партнеров. В случае необоснованного предоставления (за вознаграждение) льгот и преимуществ одним участникам рынка перед другими ущерб наносится также деловой репутации и деловым связям банка.

Статья 204 «Коммерческий подкуп» УК РФ устанавливает уголовную ответственность для двух категорий лиц.

К первой (ч. 1 и 2 ст. 204 УК РФ) — относятся субъекты, незаконно передающие лицу, выполняющему управленческие функции в коммерческой или иной организации, деньги, ценные бумаги, иное имущество, а равно незаконно

[1] Банкира подкупили для того, чтобы получить кредиты // Самарское обозрение. 1999. № 13. 29 марта.

[2] Банкир.РУ. 2007. 29 мая.

оказывающие ему услуги имущественного характера за совершение действий в интересах дающего. Для совершения указанных действий лицо, выполняющее управленческие функции, использует свое служебное положение.

Вторую (ч. 3 и 4 ст. 204 УК РФ) — составляют лица, незаконно получающие деньги, ценные бумаги, иное имущество, а равно незаконно пользующиеся услугами имущественного характера за совершение действий в интересах дающего. Указанные действия совершаются в связи со служебным положением, которое занимает лицо, получающее незаконное вознаграждение.

В качестве выгод или услуг имущественного характера, составляющих незаконное вознаграждение, судебная практика рассматривает подлежащие оплате (но не оплаченные лицом, которое получило блага) предоставление туристических и санаторных путевок, ремонт квартиры, строительство дачи и т. п. К выгодам имущественного характера, по смыслу закона, следует относить также занижение стоимости передаваемого имущества, уменьшение арендных платежей, процентных ставок за пользование банковскими ссудами.

Деяние, предусмотренное ч. 1 ст. 204 УК РФ, совершается с прямым умыслом и специальной целью склонить лицо, выполняющее управленческие функции в банке, совершить за вознаграждение определенные действия (бездействие). Ответственность за коммерческий подкуп может нести любой вменяемый гражданин, достигший 16-ти лет.

Действия субъекта, выполняющего управленческие функции, которые он совершает в пользу лица, осуществившего коммерческий подкуп, в одних случаях могут входить в круг его служебных обязанностей, в других — быть неправомерными, не вытекать из его служебных полномочий или совершаться вопреки интересам службы. Последние могут сами по себе содержать признаки иного преступления либо правонарушения. Часть 2 ст. 183 УК РФ, например, устанавливает уголовную ответственность за незаконное разглашение сведений, составляющих коммерческую или банковскую тайну. В случаях, когда деяние, совершенное лицом, выполняющим управленческие функции в банке, содержит состав самостоятельного преступления, виновный подлежит ответственности по совокупности преступлений — по ст. 204 УК РФ.

Субъектом преступления, предусмотренного ч. 3 ст. 204 УК РФ может быть только лицо, выполняющее управленческие функции в банке (либо другой коммерческой организации).

Максимальное наказание, предусмотренное ч. 1 ст. 204 УК РФ, — лишение свободы на срок до двух лет; ч. 2 — лишение свободы на срок до четырех лет; ч. 3 — лишение свободы на срок до трех лет; ч. 4 — лишение свободы на срок до пяти лет.

Меры предупреждения и методика внутреннего разбирательства по выявленному факту коммерческого подкупа в значительной мере совпадают с порядком разбирательства по фактам злоупотребления полномочиями.

Как и в случаях разбирательства по фактам злоупотребления полномочиями следует выяснить: кто из служащих совершил правонарушение; какими документами установлены функциональные обязанности и полномочия виновного; в каких учредительных и иных документах содержатся сведения о целях, задачах и направлениях деятельности организации (банка). Кроме того, следует установить, в чем именно заключаются преимущества, предоставленные лицу, совершившему подкуп, какой вред причинен банку в результате подкупа (имущественный ущерб, ущерб деловой репутации и т. д.).

Следует также выяснить, какие именно блага получил виновный сотрудник банка, какова их оценка в денежном исчислении. В материалах разбирательства должно быть зафиксировано, за выполнение каких конкретных действий (бездействия) выполняющий управленческие функции сотрудник банка получил предмет коммерческого подкупа от заинтересованного лица. Имущественные выгоды в виде денег, иных ценностей, оказание материальных услуг в случаях коммерческого подкупа могут быть предоставлены не самому сотруднику банка, а родным и близким сотрудника с его согласия. Оказанные услуги оцениваются на основании цен, расценок или тарифов за услуги, действовавших на момент совершения преступления.

Как и в случаях злоупотребления полномочиями, к материалам разбирательства желательно приобщить документы, подтверждающие факт незаконного получения денег сотрудником банка, существо действий, выполненных им в интересах дающего лица, вид и размеры причиненного ущерба.

При решении вопроса об ответственности сотрудника банка, совершившего действия (бездействие) в интересах дающего лица, применяется общее правило для всех деяний, предусмотренных главой 23 «Преступления против интересов службы в коммерческих и иных организациях» УК РФ: отказ законодателя от принципа публичности. В случаях, когда в результате коммерческого подкупа вред причинен исключительно коммерческой организации, уголовное дело может быть возбуждено только по заявлению этой организации или при ее согласия.

Если банком будет принято решение о направлении заявления в правоохранительные органы для решения вопроса о возбуждении уголовного дела, материалы проверки следует приложить к заявлению.

В случае отказа банка от намерения привлечь виновного к уголовной ответственности эти материалы могут быть использованы в качестве основания для принятии решения о расторжении трудового договора с виновным в связи с утратой доверия к нему со стороны работодателя (в соответствии с п. 7 ст. 81 ТК РФ).

Кроме того (наряду с решением вопроса о персональной ответственности подкупленного сотрудника), перед банком возникает задача компенсировать потери, причиненные неправомерными действиями. Одним из путей ее решения является обращение в суд с гражданско-правовым иском. В указанных случаях материалы, полученные в результате внутренней проверки (разбирательства),

могут быть использованы в качестве основания для иска и судебных доказательств.

Предупреждение коммерческого подкупа осуществляется путем применения комплекса мер организационного, административного и финансового характера, а также приемов и методов, использующихся службой безопасности банка.

Задача административного контроля заключается в предупреждении отклонений от порядка проведения операций, которые должны осуществляться в строгом соответствии с определенными банком полномочиями и процедурами принятия решений.

Финансовый контроль должен предупреждать возможные отступления от принятой и закрепленной документами политики банка применительно к разным видам финансовых услуг и их адекватного отражения в учете и отчетности.

Меры предупреждения ущерба от противоправных действий работников банка, совершаемых в результате коммерческого подкупа, в целом совпадают с системой, которая используется для предупреждения злоупотребления полномочиями. Они начинаются с контроля за отбором и расстановкой кадров с целью ограждения банка от лиц с сомнительной деловой и общественной репутацией (меры организационного характера). Проверяется также содержание заключенного с работником трудового соглашения (контракта) и наличие документа (служебной инструкции), четко регламентирующего должностные обязанности сотрудника до того, как он непосредственно приступил к исполнению служебных обязанностей.

В процессе исполнения работником возложенных на него обязанностей службой внутреннего контроля отслеживается соблюдение им установленных правил совершения банковских операций, надежность процедур и механизмов, исключающих выход работника за пределы установленного ему объема и состава банковских операций, соответствие условий осуществляемых работником сделок и операций общей политике привлечения или размещения ресурсов банка.

Кроме того, служба внутреннего контроля проверяет корректность ведения работником первичной документации; проведение в полном объеме установленных в банке процедур сверки, согласования и визирования, а также соблюдение процедуры формирования на базе документов балансовых данных.

Служба безопасности банка принимает меры к обнаружению информации о попытках коммерческого подкупа сотрудников, о возможных нарушениях порядка проведения операций и соблюдения финансовой политики банка, о действиях сотрудников банка, выходящих за пределы установленных полномочий. В указанных целях используются методы частного сыска и криминалистики.

7.3. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну

Законодательство о защите банковской тайны, основанное на Конституции РФ, включает в себя положения Гражданского кодекса РФ, Уголовного кодекса РФ, Закона о банковской деятельности, Закона о коммерческой тайне, ряда других законов и подзаконных актов.

Принципиальной основой для разработки законодательных норм, посвященных регулированию отношений, связанных с созданием, использованием и защитой информации, составляющей банковскую тайну, служат положения Закона об информации. Названный закон ввел понятие конфиденциальной информации, разновидностью которой является банковская тайна, и явился основанием для правомерного ограничения доступа к составляющим ее сведениям и их защите от посторонних в порядке, предусмотренном законодательством Российской Федерации.

Определяющую роль в формировании системы норм, регулирующих отношения по поводу банковской тайны, играет отнесение информации, в соответствии со ст. 128 ГК РФ к одному из видов объектов гражданских прав, наряду с вещами, деньгами и ценными бумагами, иным имуществом, имущественными правами; работами и услугами; результатами интеллектуальной деятельности и нематериальными благами.

Согласно ст. 26 Закона о банковской деятельности банковскую тайну составляют сведения об операциях, о счетах и вкладах клиентов и корреспондентов, а также иные сведения, устанавливаемые кредитной организацией, если ограничение свободного доступа к этим сведениям не противоречит федеральному законодательству. К числу не конкретизированных законодателем в данной норме «иных сведений», составляющих банковскую тайну, относятся: содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности; данные аналитических и специальных исследований о состоянии и тенденциях развития рынка, о надежности и финансовой устойчивости клиентов (в том числе потенциальных); сведения о средствах и способах обеспечения работы автоматизированных информационных систем и их технологий (программных, технических, лингвистических и организационных); сведения, раскрывающие систему, средства и методы защиты информации на средствах вычислительной техники банка от несанкционированного доступа, а также значения действующих кодов и паролей; информация о деятельности по защите интересов банка, о лицах (сотрудниках и клиентах банка), участвующих в деятельности банка и банковских операциях, а также о силах, средствах и способах обеспечения безопасности банка.

В числе субъектов, обязанных хранить банковскую тайну, законодательство называет сотрудников банка, контрагентов банка, аудиторов и государственных служащих, получивших доступ к закрытым сведениям в связи с исполнением служебных обязанностей.

В практике организации защиты банковской тайны нередко возникает вопрос о соотношении составляющих ее сведений со сведениями, отнесенными к коммерческой и служебной тайне. Анализ правовых норм, регулирующих отношения по поводу названных видов информации, свидетельствует о том, что банковская тайна является частным видом коммерческой тайны, точно так же, как банковская деятельность представляет собой один из видов коммерческой деятельности. В свою очередь коммерческая и банковская тайна в определенных ситуациях могут получить статус «служебной тайны», не меняя при этом фактического содержания. Критерием отнесения информации к различным категориям тайн (банковской, коммерческой или служебной) в таких случаях является правовой статус субъектов, в собственность (распоряжение) которых поступили конфиденциальные сведения. Так, например, согласно ч. 4 ст. 10 Закона о бухгалтерском учете, содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности организаций является коммерческой тайной. Вполне понятно, что применительно к деятельности банка содержание названных регистров одновременно приобретает статус банковской тайны.

Возможность изменения правового статуса сведений, *защищаемых в соответствии с Гражданским кодексом РФ*, на статус *служебных* предусмотрена Указом Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». Основанием для указанных изменений является принятие органами государственной власти решения об ограничении доступа к поступившим к ним конфиденциальным сведениям коммерческого характера.

Законодательство Российской Федерации относит к сведениям служебного характера лишь ту информацию, которая связана с деятельностью по обеспечению государственной службы. Часть такой информации (в том числе составляющей банковскую тайну) истребуется у кредитных организаций государственными структурами (правоохранительными и другими органами). Кроме того, в соответствии со ст. 14 Закона о государственной службе, государственные служащие имеют право на получение в установленном порядке информации и материалов, необходимых для исполнения своих должностных обязанностей. В этих целях они могут посещать предприятия, учреждения и организации независимо от форм собственности. Конфиденциальные сведения (в том числе банковская тайна), полученные государственными органами (и их сотрудниками) в связи с исполнением должностных обязанностей, приобретают статус «служебной тайны», порождающий правовые последствия как для государственных структур в целом, так и для отдельных служащих, допущенных к этой информации. Использование указанных сведений регламентировано Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденным постановлением Правительства РФ № 1233 (и соответствующими ведомственными инструкциями).

Общее требование законодательства о государственной гражданской службе об обязанности служащих хранить в тайне доверенные им закрытые сведения могут конкретизироваться нормами «отраслевых» законов. Так, Таможенный кодекс РФ (Тм РФ) запрещает таможенным органам и их должностным лицам разглашать, использовать в личных целях либо передавать третьим лицам, в том числе государственным органам, информацию, составляющую государственную, коммерческую, *банковскую,* налоговую или иную охраняемую законом тайну, и другую конфиденциальную информацию (ч. 2 ст. 10 Тм РФ).

Закон связывает существование банковской, коммерческой и служебной тайны с обязательным одновременным наличием трех составляющих ее элементов:

1) действительной или потенциальной коммерческой ценностью информации в силу неизвестности ее третьим лицам;

2) отсутствием свободного доступа к ней на законном основании;

3) мерами по охране конфиденциальности информации, принимаемыми ее обладателем.

Отсутствие хотя бы одного из перечисленных элементов лишает информацию статуса коммерческой тайны.

Сведения коммерческого, управленческого, научно-технического и иного характера (например, информация о способах организации работы либо о применении приемов, позволяющих повысить доходность, сведения о фактических затратах банка в конкретных операциях, на основании которых можно рассчитать его финансовую конкурентоспособность), не имеют изобретательского уровня и не охраняются патентным правом. Однако они находятся в исключительном владении субъекта хозяйственной деятельности, которому их раскрытие может причинить экономический ущерб. В связи с этим законодательство наделяет обладателя указанной информации правом придать ей статус охраняемой путем отнесения к банковской тайне и таким образом закрыть свободный доступ к ней на законном основании.

Приняв решение об отнесении сведений к банковской тайне, их обладатель обязан применить ряд установленных законодательством средств и методов их защиты и носителей, на которых они размещены, и выполнить в этих целях определенные мероприятия по охране конфиденциальности информации.

Для того чтобы стать объектом правовых отношений, информация, составляющая банковскую тайну, должна быть зафиксирована на материальном носителе (бумаге, магнитном носителе или других материальных объектах, в том числе физическом поле) и снабжена реквизитами, позволяющими ее идентифицировать. Право собственности на информацию, зафиксированную на материальном носителе, возникает с момента регистрации в установленном порядке документа, в котором она содержится.

Зафиксировав право собственности на документ, обладатель банковской тайны обязан установить специальный порядок обращения с ним (включить его в систему охранительных отношений).

Факт внесения документа в эту систему отражается в соответствующем грифе конфиденциальности, который наносится на каждый экземпляр носителя информации (например, «банковская тайна — конфиденциально», «тайна банка» — конфиденциально и т. п.). Установленный таким образом гриф является официальным охранительным знаком — предупреждением о закрытии свободного доступа к документу. Дальнейшее обращение с документами, включенными в охранительную систему, осуществляется в особом правовом режиме. Лица, допускаемые к конфиденциальным документам и содержащейся в них информации, должны дать соответствующие письменные обязательства в отношении их защиты.

Наряду с грифом конфиденциальности защищаемый документ должен содержать регистрационный номер, товарный знак (знак обслуживания, фирменное наименование) или иные знаки, зарегистрированные в установленном порядке, позволяющие идентифицировать законного обладателя сведений, принявшего меры по охране их конфиденциальности[1].

Применение этих мер призвано предотвратить возможное заявление нарушителя порядка обращения с конфиденциальными сведениями о непреднамеренном характере своих действий. Кроме того, соблюдение установленного порядка позволяет использовать документы, подготовленные с помощью ЭВМ, в качестве доказательств[2].

Охранительная система должна не только ограничить круг лиц, имеющих доступ к документам, содержащим конфиденциальные сведения, и сделать их недоступными для посторонних, но и обеспечить оптимальный режим пользования ими для тех, кому они доверены.

Обязательства лиц и организаций по сохранению банковской тайны оговариваются в отдельных пунктах трудовых (для работников банка) и гражданско-правовых (организаций) договоров.

Лица, не имеющие доступа к банковской тайне, относятся к категории посторонних.

Следует учесть, что согласно ст. 5 Закона о коммерческой тайне и постановлению Правительства РФ от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну» (с учетом изменений, внесенных Постановлением Правительства РФ от 3 октября 2002 г. № 731 «Об изменении и признании утратившими силу некоторых постановлений Совета Министров РСФСР, Правительства РСФСР и Правительства Российской Федерации, касающихся государственной регистрации юридических лиц») к категории сведений, составляющих коммерческую (а следовательно и банковскую) тайну, не могут быть отнесены учредительные документы и устав банка; лицензия на право осуществления банковской деятельности; документы, подтверждающие факт внесения записей о юридических лицах в Единый государственный реестр юридических лиц; сведения по установленным формам отчетности о результатах финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему России; документы о платежеспособности; сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных мест; документы об уплате налогов и обязательных платежах; данные о нарушениях законодательства России.

В процессе обмена информацией с органами Министерства по налогам и сборам России, Федеральной службе по финансовому мониторингу России и другими государственными структурами банки вынуждены сообщать по требованию их представителей сведения, выходящие за пределы указанного выше перечня и составляющие банковскую тайну. Такая информация охраняется как совместная собственность государства и представивших ее субъектов. Ответственность за ее сохранность в государственных учреждениях несут государственные служащие.

Основания и виды ответственности за нарушения законодательства о банковской тайне

Основными видами нарушений законодательства о банковской тайне, влекущими правовые последствия, являются незаконное получение, разглашение или использование сведений, составляющих коммерческую (банковскую) тайну. Ответственность за совершение указанных действий предусмотрена системой норм уголовного, гражданского, трудового и административного законодательства.

Уголовно-правовая ответственность за преступные посягательства на коммерческую (банковскую) тайну установлена ст. 183 «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» УК РФ. Названная статья предусматривает два состава преступления: собирание сведений, составляющих коммерческую, налоговую или банковскую тайну (ч. 1 ст. 183 УК РФ), и незаконное разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца (ч. 2 ст. 183 УК РФ).

Объектом преступления, предусмотренного ст. 183 УК РФ, являются отношения по поводу нормальной предпринимательской деятельности; предметом

[1] Соблюдение указанных условий обязательно также и для информации, которая циркулирует (поступает, обрабатывается, хранится и выдается) в средствах вычислительной техники.

[2] Инструктивные указания от 29 июня 1979 г. № И-1–4 Госарбитраж СССР «Об использовании в качестве доказательств по рабитражным делам документов, подготовленных с помощью электронно-вычислительной техники».

юсягательства — банковская тайна (информация, обладающая признаками, /становленными ст. 26 Закона о банковской деятельности и ст. 857 ГК РФ.

Для наступления уголовной ответственности по ч. 1 ст. 183 УК РФ доста-очно установления факта собирания сведений, составляющих банковскую айну, независимо от последствий этих действий. В отличие от этого состава /головная ответственность по ч. 2 ст. 183 УК РФ за разглашение и использо-ание указанных выше сведений без согласия владельца наступает лишь в слу-ае причинения указанными действиями крупного ущерба. Объективная сто-рона преступления, предусмотренного ч. 1 ст. 183 УК РФ, состоит в собира-нии указанных сведений одним из способов, указанных в диспозиции: путем ювхищения документов, подкупа или угроз, а равно иным незаконным путем.

При этом законодатель не устанавливает разграничений по способу похи-щения документов. Оно может быть тайным либо открытым, с применением насилия или путем обмана.

Собирание сведений, составляющих банковскую тайну, путем подкупа оз-начает незаконное получение соответствующей информации от лиц, которым она доверена, в обмен на вознаграждение денежного либо имущественного характера.

Факт подкупа лица, которому была доверена банковская тайна, установлен при расследовании упомянутого выше дела бывшего начальника службы ин-формационной безопасности процессинговой компании Union Card в России Андрея Голова. Последний в течение нескольких лет обеспечивал группу меж-дународных преступников информацией о счетах, вкладах, номерах пластико-вых карт и персональных кодах иностранцев, которые обслуживались процес-синговым центром Union Card. Разглашенная Головым информация использо-валась его сообщниками для хищений денежных средств со счетов владельцев карт.

Понятие угрозы в смысле ст. 183 УК РФ охватывает угрозу убийством, ричинением вреда здоровью, уничтожением или повреждением имущества лица, располагающего коммерческой тайной, а равно его близких. Приме-ие подкупа или угрозы является приемом, с использованием которого субъ-ект преступления (организатор, подстрекатель) склоняет или понуждает к раз-глашению информации лицо, которому она доверена.

Иные незаконные способы собирания банковской тайны могут составлять действия по завладению сведениями без изъятия содержащих информацию документов: путем выведывания ее у осведомленных лиц, перехвата информа-ции, циркулирующей в технических средствах и помещениях, и т. п.

В случаях, когда лицо, собирающее указанные выше сведения, совершает действия, выходящие по степени общественной опасности за рамки ст. 183 УК РФ, содеянное следует квалифицировать по совокупности преступлений. Например, кража ПЭВМ с целью завладения содержащейся в ней информа-ции представляет собой совокупность преступлений, предусмотренных ст. 158 и 183 УК РФ.

Преступление совершается с прямым умыслом и специальной целью. То есть лицо сознает, что собирает сведения, составляющие банковскую тайну, и желает этого в целях их разглашения или незаконного использования.

Субъект преступления, предусмотренного ч. 1 ст. 183 УК РФ, — лицо, дос-игшее 16-ти лет. Уголовное законодательство России не содержит отдельной нормы, устанавливающей наказание для лиц, специально внедренных в орга-низацию либо завербованных из числа ее сотрудников для незаконного соби-рания сведений, составляющих банковскую тайну. Действия таких лиц отно-сятся к обстоятельствам, отягчающим наказание (ст. 63 УК РФ — совершение преступления с использованием доверия, оказанного виновному в силу его служебного положения или договора).

Максимальное наказание, предусмотренное ч. 1 ст. 183 УК РФ, — лишение свободы на срок до двух лет.

Незаконное разглашение или использование сведений, составляющих коммерческую или банковскую тайну (ч. 2 ст. 183 УК РФ), выражается в предании сведений огласке, т. е. в совершении таких действий, в результате которых находящиеся в обладании виновного сведения, составляющие ком-мерческую или банковскую тайну, стали достоянием посторонних лиц. Све-дения могут быть разглашены в процессе частной переписки или разговора либо переданы лицу, которое их незаконно собирает, в результате подкупа или угрозы.

Посторонним является любое лицо, не имеющее права доступа к подобно-го рода информации.

Использование сведений, составляющих банковскую тайну, предполагает их применение в ущерб владельцу, чаще всего для незаконного завладения его денежными средствами (путем их хищения с банковского счета) или в целях недобросовестной конкуренции.

Субъективная сторона разглашения характеризуется умышленной формой вины. Лицо сознает, что незаконно разглашает или использует коммерческую тайну, предвидит причинение ущерба ее владельцу и желает либо сознательно допускает наступление этих последствий.

Субъект преступления — лицо, которому по роду работы или выполняе-мых служебных обязанностей стали известны сведения, составляющие бан-ковскую тайну.

Максимальное наказание, предусмотренное ч. 2 ст. 183 УК РФ, — лишение свободы на срок до трех лет.

Обязанность возместить материальный ущерб за несанкционированное разглашение или использование банковской (коммерческой) тайны может быть возложена не только на физических лиц, но и на организацию, приняв-шую на себя соответствующее обязательство по договору о неразглашении информации.

При этом организация принимает на себя ответственность за действия лиц, которые работают или работали в ней по найму. Основанием для

предъявления иска является несоблюдение оговариваемой в необходимой степени осторожности в обращении с конфиденциальной информацией, в частности, в невыполнении соответствующих организационных и правовых мер ее защиты, которые способствовали выходу информации из законного владения.

Ответственность работников банка за нарушение порядка обращения с конфиденциальной информацией предусмотрена Трудовым кодексом РФ. Необходимым условием установления такой ответственности является заключение трудового договора, содержащего обязательства работника о неразглашении охраняемой законом тайны (в соответствии со ст. 57 ТК РФ).

Разглашение сведений, составляющих охраняемую законом тайну (в том числе банковскую), является основанием для расторжения трудового договора по инициативе работодателя (подп. «в» п. 6 ст. 81 ТК РФ) и возложения на работника материальной ответственности в полном размере причиненного ущерба (п. 7 ст. 243 ТК РФ).

Обязанности работника по сохранению банковской тайны регламентируются действующими в организации правилами конфиденциального делопроизводства, которые устанавливают прямой запрет на незаконное получение, разглашение или использование сведений, составляющих банковскую тайну.

В установленном Трудовым кодексом РФ порядке реализуется также ответственность *государственных служащих*, нарушивших установленные в государственном органе правила работы со служебной информацией и не выполнивших обязанность хранить государственную и иную охраняемую законом тайну (в том числе банковскую).

Указанные обязанности возложены на государственных служащих п. 7 ст. 15 Закона о государственной службе.

Нарушение правил работы со служебной информацией дает основание для наложения на виновного дисциплинарного взыскания, предусмотренного ст. 57 Закона о государственной службе (замечание, выговор, предупреждение о неполном должностном соответствии, освобождение от замещаемой должности гражданской службы, увольнение с гражданской службы).

Разглашение государственным служащим сведений, составляющих государственную и иную охраняемую законом тайну (банковскую тайну), является (наряду с уголовно-правовыми последствиями) основанием для расторжения служебного контракта по инициативе представителя нанимателя (ст. 37 о государственной службе).

Криминалистическая характеристика субъектов разглашения банковской тайны

С позиций криминалистики субъекты разглашения банковской тайны представляют собой четыре основных группы, в которые входят:

а) лица, состоящие в трудовых отношения с банком (работники банков) и обладающие конфиденциальными сведениями в связи с исполнением должностных обязанностей.

В современной российской действительности широкую огласку получило появление на «черном рынке» базы данных Банка России, в которой содержатся данные о банковских операциях и счетах коммерческих организаций, в том числе об операциях самого Центробанка с апреля 2003 г. по IV квартал 2004 г. Этот факт косвенно свидетельствует об имевшем место незаконном собирании и разглашении сведений, составляющих банковскую тайну так называемыми инсайдерами — лицами из числа работников Банка России[1];

б) бывшие работники банков, которым конфиденциальные сведения были доверены ранее в связи с исполнением должностных обязанностей;

в) работники организаций контрагентов (деловых партнеров) банка, которым сведения, составляющие банковскую тайну, были доверены в порядке, установленном Гражданским кодексом РФ;

г) служащие правоохранительных, контролирующих и иных государственных организаций, получившие доступ к банковской тайне в связи с исполнением служебных обязанностей.

Незаконная передача конфиденциальной информации, поступающей в государственные органы из коммерческих структур, — явление нередкое и порой совершается не только рядовыми сотрудниками, но и руководителями ведомств. Так, в 2003 г. осуждены за разглашение коммерческой информации и получение взяток бывшие руководители (председатель и первый заместитель председателя) бывшего Госкомстата РФ. Согласно официальному сообщению, обвиняемые систематически продавали конфиденциальную информацию о конкурентах заинтересованным лицам и структурам. При обысках у преступников было изъято более 1,5 млн долл. и значительное количество ювелирных изделий[2].

В феврале 2005 г., по сообщению пресс-службы столичной прокуратуры, в Москве задержан с поличным руководитель налоговой инспекции № 29, разглашавший за взятки информацию, составлявшую коммерческую тайну.

Криминалистическая характеристика субъектов незаконного собирания сведений, составляющих банковскую тайну

Названные субъекты представлены тремя основными группами, в которые входят:

а) отечественные и зарубежные структуры, специализирующиеся на собирании конфиденциальных сведений экономического характера по заказам клиентов под прикрытием аналитической, частной детективной и иной деятельности;

б) банки-конкуренты, собирающие конфиденциальную информацию в целях недобросовестной конкуренции;

[1] *Концова М.* Тайные сделки Центробанка продаются за $100 // Утро.ru. 2005. № 143 (1904). 20 мая.

[2] Дело статистиков // Финансы России. 2003. № 3 (19). С. 50.

в) криминальные элементы, добывающие конфиденциальные сведения в целях подготовки к хищению денежных средств и иного имущества путем подделки платежных поручений, чеков, пластиковых карт и т. д.

В настоящее время добыванием конфиденциальной информации о субъектах экономической деятельности в России занимается значительное число частных структур, учрежденных под видом консалтинговых, аудиторских, издательских и прочих фирм.

Для сбора информации такие структуры, как правило, используют сеть платных осведомителей из числа действующих и бывших сотрудников интересующих их организаций, в том числе пенсионеров, а также сотрудников государственных и частных организаций, имеющих доступ к информации организации-конкурента по роду служебной деятельности.

Способы незаконного получения сведений, составляющих банковскую тайну

Незаконное собирание конфиденциальной информации экономического характера, как правило, осуществляется на профессиональной основе с использованием традиционного набора шпионских методов и средств, применяемых во всем мире. Большую изобретательность в этой сфере проявляют некоторые частные российские организации, занимающиеся коммерческим шпионажем под прикрытием различных форм легальной деятельности.

Как правило, такие организации укомплектованы бывшими сотрудниками спецслужб и правоохранительных органов, имеющими опыт оперативно-розыскной, контрразведывательной и разведывательной деятельности. Некоторые из этих организаций, действуя под прикрытием легального бизнеса, специализируются на незаконной деятельности в виде выполнения заказов по слежке, перехвату линий связи, подслушиванию, используют в этих целях специальные технические средства.

Различаются два основных способа незаконного получения сведений, составляющих коммерческую тайну:

1) получение сведений путем завладения документом (или иным носителем информации);

2) получение сведений без завладения документом.

Первый способ включает в себя:

а) похищение документов, находящихся во владении лица, ответственного за их сохранность (в том числе «заказные похищения» с участием специально внедренных «кротов» (агентов) либо представителей криминальных структур);

б) завладение документами, вышедшими из законного владения в результате их утраты и находящимися без охраны.

Вторым способом охватывается:

а) получение сведений в устной форме от осведомленных о них лиц;

б) получение неучтенных копий документов (изготовленных путем ксерокопирования, сканирования, копирования магнитных носителей), которые не являются документом в правовом смысле слова;

в) получение сведений в результате перехвата информации, циркулирующей в технических средствах, помещениях, средствах транспорта.

Как правило, для незаконного получения информации применяются:

- подкуп (либо угрозы) работников организации, имеющих доступ к документам, содержащим коммерческую тайну;
- склонение к разглашению коммерческой тайны сотрудников организации, имеющих доступ к конфиденциальным сведениям, а также сотрудников, сменивших место работы, и пенсионеров, имевших доступ к закрытой информации (с использованием подкупа, угроз либо на основе этнической, религиозной или расовой близости);
- внедрение «кротов» (агентов) на должности, позволяющие получить непосредственный доступ к сведениям и документам, содержащим банковскую тайну, либо скрытно собирать конфиденциальную информацию в процессе служебной (производственной) деятельности;
- перехват информации, циркулирующей в технических средствах и помещениях (служебных, жилых и иных);
- несанкционированный доступ к сведениям, содержащимся в средствах вычислительной техники и электронных банках данных.

Среднестатистический ущерб от преступлений в кредитно-финансовой сфере США, совершенных с использованием информационных технологий, более чем в 60 раз превышает урон, нанесенный обычным ограблением банка[1].

Особым приемом незаконного получения сведений, составляющих банковскую тайну, без завладения документом является так называемый разведывательный опрос. Его суть заключается в замаскированном выведывании информации у осведомленных лиц, которые разглашают конфиденциальную тайну, не осознавая этого. Вследствие трудностей, возникающих при доказывании субъективной стороны подобных деяний, лица, собирающие информацию, как правило остаются безнаказанными.

Обобщение практики правоохранительных органов и подразделений безопасности банков свидетельствует о том, что правонарушители активно используют все перечисленные выше способы незаконного получения конфиденциальной информации, как в целях недобросовестной конкуренции, так и для подготовки хищений денежных средств и иного имущества. Факты перехвата информации с применением технических средств (подсматривание номера набираемого кода с использованием микровидеокамер и других специальных приспособлений, подслушивание без применения технических средств, выведывание информации путем замаскированного опроса владельца

[1] *Казакевич О.* Некоторые проблемы информационной безопасности банковского сообщества // Вестник АРБ. 2003. № 19. С. 63.

либо других осведомленных лиц, вовлечение в незаконное получение сведений работников банков и организаций, имеющих непосредственный доступ к сети и базам данных) подробно описаны в предыдущих главах.

В ноябре 2007 г. закончено расследование уголовного дела по обвинению главного специалиста дирекции информационных технологий Московского филиала ОАО «АКБ «Р» Е. в совершении преступления, предусмотренного ч. 2 ст. 272 УК РФ (неправомерный доступ к компьютерной информации), ч. 3. ст. 183 УК РФ (незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну) и ч. 3. ст. 159 (мошенничество, совершенное лицом с использованием своего служебного положения) УК РФ. Согласно обвинительному заключению, Е. на своем рабочем месте внедрил в компьютерную систему банка собственноручно написанную программу, скопировал часть базы данных платежных карт клиентов банка, а затем, используя полученную информацию, незаконно снял со счетов денежные средства, причинив ущерб банку на общую сумму 284 тыс. руб.[1]

Организация защиты банковской тайны

Закрытие свободного доступа к сведениям, составляющим банковскую тайну. Разработка и реализация практических мер по организации защиты банковской тайны в соответствии с действующим законодательством возлагается на ее обладателя. Именно он должен создать систему защиты сведений, составляющих банковскую тайну или конфиденциальную информацию, и обеспечить ее эффективную работу.

Цель функционирования указанной системы — обеспечить оптимальный режим работы организации с таким расчетом, чтобы сделать информацию и сведения конфиденциального характера недоступными для посторонних лиц и создать необходимые условия работы сотрудникам, имеющим к ним доступ. Для этого устанавливается единый порядок работы с защищаемой информацией. Основная особенность этого порядка заключается в организации конфиденциального делопроизводства, принятии работниками обязательства строгого исполнения его правил и индивидуальной ответственности за обеспечение сохранности доверенных конфиденциальных сведений и их носителей.

В рамках системы организуется обучение работников правилам соблюдения банковской тайны. Осуществляется систематический контроль за исполнением организационно-распорядительных документов и инструкций по защите конфиденциальной информации. Система предусматривает наличие типовой процедуры анализа и разбирательства (ведомственного расследования) по фактам нарушения порядка работы со сведениями, составляющими банковскую

[1] В суд Москвы было направлено уголовное дело в отношении сотрудника Росбанка, похитившего средства клиентов. РосБизнесКонсалтинг (Москва), 23 ноября 2007 г.

йну. и выработку предложений по совершенствованию защиты информации.

Осуществление указанных мероприятий целесообразно начать с подготовки соответствующих организационно-распорядительных и нормативных документов, наделяющих специально выделенных работников организации (далее — комиссию) правом относить информацию к числу сведений, составляющих банковскую тайну. Нормативной основой работы комиссии должно служить специально разработанное *положение о банковской тайне* (далее — положение).

Этот документ, разрабатываемый в соответствии с законодательством Российской Федерации, устанавливает порядок выявления и оценки степени конфиденциальности сведений, составляющих коммерческую тайну организации, регламентирует основные направления и механизм защиты этих сведений и утверждается руководителем организации. Поскольку содержание перечня может само по себе представлять интерес для недобросовестных конкурентов, руководитель банка вправе принять решение об отнесении указанного документа к числу конфиденциальных.

Перечень доводится до сведения сотрудников, уполномоченных относить информацию к категории «банковской тайны» (в полном объеме либо в части, их касающейся). Он изменяется и дополняется по мере целесообразности (устаревания сведений, появления новых технологических достижений и проч.).

Как правило, в перечень включаются следующие основные категории сведений, обеспечивающие организации преимущество в конкурентной борьбе.

В сфере административной:

- о руководителях подразделений банка и лицах, ответственных за реализацию ее технологических и коммерческих программ;
- о предмете и целях совещаний сотрудников органов управления банка;
- о представителях или посредниках;
- об организации труда (структуре, штатах, расстановке работников на технологических участках, способах стимулирования эффективности труда работников);
- о методике отбора и профессиональной подготовки персонала организации;
- о базах данных ЭВМ и характеристиках программного обеспечения автоматизированных участков производства;
- о планах развития предприятия и привлечении инвестиций.

В финансовой сфере:

- о размерах и условиях банковских кредитов;
- о финансовом положении организаций — клиентов банка;
- об источниках финансирования организации;
- о кредитоспособности и получении кредитов под конкретный проект, их размере и условиях;
- о вложении средств в ценные бумаги и на депозитные счета;

- о состоянии материально-технической базы организации;
- о характеристиках телекоммуникационных систем банка;
- об электронных системах накопления, обработки и передачи информации банка, их программном обеспечении и средствах защиты и т. д.

Следующим шагом в организации защиты информации должна быть *организация защиты сведений, отнесенных к коммерческой тайне*, от незаконного получения, разглашения, утраты и использования. С этой целью устанавливается ограничение доступа к носителям информации, содержащей коммерческую тайну. Оно предполагает соответствующую организацию правомерного доступа к сведениям, составляющим коммерческую тайну.

Основанием для доступа к сведениям, составляющим коммерческую тайну, является соответствующее решение обладателя названной информации (руководителя организации). Для сотрудников организации, которым доступ к коммерческой тайне необходим по характеру выполняемой ими работы, оно оформляется приказом о допуске либо иным документом произвольной формы. Из него должно ясно усматриваться, к работе с какими конкретно сведениями допускается работник, какого рода работа с информацией ему разрешается (ознакомление, хранение). Документ должен иметь подпись руководителя организации либо иного специально уполномоченного лица.

Решение о допуске принимается после ряда обязательных процедур, порядок выполнения которых целесообразно регламентировать в соответствующих распорядительных документах.

Основные мероприятия по организации правомерного доступа сотрудников к сведениям, составляющим коммерческую тайну, излагаются, как правило, в виде раздела положения. Однако в случае необходимости может быть разработана специальная инструкция, детализирующая процедуру доступа.

Оба документа могут составляться с различной степенью детализации, зависящей от специфики деятельности организации, однако ряд положений, отражающих права и обязанности сторон, возникающие в связи с допуском к коммерческой тайне, должен быть включен в нее непременно.

В них устанавливается механизм реализации норм конституционного права, гражданского, трудового и иного законодательства в процессе защиты коммерческой тайны.

Они учитываются сторонами при заключении трудовых договоров и контрактов. Их нарушение может служить основанием для наложения дисциплинарных взысканий на работника либо предъявления судебных исков одной из сторон.

В частности, инструкция должна содержать указания на то, что допуск граждан к коммерческой тайне осуществляется в добровольном порядке и предусматривает:

- принятие на себя обязательств о нераспространении доверенных им сведений, составляющих коммерческую тайну;

- согласие на частичные временные ограничения их прав в соответствии с условиями трудового договора;
- письменное согласие на проведение в отношении них проверочных мероприятий соответствующими службами организации либо иной частной коммерческой службой по договору с организацией (выяснение биографических и других характеризующих личность данных в пределах, установленных ст. 3 Закона о частной детективной деятельности);
- обязательство гражданина представлять кадровому аппарату сведения о возникновении оснований для отказа к допуску к коммерческой тайне;
- определение видов, размеров и порядка предоставления льгот в качестве компенсации за исполнение указанных выше обязательств и ограничения прав (взаимные обязательства организации и лица, получающего допуск, фиксируются в трудовом договоре (контракте)).

Инструкция должна содержать исчерпывающий перечень оснований для отказа гражданину в допуске к коммерческой тайне:

- признание его судом недееспособным, ограниченно дееспособным, нахождение его под судом и следствием за тяжкие и особо тяжкие преступления, наличие у него не снятой судимости за преступления;
- наличие медицинских противопоказаний для работы с использованием сведений, составляющих коммерческую тайну;
- выявление в результате проверочных мероприятий таких данных, которые свидетельствуют о деятельности оформляемого лица или обстоятельствах, создающих угрозу разглашения сведений, составляющих коммерческую тайну;
- уклонение от проверочных мероприятий и (или) сообщение заведомо ложных анкетных данных.

В инструкцию следует включить указание на то, что допуск к коммерческой тайне может быть прекращен по решению руководителя организации в случае:

- нарушения предусмотренных трудовым договором (контрактом) обязательств гражданина, связанных с сохранением коммерческой тайны;
- возникновения обстоятельств, являющихся основанием для отказа гражданину в допуске к коммерческой тайне.

Следует отметить также, что прекращение допуска гражданина к коммерческой тайне может стать основанием для расторжения трудового договора (контракта) с ним, если такое условие предусмотрено в этом договоре (контракте). Прекращение допуска гражданина к информации не освобождает его от взятых обязательств по неразглашению сведений, составляющих коммерческую тайну.

Вместе с тем решение руководителя организации о прекращении допуска гражданина к коммерческой тайне и расторжении на основании этого трудового договора (контракта) с ним может быть обжаловано в суде.

Кроме того, в положение целесообразно включить разделы, посвященные организации работы с конфиденциальными сведениями; участию сотрудников в защите сведений, составляющих коммерческую тайну; основам деятельности подразделения защиты информации.

Важным звеном системы защиты информации является *организация конфиденциального делопроизводства* — особого порядка обращения со сведениями и документами, в которых она содержится. Защищенность информации при работе с нею обеспечивается соблюдением требований инструкции об организации конфиденциального делопроизводства, которая разрабатывается в развитие соответствующего раздела положения о защите коммерческой тайны.

Нормы инструкции должны предусмотреть необходимые способы технологической и физической защиты носителей информации независимо от их вида (письменная, графическая, электронная, память человека) на всех стадиях работы. Устанавливается единый порядок работы со всеми видами носителей конфиденциальной информации.

Вводится личная ответственность работников за защиту информации на всех этапах работы. Устанавливается единый порядок доступа к носителям информации всех категорий сотрудников, получивших право работать с ними.

Предписывается строгий контроль за соответствием выдаваемой в пользование информации с видом и объемом полномочий субъекта. Ведется обязательный учет всех фактов разрешенного доступа к информации (носителю), а также попыток неправомерного завладения информацией.

Инструкция должна детально регламентировать порядок подготовки, регистрации, приема и передачи, пересылки и доставки конфиденциальных документов, контроля за их прохождением. Ею устанавливаются режим хранения конфиденциальных документов, порядок их уничтожения, а также проверки их наличия.

Значительная часть предписаний инструкции имеет своей целью предупредить действия ответственного лица (неосторожные либо умышленные), которые могут повлечь выход документов из законного владения.

К их числу относятся, в частности, предписания, обязывающие принимать и передавать документы под расписку, держать их в хранилищах (сейфах), а ключи от хранилищ — у дежурного либо непосредственно у ответственного лица, в условиях, исключающих их использование посторонними.

Кроме того, в инструкцию следует включить необходимый перечень требований по обеспечению защиты помещений, выделенных для хранения и обработки конфиденциальных материалов. Минимально необходимыми мерами предосторожности являются:

- установка электроконтактных или магнитных датчиков охранной сигнализации на двери и окнах;
- выдача ключей от помещений и хранилищ только лицам, ответственным за это помещение;

- установка и замена оборудования и мебели только по согласованию с подразделением по защите информации предприятия, а уборка — в присутствии ответственного лица или лица, его замещающего;
- проведение ремонта помещений под наблюдением лица, назначенного по согласованию с подразделением по защите информации.

Принципиальным требованием правил конфиденциального делопроизводства является *установление персональной ответственности лиц, работающих материалами, за сохранность доверенных им документов и сведений.*

В этой связи лицо, допущенное к сведениям, составляющим коммерческую тайну, должно принять на себя ряд определенных обязательств и ограничений, связанных с будущей деятельностью.

К ним относятся: обязательство нести персональную ответственность за сохранность доверенных конфиденциальных сведений, твердо и неукоснительно выполнять правила конфиденциального делопроизводства, обеспечивать надежное хранение конфиденциальных документов, незамедлительно сообщать уполномоченным лицам об утрате конфиденциальных документов, ключей от их хранилищ, личных печатей, а также о признаках утечки конфиденциальных сведений и давать устные и письменные пояснения по фактам нарушения правил обращения с конфиденциальными документами.

В число ограничений входят запреты на совершение определенных действий, которые могут повлечь утрату документов или разглашение конфиденциальных сведений (передачу содержания конфиденциальных сведений посторонним, вынос документов из рабочего помещения без производственной необходимости и оставление их в неохраняемых местах, уничтожение документов с нарушением установленного порядка и проч.).

Кроме того, при проведении разбирательств по фактам нарушения инструкции об организации конфиденциального делопроизводства сотрудники организации обязаны давать письменные объяснения об известных им обстоятельствах.

Несмотря на то что перечень указанных выше обязательств и ограничений (запретов), как правило, содержится в инструкции по организации конфиденциального делопроизводства, и работники знакомятся с ними под расписку, факт принятия этих условий конкретным лицом оформляется в виде договоров, предусмотренных гражданским законодательством либо законодательством о труде.

Сотрудник организации, не принявший указанных обязательств, правовой ответственности за нарушение порядка обращения с конфиденциальными материалами не несет.

Особенности организации защиты информации, составляющей коммерческую тайну, от утечки по техническим каналам. Главной задачей этой деятельности является создание системы защиты конфиденциальной информации, циркулирующей в технических средствах и помещениях, от утечки и умышленного перехвата с противоправными целями. Такая система должна состоять из двух

блоков: технического и функционального. В рамках первого ведется разработка и внедрение технических средств зашиты информации, циркулирующей в средствах техники и связи.

С указанной целью технической защитой обеспечиваются:

- помещения, предназначенные для ведения конфиденциальных переговоров;
- средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники), средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства), средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео-смысловой и буквенно-цифровой информации, программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации;
- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где обрабатывается (циркулирует) конфиденциальная информация, чтобы предупредить незаконное получение конфиденциальной информации путем перехвата акустического, электрического, электромагнитного, вибрационного и других видов излучений, возникающих при обработке информации техническими средствами), а также радиоизлучений или электрических сигналов от внедренных в технические средства и помещения специальных электронных устройств перехвата информации («закладок») и от устройств перехвата информации, подключенных к каналам связи, а также к отдельным носителям информации.

Кроме того, технические средства защиты информации от утечки должны препятствовать непреднамеренному попаданию конфиденциальных сведений к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны. Например, вследствие прослушивания разговоров, ведущихся в выделенном помещении, из-за недостаточной звукоизоляции стен, систем вентиляции и кондиционирования воздуха; случайного прослушивания телефонных переговоров при проведении профилактических работ на АТС; просмотра информации с экранов дисплеев и других средств ее отображения через двери и окна.

Решение технических задач возлагается на подразделения (либо отдельных специалистов) разработки технических средств защиты информации.

Второй важной задачей создания системы защиты информации является организация функционирования указанных выше технических и программных средств в определенном режиме. Ее решение требует принятия пакета организационно-распорядительных и рабочих документов.

В частности, издания приказов о создании соответствующих подразделений по защите информации и назначении лиц, ответственных за эксплуатацию технологического оборудования и электронных банков данных.

Созданные подразделения, в свою очередь, готовят совместно с разработчиками средств технической защиты инструкции с описанием требований по защите информации, которые должны выполнять в процессе обработки (передачи) информации лица, ответственные за эксплуатацию технологического оборудования и электронных баз данных, пользователи конфиденциальной информации и сотрудники подразделений по защите информации.

Программа обеспечения функционирования системы защиты конфиденциальной информации должна включать в себя выполнение специальной проверки технических средств и служебных помещений на предмет отсутствия в них возможно внедренных электронных устройств перехвата информации («закладок»); организацию охраны и физической защиты объекта информатизации и отдельных технических средств, исключающих несанкционированный доступ к ним, а также контроль состояния и эффективности зашиты информации.

С целью предупреждения внедрения «закладок» в технические средства и интерьер, подразделение по защите информации составляет технический паспорт на каждое защищаемое помещение. Этот документ должен содержать план размещения оборудования и схему его кабельных соединений.

В паспорт включается перечень оборудования и мебели, установленных в помещении, с указанием типа, учетного или инвентарного номера и даты установки и замены. Кроме того, в нем отражаются перечень реализованных мероприятий по защите информации, даты и результаты периодических проверок системы защиты.

Детальные описания порядка осуществления работ, основные требования и рекомендации, способы и средства защиты информации, циркулирующей в технических средствах и помещениях, изложены в документе под названием «Специальные требования и рекомендации по технической защите конфиденциальной информации» (Гостехкомиссия России, 2001 г.).

Задача обеспечения защиты информации от утечки по техническим каналам, как и во всех иных указанных выше случаях, возлагается на руководителей организации и подразделений, которые разрабатывают и эксплуатируют объекты информатизации, организуют и осуществляют защиту информации (службы безопасности).

Однако в случае необходимости руководитель организации может прибегнуть на договорной основе для разработки средств защиты информации и осуществления мероприятий по ее защите специализированные учреждения предприятия, имеющие лицензию Гостехкомиссии России или ФАПСИ на право осуществления указанных видов деятельности. Контроль за соблюдением правил эксплуатации системы защиты информации, ее состоянием

эффективностью защиты информации осуществляется подразделениями защите информации предприятия-заказчика.

7.4. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка

Исходным условием защиты компьютерной информации банка является аво собственности на нее, полученное на основаниях, предусмотренных за-ном: в результате прямого участия в создании информационного продукта тдельных документов и их совокупности) или приобретения его иными спо-бами, не противоречащими действующему законодательству Российской едерации. Собственник информационных ресурсов пользуется всеми права-и, предусмотренными законодательством Российской Федерации, в том чис-е (на основании ст. 16 Закона об информации) имеет право устанавливать пределах своей компетенции режим и правила обработки и защиты информационных ресурсов, а также доступа к ним.

С другой стороны, наличие такого режима и правил, закрытие собственником свободного доступа к информации на законном основании и выполнение ер по ее охране является обязательным условием для отнесения информационных ресурсов к категории объектов, охраняемых уголовным законом. Порядок защиты информационных ресурсов и информационных систем банк устанавливает самостоятельно, применяя для этого в пределах собственной компетенции меры организационного, нормативного и технического характера. евыполнение этих мер лишает информацию защиты способами, предусмотренными законодательством.

Преступления в сфере компьютерной информации являются одним из наиболее опасных видов угроз информационной безопасности банка. Задачи их выявления, предупреждения и пресечения тесно переплетаются с проблемами обеспечения защиты конфиденциальной информации банка. Это объясняется тем, что сведения, составляющие банковскую, коммерческую и служебную тайну, хранятся не только на бумажных носителях, но и в компьютерных базах данных, либо на отдельных носителях компьютерной информации.

Когда преступники посягают на конфиденциальную информацию банка с целью неправомерного завладения сведениями, находящимися в ЭВМ, их объекты противоправных посягательств (отношения по поводу защиты конфиденциальной информации и отношения в сфере защиты компьютерной информации) частично совпадают и взаимно дополняют друг друга. Определенный вред конфиденциальной информации способны причинить и другие формы незаконного вмешательства в информационные ресурсы и информационные системы, посягающие на безопасность самих компьютерных систем их программного обеспечения.

По конечным целям, которые преследуют преступные посягательства в сфере компьютерной информации банка, их можно условно объединить в два

основных вида. Цель первая — завладение имуществом банка путем воздействия на информацию. Мотивы деяний — корысть. Цель вторая — причинение ущерба банку путем разрушения его инфраструктуры и нарушения порядка управления деятельностью банка. Мотивы деяний — корысть (устранение конкурента), месть, хулиганские мотивы. Все виды преступных посягательств в сфере компьютерной информации совершаются с прямым умыслом. Мотивы «случайных» проникновений в защищенную информационную систему банка (любопытство, самоутверждение и т. д.) нами в данной работе не рассматриваются из-за их «непрофильности» и малочисленности. Хотя в отдельных случаях эти действия могут повлечь определенный ущерб.

Основными целями защиты информационных ресурсов и информационных систем банка являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности; сохранение конфиденциальности документированной информации в соответствии с законодательством.

Уголовно-правовая ответственность за преступные посягательства на отношения в сфере компьютерной информации установлена ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ» и ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» УК РФ.

Неправомерный доступ к компьютерной информации. Статья защищает права собственника (обладателя) компьютерной системы на неприкосновенность находящейся в ней информации.

Указанная норма устанавливает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, т. е. информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Под блокированием в данном случае принято понимать невозможность доступа к информации со стороны законного пользователя. Модификация представляет собой внесение изменений, искажающих содержание информации вопреки интересам ее законного пользователя. Копирование заключается в незаконном воспроизведении оригинала с целью его получения незаконным пользователем.

С точки зрения закона неправомерным признается доступ к закрытому информационному массиву постороннего, т. е. лица, не являющегося законным пользователем и не имеющего разрешения собственника на ознакомление с данными, содержащимися на машинных носителях или в ЭВМ.

Способы неправомерного доступа к охраняемой законом компьютерной информации. Для осуществления неправомерного доступа к охраняемой компьютерной информации правонарушителям приходится преодолевать технические и программные меры зашиты. С этой целью они используют похищенные программные и аппаратные ключи и средства криптографической защиты, получая таким образом доступ к ЭВМ от имени других лиц; внедряют в объект информатизации программные или технические средства, позволяющие обойти средства защиты и получить возможность копирования информации или несанкционированной работы в информационном массиве; перехватывают информацию из средств вычислительной техники, пользуясь радиоэлектронными средствами; подключают аппаратуру записи с каналам связи; похищают накопители памяти ЭВМ, в которых хранится информация, магнитные или бумажные носители информации.

В качестве примера неправомерного доступа к компьютерной информации банка может служить факт разработки и внедрения в информационную систему ГРКЦ ГУ ЦБ РФ по Москве в 1993 г. специально разработанной программы с целью хищения денежных средств. Названная программа открыла технологический счет, имеющий первоначально нулевой остаток. Затем преступники осуществили несанкционированное «дописывание» документов в массив «операционного дня» в пользу 8 коммерческих банков Москвы на сумму 68 млрд руб.

Под проведенную электронную проводку дополнительно в ГРКЦ были внедрены для дальнейшей обработки и рассылки по банкам носители — фальшивые платежные поручения[1].

О неправомерном доступе в компьютерную информационную систему банка с целью завладения конфиденциальной информацией сообщила 30 марта 2000 г. пресс-служба ГУВД Москвы. К уголовной ответственности привлечен 20-летний житель Москвы, который, «взломав» защиту компьютерной информационной системы одного из банков с помощью программы-вируса, получил информацию о 20 тыс. клиентов, владельцев пластиковых карт этого банка. В дальнейшем он потребовал у руководителей банка 20 тыс. долл., угрожая в противном случае предать огласке добытые им сведения[2].

Обязательным элементом преступления, предусмотренного ст. 272 УК РФ, является наступление вредных последствий (уничтожение, модификация, блокирование и копирование информации, а также нарушение работы ЭВМ, системы ЭВМ или их сети).

Субъектом преступления является лицо, достигшее 16-ти лет, в том числе и законный пользователь компьютерной сети, не имеющий допуска к работе с информацией определенной категории.

[1] *Мельников Ю. Н.* Информационная безопасность в банке: Проблемы и рекомендации // Банковская технология. 1997. № 7.

[2] Независимая газета. 2000. 30 марта.

Максимальное наказание за совершение преступления, предусмотренного ч. 1 ст. 272 УК РФ, — лишение свободы на срок до двух лет.

Совершение указанных выше деяний группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющего доступ к ЭВМ, системе ЭВМ или их сети является (в соответствии с ч. 2 ст. 272 УК РФ) отягчающим обстоятельством.

Указанные действия могут повлечь максимальное наказание в виде лишения свободы на срок до пяти лет.

Создание, использование и распространение вредоносных программ для ЭВМ. Нормы, установленные ст. 273 УК РФ, защищают права собственника (обладателя) компьютерной системы на неприкосновенность порядка ее функционирования и сохранности находящейся в ней информации.

Действия преступника заключаются в создании программ для ЭВМ или внесении изменений в существующие программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; в использовании названных программ; в распространении таких программ или машинных носителей с такими программами.

Программа для ЭВМ представляет собой упорядоченную последовательность команд, предназначенных для управления конкретными компонентами системы обработки данных. Совокупность программ и документации к ним образует программное обеспечение (математическое обеспечение).

Под вредоносными программами, в смысле ст. 273 УК РФ, подразумеваются программы-вирусы, способные внедряться в другие программы, копировать их (размножаться), а также выполнять другие задания, приводящие к последствиям, перечисленным в диспозиции ст. 273 УК РФ[1].

Опасность вредоносной программы-вируса заключается в возможности полного или частичного вывода из строя информационных ресурсов и информационных систем, нарушения порядка функционирования банка (и других организаций).

Специалисты в области защиты компьютерной информации различают несколько основных видов вредоносных программ-вирусов. К последним относятся программы: сканирования системы защиты объекта посягательства и содержимого памяти ЭВМ; подборщики паролей и генераторы номеров кредитных карт; «логические бомбы», срабатывающие в определенных условиях и разрушающие частично или полностью компьютерную систему, «троянские кони», уничтожающие компьютерные программы и распространяющиеся по коммуникационным сетям. Число программ-вирусов и география их противоправного применения непрерывно растет. Об этом свидетельствуют

[1] *Файтс Ф., Джонстон П., Кратц М.* Компьютерный вирус: Проблемы и прогноз / пер. с англ. М.: Мир, 1994. С. 33.

публикации в специальных изданиях и сообщения «хакеров» — взломщиков защиты компьютерных сетей, помещаемые ими в Интернете.

Об использовании вредоносной программы-вируса с целью хищения денежных средств инженером Миллеровского отделения Сбербанка Ростовской области Н. сообщило ГУВД Ростовской области. Злоумышленник ввел в программно-технический комплекс банка программу-вирус «троянский конь», в результате действия которой в ряде филиалов были созданы 23 фальшивых счета. На эти счета было перечислено 885 тыс. руб.

Наказуемым, согласно ст. 273 УК РФ, является сам факт создания программ-вирусов или внесения изменений в нормальное функционирование существующих программ, заведомо приводящих к указанным негативным последствиям (вне зависимости от реального наступления последних)[1].

По смыслу статьи, программы-вирусы создаются именно как вредоносные. Поэтому не является наказуемым факт создания программы — вируса вследствие ошибки. Также не влечет ответственности умышленное создание программы-вируса для последующей разработки способов антивирусной защиты.

Под использованием вредоносных программ-вирусов принято понимать их внедрение в программное обеспечение ЭВМ, записи на материальный носитель (в том числе на бумажный), распространение по сетям, передачу другим лицам и другие действия по их введению в оборот с целью наступления вредных последствий, предусмотренных ст. 273 УК РФ.

Распространением программы-вируса признается ознакомление с ней других лиц либо передача им программы в любой материальной форме (магнитной записи, записи на бумажном носителе и т. п.).

Преступление, предусмотренное частью 1 ст. 273 УК РФ, может быть совершено только умышленно. Максимальное наказание за совершение деяния, предусмотренного ч. 1 ст. 273 УК РФ, — лишение свободы до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

Часть 2 ст. 273 УК РФ предусматривает наличие в деянии отягчающего (квалифицирующего) признака в виде наступления тяжких последствий по неосторожности. Это означает, что виновный должен сознавать, что создает вредоносную программу, использует либо распространяет такую программу или ее носители. При этом он предвидит возможность наступления тяжких последствий, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение либо не предвидит этих последствий, хотя должен их предвидеть. К тяжким последствиям можно отнести ущерб в виде хищения

[1] Нормальное функционирование «штатной» программы означает выполнение ею операций, указанных в документации на ее разработку.

денежных средств банка, уничтожения его баз данных, дезорганизации работы банка и упущенную в связи с этим выгоду и т. п.[1]

По этой части суд может назначить максимальное наказание до семи лет лишения свободы.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Статья 274 УК РФ устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.

Статья защищает права собственника (обладателя) компьютерной системы и безопасность ее функционирования, которая обеспечивается соблюдением правил эксплуатации системы.

Правила эксплуатации информационной системы устанавливаются ее собственником (владельцем) в виде соответствующего положения, инструкции, регламента и объявляются приказом, с которым в обязательном порядке должны быть ознакомлены все лица, имеющие доступ к ЭВМ, системе ЭВМ или их сети. Статья 274 УК РФ призвана обеспечить защиту локальных информационных систем и распространяется только на сотрудников, имеющих к ним разрешенный доступ.

Охраняемая законом информация ЭВМ представляет собой информацию, в отношении которой установлен специальный режим ее правовой защиты.

Обязательным условием наступления уголовной ответственности по ст. 274 УК РФ должно быть наличие причинной связи между допущенным нарушением правил эксплуатации и наступившим существенным вредом.

Понятие существенного вреда применительно к данной статье является оценочным. Степень нанесенного ущерба оценивается судом в каждом конкретном случае.

Виновным в нарушении правил эксплуатации по смыслу ст. 274 УК РФ может быть признано только лицо, имеющее официальный доступ к компьютерной системе, обязанное соблюдать установленные правила ее эксплуатации и достигшее 16-ти лет.

Данное преступление может совершаться как умышленно, так и по неосторожности.

[1] Иллюстрацией наступления возможных тяжких последствий вследствие применения вредоносной программы-вируса может служить сообщение, которое сделала 3 июля 2000 года генеральный инспектор НАСА Roberta Gross в интервью программе «Панорама» телекомпании ВВС. По ее словам, в 1997 г. из-за действий неустановленного хакера под угрозой оказались жизни астронавтов на корабле «Шаттл», летевшем к российской космической станции «Мир». В результате неких манипуляций хакеру удалось вызвать перегрузку информационной системы, которая непрерывно передает информацию о состоянии здоровья космонавтов, что в итоге могло сказаться на функционировании всей системы связи с космическим кораблем. К счастью, операторам удалось быстро переключить связь на резервную систему.

Максимальное наказание за совершение деяния, предусмотренного ч. 1 ст. 274 УК РФ, — ограничение свободы на срок до двух лет.

Часть 2 ст. 274 УК РФ предусматривает наличие в деянии отягчающего (квалифицирующего) признака в виде наступления тяжких последствий по неосторожности, т. е. виновный должен предвидеть возможность наступления тяжких последствий, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение либо не предвидит этих последствий, хотя при необходимой внимательности и предусмотрительности должен и мог их предвидеть.

Максимальное наказание за совершение деяния, предусмотренного ч. 2 ст. 274 УК РФ, — лишение свободы на срок до четырех лет.

Среди субъектов, совершающих противоправные посягательства на компьютерную информацию банка, следует выделить:

1. Лиц, совершающих преступления с целью завладения денежными средствами или имуществом банка. Такие лица могут действовать в одиночку, однако чаще всего они объединяются в группы, численность которых доходит до 10–15 человек. Кроме специалистов в области компьютерной техники, такие группы включают в себя лиц, хорошо знакомых с банковским делом. Это объясняется тем, что для перевода денег из банка недостаточно проникнуть в его компьютерную систему. Необходимо также досконально знать детали специфических банковских технологий. Отражением процесса коммерциализации преступлений в компьютерной сфере стало также появление в Интернете предложений о продаже сведений, составляющих банковскую тайну, в первую очередь информации о владельцах банковских счетов и пластиковых картах.

2. Лиц, добывающих конфиденциальную компьютерную информацию или дезорганизующих работу компьютерных сетей банка по заказу конкурентов.

3. Взломщиков (хакеров) — любителей, проникающих в защищаемые компьютерные системы из интереса, с целью самоутверждения и т. п., в том числе для разрушения компьютерных систем из хулиганских и других корыстных побуждений.

4. Лиц с психическими аномалиями.

По отношению к объекту посягательства указанные лица могут быть посторонними, сотрудниками банка либо сотрудниками организации-партнера подрядчика), в том числе представители технического персонала компьютерной системы или сети, разработчики системы и их руководители, операторы, рограммисты, инженеры связи, специалисты по защите информации и другие.

Как показывает мировой опыт, около 90% злоупотреблений в финансовой ере, связанных с нарушениями в области информационной безопасности, юисходит при прямом или косвенном участии действующих или бывших ботников банков. При этом на преступный путь часто становятся самые

валифицированные, обладающие максимальными правами в автоматизированных системах, категории банковских служащих — системные администраторы и другие сотрудники служб автоматизации банков. Достаточно напомнить упоминавшееся дело бывшего начальника службы информационной безопасности процессинговой компании Union Card в России Андрея Голова, незаконно собиравшего и передававшего сообщникам по преступной деятельности информацию о счетах, вкладах, номерах, персональных кодах пластиковых карт для хищений денежных средств со счетов их владельцев.

Целями противоправных посягательств в сфере компьютерной информации банка обычно являются:

1. Незаконное завладение деньгами банка.
2. Незаконный сбор информации в интересах организации-конкурента.
3. Незаконный сбор информации с целью ее последующего сбыта.
4. Разрушение информационных систем банка-конкурента с целью его удаления с рынка услуг либо ограничения его деятельности. Иногда эти задачи объединяются. Отечественной правоохранительной практике известен случай выполнения хакером заказа одной фирмы, в результате чего была скопирована определенная информация, а затем нанесен ущерб системе ЭВМ конкурента (уничтожен web-сайт и вся информация на сервере).
5. Разрушения информационных систем банка из мести, совершаемые его работниками или бывшими работниками.
6. «Взлом» web-сайта с целью подмены подлинной информации и размещения сведений, порочащих деловую репутацию конкурента.

Способы совершения преступлений в сфере компьютерной информации. С позиций криминалистической характеристики способы совершения преступлений, предусмотренные ст. 272, 273 и 274 УК РФ, тесно связаны между собой и взаимодополняют друг друга. Такая ситуация объясняется в определенной мере искусственным разграничением названных выше составов на уголовно-правовом уровне. Так, нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети в определенных случаях может рассматриваться как частный случай неправомерного доступа к компьютерной информации. А создание, использование и распространение вредоносных программ для ЭВМ может быть составной частью обоих названных выше составов.

Ведущими во всех составах преступлений в сфере компьютерной информации с точки зрения криминалистической характеристики являются способы неправомерного доступа к компьютерной информации. В их числе наибольшее распространение получили:

- использование для получения доступа к компьютерной информации чужого имени (путем применения кодов и паролей законных пользователей);
- внедрение в объект информатизации программных или технических средств, позволяющих обойти средства защиты и получить возможность

копирования информации или несанкционированной работы в информационном массиве;

- изменение адреса получателя доступа к сети (или информации) путем внедрения программы-вируса или неправомерного аппаратного воздействия. В результате указанных действий нарушается нормальное управление потоком информации (маршрут передачи информации), и фактический доступ к сети под видом законного пользователя получает постороннее лицо;
- перехват информации из средств вычислительной техники с использованием радиоэлектронных способов;
- подключение аппаратуры записи с каналам связи;
- похищение накопителей памяти ЭВМ, в которых хранится информация;
- похищение магнитных или бумажных носителей информации.

Посягательства на компьютерную информацию по месту совершения дифференцируются:

- на внешнее, которое осуществляется с компьютеров, не входящих в структуру сети банка;
- на внутрисетевое, которое совершается с использованием компьютеров, входящих в банковскую сеть.

Подготовительные действия к совершению указанных преступлений условно могут быть разделены на два основных вида направленные на преодоление мер защиты ЭВМ (системы ЭВМ) программно-аппаратным методом и на достижение указанной цели путем незаконного использования информации, доверенной сотрудникам организации — объекта посягательства, либо полномочий указанных сотрудников. Это разграничение однако не является абсолютным. Оба вида подготовки могут объединяться и дополнять друг друга полностью либо частично.

К числу подготовительных действий *первого вида* следует отнести:

- *виртуальную разведку с целью выявления уязвимых мест («люка», обеспечивающего вставку в программу дополнительно одной или нескольких программ-вирусов) в защите объекта посягательства.*

Для выявления уязвимых мест защиты объекта посягательства определяют-я: адресное пространство сети, в которой расположен объект удаленного воз-ействия; активные сетевые устройства ЭВМ; открытые порты и службы ЭВМ; тип операционной системы, используемой сетевым устройством.

Определенную часть сведений о компьютере потерпевшего злоумышленник собирает из открытых источников, в число которых входят: web-страница организации (адреса и место расположения офисов; номера телефонов; адреса электронной почты; список деловых партнеров; ссылки на другие web-узлы, имеющие отношение к организации); информация из архивов групп новостей и списков рассылки; информация об администраторе сети и проч. Затем, используя специальные программы и протоколы (они распространяются,

частности через Интернет и специальные журналы), преступник узнает адреса компьютеров интересующей его организации, устанавливает адресное пространство сети, выявляет работающие компьютеры, осуществляет сканирование портов — процесс пробного подключения к портам исследуемого компьютера, проводит сбор маркеров (подключение к различным портам компьютера потерпевшего) с использованием специальных утилит.

В результате описанных действий злоумышленник получает необходимую информацию о схеме расположения сетевых устройств, их адресах, открытых портах, используемых операционных системах, особенностях взаимодействия работы, Кроме того, используя анализатор пакетов (передающейся по сети информации) он может перехватить сведения о паролях и логинах доступа интересующей его ЭВМ[1]:

- *проверку результативности (испытание) программы-вируса на других похожих системах по договору с их администраторами (испытывать на реальном объекте бывает опасно ввиду сложности сокрытия следов);*
- *внедрение программ-закладок в систему жертвы через системы коммуникации либо с участием сотрудников объекта посягательства. Лица, имеющие официальный доступ к компьютерной системе объекта, могут внедрить программу-вирус в защищаемый объект умышленно. Однако во многих случаях они используются «втемную». Нарушая правила эксплуатации ЭВМ, указанные лица вносят в компьютер замаскированную программу-вирус при использовании «новой компьютерной игры» или «демонстрационной программы», врученных им злоумышленниками под благовидным предлогом.*

Подготовительные действия *второго вида* заключаются в противоправном воздействии на сотрудников банка (в том числе бывших), имеющих официальный доступ к работе в информационной системе с целью:

- получения информации о технологии электронных банковских операций, о способах защиты компьютерной сети, паролях, кодах (применяются выведывание, подкуп, угрозы, а также другие незаконные приемы);
- неправомерного завладения программными ключами, аппаратными ключами, средствами криптографической защиты.

Наиболее распространенные способы маскировки действий злоумышленников при неправомерном доступе к компьютерной информации носят нередко изощренный характер и призваны:

а) направить поиск виновного по ложному пути. В этих целях используются входы на компьютеры других пользователей, в том числе в других странах, через которые осуществляется посягательство. Программы-«взломщики» компьютерной защиты сначала внедряются без ведома владельцев в сервер

[1] *Милашев В. А.* Проблемы поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ. Дис. ... канд. юрид. наук. М., 2004. С. 58.

третьей организации (нередко находящийся за рубежом), который по заданному алгоритму периодически посылает зараженные вирусом документы по адресу потерпевшего;

б) исключить либо затруднить своевременное обнаружение преступления или преступника. Для соединения с ЭВМ жертвы используются: телефон, номер которого не определяется; квартира с телефоном, снятая на имя подставного лица; подключение компьютера непосредственно к парам в распределительной телефонной коробке. При наличии возможности правонарушители уничтожают следы своего пребывания в информационной системе объекта посягательства с использованием специальных программ.

Наиболее распространенными видами следов противоправных посягательств в сфере компьютерной информации являются нижеперечисленные.

1. Зарегистрированные ЭВМ признаки команд, имеющих целью копирование, модификацию или уничтожение информации.

Следы указанных действий (команд) правонарушителя остаются в виде учетных записей в файлах, формируемых активным сетевым оборудованием корпоративной информационной сети, которые затем собираются в базе данных службы защиты информации (далее — СЗИ).

Именно здесь администратор локальной сети (сотрудник СЗИ) организации, как правило, обнаруживает отдельные (первичные) признаки неправомерного воздействия на компьютерную информацию.

Носителями указанной следовой информации в типичной компьютерной сети организации (предприятия) являются:

- маршрутизатор сегментов локальной вычислительной сети (ЛВС);
- пограничный маршрутизатор (межсетевой экран) для выхода в Интернет либо заменяющий его proxy-сервер;
- файловый сервер (вместе с контроллером домена, при его наличии), в котором хранятся сетевые папки сотрудников, расширенные папки с файлами вспомогательных баз данных (Access, DBase, Foxpro, FireBird и т. п.);
- сервер Интранет (HTTP-сервер, FTP-сервер), на котором содержится внутренний сайт предприятия, как правило размещенный на сервере провайдера (поставщика услуг) Интернет;
- сервер базы данных СУБД MS ACCESS, СУБД ORACLE, на которых хранятся основные базы данных деловой активности организации (предприятия);
- proxy-сервер сети Интернет для оптимизации доступа сотрудников организации (предприятия) в сеть, выполняющий функции кэширования файлов, учет трафика;
- сервер электронной почты Exchange, предназначенный для обмена почтовыми сообщениями как внутри организации, так и с внешними адресатами сети Интернет (для этого, как правило, на сервере провайдера заводится дополнительный почтовый сервер и организуется синхро-

ный обмен сообщениями с внутренним почтовым сервером организации).

2. Внештатные программные или технические средства, обнаруженные на объекте информатизации.

3. Автоматические закладные регистрирующие и передающие устройства, не предусмотренные проектной документацией и технологией отводы от технических средств и линий связи, а также посторонние подключения к ним; обнаруженные нештатные программы с неизвестными функциями, а также нештатные запоминающие и другие технические устройства, способные выполнять функции скрытого отбора и накопления информации.

Признаками неправомерного доступа к информационной системе могут служить также следы хищения машинных или других оригиналов носителей информации, программных или аппаратных ключей и средств криптографической защиты информации. Способы их обнаружения и фиксации не имеют принципиальных отличий от способов обнаружения следов похищения документов, содержащих сведения конфиденциального характера, изложенных в предыдущем параграфе.

Меры предупреждения преступных посягательств на компьютерную информацию банка. Выполнение задач по *организации защиты компьютерной информации* возлагается на специально создаваемую систему ее защиты. Последняя согласно ГОСТ Р 50922–96) включает в себя совокупность органов и (или) исполнителей, технических средств защиты информации, а также объект зашиты. Создание и организацию работы СЗИ следует начинать с разработки и принятия документов, служащих правовой, организационно-распорядительной и нормативной основой деятельности по защите информации.

Основные направления защиты информации реализуются путем осуществления мер правового, организационного, программно-технического характера, в том числе путем применения криптографических средств защиты.

Наиболее распространенными обстоятельствами, способствующими противоправным посягательствам в сфере компьютерной информации, являются: просчеты в организации программной и технической защиты ЭВМ; легкомыслие или небрежность системного администратора службы безопасности информации (лица, ответственного за защиту информации на объекте); бесхозяйственность или умышленные действия сотрудников банка, разглашающих конфиденциальные сведения о компьютерной системе банка.

Примером ненадлежащего отношения к защите компьютерной информации могут служить обстоятельства преступления, известного по публикациям отечественных и зарубежных СМИ как «дело Левина». Группа лиц, работавших в одной из фирм Санкт-Петербурга, в том числе Владимир Левин, используя телекоммуникационные сети, несанкционированно входила в систему управления наличными фондами Ситибанка (США, Нью-Йорк). В про-

осуществили не менее сорока переводов на общую сумму свыше 10 млн долл., из которых около 400 тыс. долл. им удалось похитить.

Как выяснилось позднее, «входы» в некоторые компьютеры Ситибанка даже не были прикрыты паролями. Всего на этих компьютерах «побывало» более ста несанкционированных пользователей из России, которые использовали твердые диски банковских вычислительных машин для хранения своих программ, просматривали внутреннюю банковскую документацию, установили на эти компьютеры программу, при помощи которой общались друг с другом. Указанные действия оставались вне поля зрения администраторов сети в течение года[1].

Меры правовой и организационной защиты компьютерной информации банка заключаются в разработке и принятии банком специальных правовых и нормативных актов, предписывающих выполнение соответствующих правил и процедур, обеспечивающих защиту информации на правовой основе. Указанные документы представляют собой систему положений, инструкций, руководств, призванную четко регламентировать права и обязанности пользователей информации, правовой статус органов, технических средств и способов ее защиты. На этой основе устанавливаются полномочия руководителей банка по отнесению информации к сведениям ограниченного доступа и вводится порядок назначения и снятия грифа конфиденциальности. Организуется специальное делопроизводство, обеспечивающее сохранность носителей информации ограниченного доступа, а также техническую и физическую защиту информации.

Устанавливается персональная ответственность пользователя за сохранность доверенных ему конфиденциальных документов (носителей), за неправомерные действия в информационной системе, которые повлекли или могли повлечь несанкционированное ознакомление с защищаемой информацией, ее искажение или уничтожение, которые сделали информацию недоступной для законных пользователей. В этих целях организуется разрешительная система допуска исполнителей к работе с компьютерной информацией, документами и сведениями различного уровня доступа.

Одновременно разрабатывается и вводится в силу должностная инструкция, определяющая задачи, права, функции, ответственность и обязанности администратора СЗИ — лица, ответственного за защиту информации в банке. Эта инструкция должна предусматривать порядок ведения служебной документации средств защиты информации (смену паролей, ключей, изменения списка субъектов, имеющих право на доступ), организацию их надежного хранения. На администратора СЗИ возлагается задача оперативного контроля целостности программного и технического обеспечения, контроля за ходом технологического процесса обработки информации.

[1] Сегодня. 1996. 21 марта.

В соответствии с инструкцией, администратор СЗИ должен вести учет, хранение и выдачу пользователям носителей конфиденциальной информации, бумаги для распечаток (в случае отсутствия программной реализации печати учетных реквизитов и контроля за выдачей распечаток), паролей и ключей для средств защиты информации, осуществлять ежедневный контроль работы СЗИ с целью выявления любых изменений в сетевых компонентах, происшедших в нерабочее время. Периодически тестировать СЗИ с целью выявления уязвимых мест. Кроме того, администратор СЗИ обязан вести оперативный контроль за действиями пользователей информационной системы банка, совместно с организацией физической защиты помещений, в которых производится автоматизированная обработка конфиденциальной информации.

В число организационных задач по защите следует включить мероприятия по обучению пользователей правилам безопасной работы с защищаемой информацией и ознакомления с признаками противоправных посягательств на информацию.

Повышению надежности информационной системы банка способствует такая мера, как изготовление резервных копий данных с ключевых систем и других важных данных. Названные копии следует хранить в условиях, исключающих доступ к ним посторонних.

Защита информации путем применения программных и технических средств осуществляется включением в информационную систему банка программ и механизмов, закрывающих к ней доступ посторонних, в том числе с использованием пароля, шифрования или других методов. Применение указанных мер позволяет получить доступ к чтению, записи, созданию или уничтожению информации только надлежащим образом уполномоченным лицам. Кроме того, эти меры позволяют защитить правовую силу электронных документов в процессе обработки, хранения и передачи информационных сообщений, содержащих в себе приказы, платежные поручения, контракты и другие распорядительные и финансовые документы. Для защиты электронного документа от подделки применяется электронная цифровая подпись (реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа)[1].

Информационная система банка снабжается механизмами идентификации и аутентификации (проверки подлинности пользователей) на основе использования паролей, ключей, электронной цифровой подписи, а также биометрических характеристик личности пользователя.

Устанавливается мандатный порядок доступа, при котором пользователь наделяется правом получать доступ лишь к специально поименованным объектам (файлам, папкам, программам, томам) и только в тех пределах, которые являются санкционированными конкретно для него или группы работников

[1] Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (в ред. от 8 ноября 2007 г. № 258-ФЗ).

итать объект (файл), вносить в него запись, копировать). С этой целью каж-
ому пользователю и каждому документу присваиваются классификационные
етки, отражающие их место в соответствующей иерархии, служащие основой
андатного принципа разграничения доступа к информации.

Важным элементом программно-технических средств защиты информа
вляется автоматическая регистрация (протоколирование) информационной
истемой событий, имеющих отношение к защищенности информации. В
исло входит учет фактов разрешенного (и попыток несанкционированно
оступа к защищаемой информации (например, открытие файла, запуск п
раммы), а также создания и уничтожения документа. Для каждого из этих
ытий регистрируются: дата и время; конкретный пользователь; тип собы
если регистрируется запрос на доступ, то отмечается объект и тип досту
бслужен запрос на доступ или нет. Кроме того, в целях фиксации права с
твенности на информацию и предупреждения о ее особом правовом реж
ВТ должны обеспечивать вывод документа на бумажный носитель вм
его классификационной меткой (реквизитами).

К программным методам защиты СЗИ следует также отнести примен
стойчивого к «вирусам» программного обеспечения, защищенного от
южности несанкционированной модификации за счет специальных за
ованных вставок, снабженных механизмами самоконтроля и самовосста
ения; установку специальных программ-анализаторов, осуществляющих
иодическую проверку наличия возможных следов вирусной активн
например, обнаружение нарушений целостности программного обес
ия), а также жесткий «входной» контроль новых программ перед их введ
м в вычислительную систему по характерным признакам наличия в их «
ирусных образований.

Подводя итог сказанному, следует отметить, что надежная защита ком
ерной информации предполагает комплексное использование всех пер
енных средств и методов. По мнению специалистов в области защиты
формации, самая совершенная технология, правильная стратегия разв
е смогут гарантировать от упущений в управлении. С другой стороны, п
манная практика управления всегда может справиться с пробелами в тех
ии.

Наряду с администратором СЗИ субъектами защиты информации
вляются служба внутреннего контроля и служба безопасности.

Обязанности и полномочия службы внутреннего контроля в сфере за
компьютерной информации сформулированы в Положении Банка Р
№ 242-П. Согласно этому нормативному документу участие службы вну
него контроля банка в защите компьютерной (и другой защищаемой) ин
мации должно начинаться с контроля за соблюдением установленных в
критериев подбора и расстановки кадров (такие критерии устанавлив
целью исключить заключение трудовых договоров (контрактов) с ли

обладающими сомнительной деловой и общественной репутацией, а также
остаточно компетентными).

Кроме того, проверяется наличие в заключенных с работниками трудовых
глашениях (контрактах) соответствующих обязательств обеспечивать со-
анность защищаемой информации. Устанавливается, ознакомлен ли вновь
нятый или назначенный на соответствующую должность работник с инст-
кцией, регламентирующей его обязанности.

В процессе текущего контроля проверяется эффективность и работоспо-
бность систем, контролирующих соблюдение работником установленных
авил совершения соответствующих банковских и иных операций.

Под эффективностью и работоспособностью систем контроля в данном
учае понимается наличие процедур и механизмов, исключающих выход ра-
тника за пределы установленных полномочий.

В число подлежащих контролю входят, в частности, процедуры защиты
нфиденциальной банковской информации, организации доступа работни-
в к имеющейся в банке информации в зависимости от их компетенции, ус-
новленной внутренними регламентирующими документами.

Контрольные мероприятия должны охватывать проверку наличия пакета
ументов, регулирующих деятельность банка, включая положение о распре-
ении доступа пользователей к осуществлению операций в программном
ении, а также к базам данных в компьютерных системах и наличие
ных инструкций для всех штатных должностей в банке.

Кроме того, должно быть зафиксировано наличие (или отсутствие) кон-
ля состоянием информационной системы банка и ее безопасностью,
ериодичность оценки уровня безопасности информационной систе-

Служба безопасности банка принимает меры к предупреждению, выявле-
ю и пресечению попыток противоправных действий в сфере компьютер-
ой информации банка в пределах полномочий, установленных законодатель-
ством и внутренними нормативными правовыми актами банка. В отличие
от внутреннего контроля, решающей указанные выше задачи админис-
ивными методами, служба безопасности банка использует методы част-
ивной криминалистики.

*Основные предупреждение и пресечение попыток неправомерного посяга-
ств на защищаемую информацию банка.* Задача общего предупреждения
осягательства на защищаемую информацию банка (коммерческая,
ужебная тайны; защищаемая компьютерная информация)
ет службу защиты информации, службу внутреннего контроля
безопасности банка. Указанные структуры в пределах своей компе-
ции (подробнее о разграничении их полномочий сказано выше) осуществ-
ют за функционированием системы конфиденциального делопро-
водства и системы защиты компьютерной информации.

В случаях выявления нарушений требований должностных инструкций по конфиденциальному делопроизводству и защите компьютерной информации, которые могут привести к вредным последствиям, сотрудники контролирующих подразделений принимают меры к устранению нарушений и при необходимости обращаются к руководству организации с предложением о наложении взысканий на виновных.

Сотрудники указанных подразделений принимают меры к предупреждению и пресечению случаев похищения и утраты документов, содержащих коммерческую тайну, незаконного получения, разглашения и использования указанных сведений, неправомерного доступа к компьютерной информации, нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети.

О выявленных фактах противоправных действий или нарушений порядка обращения с защищаемой информацией они докладывают руководителю банка, который принимает решение о проведении соответствующей проверки (внутреннего расследования).

В ходе ее проведения устанавливаются обстоятельства происшедшего, виновность конкретных лиц, размер причиненного ущерба, выявляются причины и условия, способствовавшие совершению посягательства. Фактические данные, имеющие отношение к событию, документируются в установленном порядке и могут служить основанием для принятия решения о наказании работника организации в дисциплинарном порядке либо решения вопроса о его увольнении (прекращении трудового соглашения, контракта).

Фактические данные, полученные в результате проведенного расследования, используются в случае необходимости в качестве доказательств в арбитражном либо третейском суде.

Рассмотрение вопросов, связанных с нарушениями порядка защиты банковской, коммерческой или служебной тайны, защиты компьютерной информации, является прерогативой внутренней деятельности банка — обладателя конфиденциальной информации.

Оно проводится для выяснения обстоятельств подобных происшествий, а также для выявления и изучения грубых нарушений инструкции по конфиденциальному делопроизводству либо защите компьютерной информации, допущенных сотрудниками организации. Задачей разбирательства является установление виновности конкретных лиц, размера причиненного ущерба, выявление причин и условий, способствовавших совершению противоправных действий и нарушений порядка защиты коммерческой тайны.

Материалы разбирательства могут быть переданы в правоохранительные органы или в суд в целях пресечения выявленных неправомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба.

Разбирательство назначается руководителем организации и проводится группой сотрудников организации (комиссией) на основании соответствующего приказа.

Разбирательство представляет собой процесс гласного сбора и документирования информации, относящейся к событию, получаемой путем опроса работников организации, а также других лиц (с их согласия).

Члены комиссии наделяются правом производить осмотр рабочих помещений, территории организации, сейфов, столов, шкафов, других мест, где могут находиться представляющие интерес документы и иные носители информации; проверять полистно конфиденциальную документацию, журналы и карточки регистрации документов, отражающие их поступление и прохождение; опрашивать работников организации и требовать с них письменные объяснения.

Организационной основой для действий лиц, осуществляющих разбирательство, является инструкция о порядке проведения служебных расследований (внутренних разбирательств)[1]. Она разрабатывается сотрудниками организации и утверждается приказом ее руководителя.

В содержание названной инструкции, как правило, включаются разделы, посвященные поводам, основаниям и задачам проведения разбирательства, процедуре его назначения, срокам проведения, способам собирания и фиксации информации и полномочиям участвующих в разбирательстве лиц, использованию полученной в результате разбирательства информации.

Нередко в результате разбирательства удается получить сведения о причастности к противоправным посягательствам на коммерческую тайну граждан, не являющихся сотрудниками организации.

Дальнейшая проверка существа события (факта) в таких случаях выходит за пределы полномочий (и возможностей) комиссии и требует проведения сыскной деятельности. На этот случай в число членов комиссии, наряду с сотрудниками секретариата, целесообразно включать сотрудников службы безопасности (охранно-сыскного подразделения предприятия), наделенных правом сыска.

Договор об участии в разбирательстве обладатель коммерческой тайны может заключить также с любым частным детективом, детективным агентством, не входящим в структуру организации.

Проводя проверку, сотрудники службы безопасности, в соответствии с Законом о частной детективной деятельности, могут устанавливать обстоятельства неправомерного использования в предпринимательской деятельности недобросовестной конкуренции, а также разглашения сведений, составляющих коммерческую тайну.

При этом Закон о частной детективной деятельности позволяет сотрудникам службы безопасности опрашивать граждан и должностных лиц (с их согласия), наводить справки, изучать предметы и документы (с письменного согласия их владельцев), осматривать строения, помещения и другие объекты, вести наблюдение для получения необходимой информации.

[1] См. Приложение.

При осуществлении частной сыскной деятельности допускается использование видео- и аудиозаписи, кино- и фотосъемки, технических и иных средств, не причиняющих вреда жизни и здоровью граждан и окружающей среде.

По результатам работы комиссии составляется заключение, в котором излагается сущность исследованного события: место, время и способ нарушения правил конфиденциального делопроизводства, мотивы, последствия нарушения и другие существенные обстоятельства; сведения, которые подтверждают совершение нарушения и виновность причастных лиц, доводы, приводимые нарушителями в свою защиту, и результаты их проверки.

В случаях выявления обстоятельств, свидетельствующих о том, что конфиденциальными сведениями неправомерно завладели посторонние лица, материалы разбирательства могут служить основанием для подачи искового заявления (в порядке ст. 126 ГПК РФ) с требованием о возмещении материального ущерба. Они же являются доказательствами, подтверждающими требования истца.

Если же в результате работы комиссии будут установлены данные, свидетельствующие о совершении преступления, связанного с незаконным получением и разглашением сведений, составляющих коммерческую тайну (или иного-либо иного преступления), руководство организации обязано сообщить об этом в правоохранительные органы.

Материалы разбирательства в указанных случаях прилагаются к сообщению о преступлении, которое составляется в порядке, предусмотренном ст. 110 УПК РФ.

При возбуждении правоохранительными органами уголовного дела по данному факту сотрудники службы безопасности в соответствии со ст. 3 Закона о частной детективной деятельности по поручению руководителя банка могут участвовать в сборе сведений, способствующих установлению истины по этому делу.

О наличии такого поручения служба безопасности обязана в течение суток письменно уведомить лицо, производящее дознание, следователя, прокурора или суд, в чьем производстве находится уголовное дело. Для участия службы безопасности в сборе сведений по уголовному делу не имеет значения, явилось ли поводом для начала расследования сообщение банка или уголовное дело возбуждено на основании информации, поступившей из других источников.

7.5. Противоправные посягательства на кадровое обеспечение банка

Современный банк, по словам В. М. Усоскина, представляет собой чрезвычайно сложное и рискованное предприятие. Человеческий фактор (ошибки,

[1] *Усоскин В. М.* Современный коммерческий банк: Управления и операции. М.: Антикор, 1998. С. 77.

халатность и нелояльность персонала), по данным исследователей, представляет главную угрозу потерь банка[1]. По этой причине его укомплектованность высокопрофессиональным и надежным персоналом, способным добиваться высокой результативности труда (прибыли), умело защищать права и интересы банка, его вкладчиков и деловых партнеров, — одно из основных условий обеспечения экономической кредитной организации.

Для формирования личного состава, отвечающего указанным выше условиям, кадровые подразделения банков, как правило, используют собственные специально разработанные методики. Последние включают в себя набор требований к деловым и личным характеристикам работников, описание процедур отбора и приема на работу, планирование мероприятий по обучению, расстановке и воспитанию сотрудников, оценке их профессиональных и личных качеств и другие специфически «кадровые» действия. Несмотря на относительное разнообразие применяемых кадровыми службами приемов и методов, их объединяет общее начало. Все они разрабатываются на основе действующего законодательства. Так, основные требования к деловым и личным характеристикам работников банка сформулированы Законом о банковской деятельности и конкретизированы нормативными актами Банка России, квалификационными характеристиками и стандартами профессиональной деятельности в кредитно-финансовой сфере. В соответствии с ними руководители, менеджеры и ряд других представителей персонала банка должны обладать необходимым образовательным цензом, высоким профессионализмом, безупречной личной характеристикой, безусловно выполнять требования законодательства, норм деловой и профессиональной этики, соблюдать приоритет интересов клиентов над своими собственными интересами, не иметь конфликтов с законом и деловыми партнерами. Соответствие кадров указанным требованиям является весомой составляющей нематериальных активов банка[2].

Однако кроме общих проблем управленческого характера, процесс кадрового обеспечения включает в себя задачу сугубо специфическую: обеспечение защиты личного состава от неблагоприятного воздействия внешних сил и от иных обстоятельств, способствующих совершению работниками действий, противоречащих интересам банка.

Основным направлением указанной защиты является ограждение банка от проникновения в его личный состав нежелательных лиц. Это понятие объединяет:

1) субъектов с противоправными корыстными устремлениями;

2) представителей враждебных (или недружественных) банку организаций (в том числе недобросовестных конкурентов); организованных преступных

[1] *Мартынова Т.* Люди — самое слабое звено // Банковское обозрение. 2004. № 10 (64). С. 40–41.

[2] В некоторых случаях, например, при заключении договора о совместной деятельности (ст. 1042 ГК РФ), профессиональные и иные знания, навыки и умения, а также деловая репутация могут быть признаны вкладом стороны и оценены в денежном исчислении.

сообществ, а также лиц и структур, занимающихся незаконным получением конфиденциальной информации.

Представители первой группы действуют, как правило, по собственной инициативе и пытаются проникнуть в кадры банка на свой страх и риск с целью совершения хищений имущества (денег) банка.

Вторая группа субъектов проникает в кадровый состав банка, используя материальные, кадровые и иные ресурсы организаций, которые они представляют. Цели такого проникновения могут быть различными, однако все они противоречат интересам банка.

Технология такого проникновения категории «своих людей» в кадровый состав банка или иной организации, а также задачи, которые им предстоит выполнять, весьма откровенно описываются в появившихся в последнее время различного рода пособиях для «предпринимателей», желающих организовать «экономическую разведку» в интересах собственной фирмы.

Вот один из примеров практических рекомендаций подобного рода: «Свои люди могут быть как внедрены (возможно, после предварительной вербовки) в нужную группу (читай — организацию, предприятие. — *Авт.*), так и завербованы из ее членов. Уровень, занимаемый своим человеком (или людьми) в группе, может быть:

- высшим (человек из руководящего звена, принимающий непосредственное участие в выработке важных решений);
- средним (лица, имеющие доступ к устной или задокументированной информации);
- нижним (люди, посещающие те места, где общаются члены группы или находятся документы, но не допущенные к самим документам);
- вспомогательным (люди, не имеющие отношения к данной структуре, но способные оказывать некоторое содействие).

Своих людей бережно используют для решения самых разнообразных задач, с учетом их возможностей, соображений безопасности и потребностей момента:

- для получения информации;
- для смещения акцента в деятельности организации в нужном для вас направлении;
- для содействия в осуществлении определенных акций с целью:
  - дискредитации организации (намеренные ошибки), ее полного или частичного развала (разжигание розни и фракционности), внедрения и проведения на нужный уровень в группе своих людей;
  - установления подслушивающих устройств или добывания документов путем их скрытого копирования (ксерография, пересъемка) либо непосредственного похищения;
  - помощи в решении некоторых промежуточных задач (пропуска в нужное помещение, сведение с необходимым человеком)»[1].

[1] *Ронин Р.* Своя разведка: практ. пособие. Мн.: Харвест, 1997. С. 32–33.

Типовое задание по негласному добыванию информации об организации и вокруг нее приводит А. И. Доронин. Документ включает в себя задачи сбора следующих сведений:

1. Регистрационные данные.
2. Учредители (акционеры).
3. История создания и развития.
4. Направления деятельности и специализация.
5. Деловая репутация (участие в судебных разбирательствах, претензии со стороны правоохранительных органов, связи с криминалом, данные об участниках арбитражных процессов).
6. Руководство (лица, реально принимающие решения степень влияния на политику; лица, связанные с организованными преступными сообществами, личные и деловые характеристики (психологический портрет), деловые связи и опыт).
7. Отношения внутри организации (разногласия в команде управления, наличие группировок и семейных кланов и др.).
8. Система безопасности.
9. Сведения о финансовом положении (последний баланс, реальная и номинальная прибыль, взаимоотношения с контрагентами, наличие задолженности, факты неудачных инвестиционных проектов).
10. Планы на ближайшую перспективу.
11. Партнеры (взаимоотношения и условия сотрудничества).
12. Конкуренты (физические и юридические лица, формы противоборства)[1].

Ограждение сотрудников банка от неправомерного воздействия со стороны враждебных (недружественных) организаций и преступных сообществ является одним из важнейших направлений защиты кадрового потенциала. Попытки нанесения ущерба интересам банка путем неправомерного воздействия на персонал могут и не быть очевидными. Довольно распространенными, например, являются целенаправленные действия по сманиванию (фактическому подкупу) сотрудника банка на работу в другую организацию с целью воспользоваться конфиденциальной информацией, которой он располагает. Не исключаются действия провокационного характера: умышленное вовлечение работников в совершение противоправных либо общественно порицаемых действий с целью нанесения ущерба деловой репутации персонала банка.

Следует отметить, что законодатель, урегулировав в целом взаимоотношения между нанимателем (банком) и его работниками, возложил решение ряда насущных вопросов обеспечения безопасности кадрового состава на сами банки, их собственные системы кадрового обеспечения, обеспечения безопасности и внутреннего контроля.

Основные направления защиты кадрового состава банка. Защита кадрового состава банка осуществляется по следующим основным направлениям:

[1] *Доронин А. И.* Бизнес-разведка. 2-е изд., перераб. и доп. М.: Ось-89, 2003. С. 43–44.

а) ограждение кадрового состава банка от проникновения нежелательных лиц на стадии отбора кандидатов на работу путем отказа от заключения трудового договора;

б) разработка специальных стандартов поведения, направленных на защиту интересов банка, его клиентов и деловых партнеров (далее — интересы банка), и принятие работниками банка дополнительных обязательств по их соблюдению;

в) осуществление мероприятий организационного, социально-экономического и воспитательного (дисциплинарного) характера, направленных на повышение заинтересованности работников в укреплении и развитии банка и удовлетворенности собственным положением в коллективе, поддержание необходимой трудовой дисциплины;

г) выявление, предупреждение и пресечение неправомерных действий, предпринятых с целью побудить работников к участию в совершении противоправных действий, направленных против интересов банка, либо привлечь их к участию в совершении таких преступлений другими лицами;

д) ограждение кадрового состава банка от работников, совершивших действия, которые причинили (либо могут причинить) вред интересам банка, его клиентам и партнерам, путем расторжения трудового договора (увольнения).

Задача реализации перечисленных выше мер является приоритетной как для подразделений кадрового обеспечения, так и безопасности банка. Общее руководство этими действиями возлагается на руководство банка.

Защита кадрового состава банка от проникновения нежелательных лиц на стадии отбора кандидатов на работу путем отказа от заключения трудового договора

1. *Отказ от заключения трудового договора в связи с обстоятельствами, указанными законодателем.* Основанием для таких отказов служат нормы, содержащиеся в ряде отраслей действующего законодательства. В обобщенном виде их содержание, согласно ст. 84 ТК РФ, представляет некие «установленные правила приема на работу», нарушение которых исключает возможность продолжения работы (п. 11 ст. 77 ТК РФ). Применение указанных правил в ряде случаев требует обращения к нормам других отраслей законодательства. Например, Трудовой кодекс РФ не содержит прямого запрета на заключение трудового договора с лицом, лишенным приговором суда права заниматься определенной деятельностью, однако, согласно смыслу ст. 84 ТК РФ, будучи заключенным, такой трудовой договор подлежит прекращению.

Таким образом, согласно «правилам приема на работу» не допускается заключение трудового договора (контракта) с кандидатами на определенные должности в сфере банковской деятельности, в случае, если они лишены такого права по приговору суда. В соответствии со ст. 47 УК РФ лишение права занимать определенные должности или заниматься определенной деятельностью устанавливается судом на срок от одного года до пяти лет в качестве основного вида наказания, если оно предусмотрено соответствующей статьей

Особенной части Уголовного кодекса РФ (например, ст. 160 «Присвоение или растрата», ст. 200 «Обман потребителей», ст. 202 «Злоупотребление полномочиями частными нотариусами и аудиторами»). Кроме того, указанная мера может быть применена в качестве дополнительного вида наказания на срок от шести месяцев до трех лет за соответствующее преступление, если с учетом характера и степени общественной опасности совершенного преступления и личности виновного суд признает невозможным сохранение за ним права занимать определенные должности или заниматься определенной деятельностью. В сфере банковской деятельности — это должности, связанные с обслуживанием денежных и товарных ценностей, с доступом к конфиденциальной информации, распоряжением имуществом банка и т. п. Запись о назначении судом этого вида наказания вносится в трудовую книжку осужденного.

Аналогичная ситуация возникает в случаях, предусмотренных ст. 16 Закона о банках и банковской деятельности. Эта норма не устанавливает прямого запрета для приема на работу отдельных категорий кандидатов на должности руководителей исполнительных органов и (или) главного бухгалтера. В то же время она предусматривает отказ в государственной регистрации кредитной организации и выдаче лицензии на осуществление банковских операций, если эти должности занимают лица:

а) имеющие судимости за совершение преступлений против собственности, хозяйственных и должностных преступлений;

б) совершившие в течение года административное правонарушение в области торговли и финансов, установленное вступившим в законную силу постановлением органа, уполномоченного рассматривать дела об административных правонарушениях;

в) с которыми в течение последних двух лет по инициативе администрации расторгнут трудовой договор (контракт) по основаниям, предусмотренным п. 7 ст. 81 ТК РФ (совершение виновных действий работником, непосредственно обслуживающим денежные или товарные ценности, если эти действия дают основание для утраты доверия к нему со стороны работодателя).

Приведенный перечень обстоятельств, служащих основанием для ограничения права гражданина на заключение трудового договора, является исчерпывающим.

2. *Отказ от заключения трудового договора на основании оценки деловых и личных качеств кандидата работодателем.* В соответствии со ст. 64 ТК РФ необоснованный отказ в приеме на работу не допускается[1]. Вместе с тем,

[1] Под необоснованным отказом, согласно ст. 64 ТК РФ понимается какое бы то ни было прямое или косвенное ограничение прав или установление прямых или косвенных преимуществ при заключении трудового договора в зависимости от пола, расы, цвета кожи, национальности, языка, происхождения, имущественного, социального и должностного положения, места жительства (в том числе наличия или отсутствия регистрации по месту жительства или пребывания), а также других обстоятельств, не связанных с деловыми качествами работников, не допускается, за исключением случаев, предусмотренных федеральным законом.

законодатель не лишает нанимателя (банк) права выбора того или иного кандидата на работу с учетом его деловых и личных качеств.

Как правило, такой выбор делается на основании результатов предварительной проверки кандидата. Основная цель указанной проверки — оценка профессиональных качеств кандидата. Убедительные данные, свидетельствующие о зависимости судьбы банка от профессионализма его персонала, приводятся в книге «Принципы безопасности банка и банковского бизнеса в России». Согласно этому изданию, 58% работников банков, попавших в кризисную ситуацию, оказались неподготовленными к работе в банковской сфере. А непрофессиональные решения работников кредитных управлений стали причиной банкротства ряда московских и региональных банков[1]. Неквалифицированное управление банками, в частности управление валютными и кредитным рисками, явилось, по оценке Председателя Банка России В. В. Геращенко, основной причиной кризисного состояния банковской системы России после августа 1998 г.[2]

Однако не менее важным для обеспечения безопасности банка является наличие у будущего работника признаков отрицательной психологической характеристики личности, свидетельствующих о внутренней готовности лица к совершению противоправных действий (асоциальной установки). Информация об указанных признаках (или их отсутствии) поступает в ходе изучения анкетных данных, характеристик, рекомендаций, публикаций в печати[3]; проверки поведения кандидата по месту предыдущей работы и месту жительства. Сведения могут быть получены также в результате изучения образа жизни и связей кандидата. С этой целью могут быть опрошены осведомленные лица из окружения будущего работника, проведено собеседование с самим кандидатом и его тестирование. В ряде случаев простейшая проверка позволяет выявить частичное или полное несоответствие действительности представленных кандидатом анкетных данных, сведений о прежних местах работы, занимаемых должностях, об образовании, о квалификации.

Информация о предшествующем поведении кандидата может быть использована для выявления попыток внедрения в банк представителей криминальных сообществ и недружественных организаций.

В целом полученные в результате проверочных мероприятий сведения сводятся в два основных блока. Первый из них составляет информация о предшествующей профессиональной деятельности, свойствах характера и психики кандидата (психологическая характеристика). Она касается наличия или отсутствия достаточной квалификации, профессионального опыта, волевых и психофизических

[1] Принципы безопасности банка и банковского бизнеса в России / под общ. ред. А. Г. Шаваева. М.: Концерн «Банковский Деловой Центр», 1997. С. 16.

[2] Деньги и кредит. 1999. № 1.

[3] При проведении проверки следует учитывать установленный ст. 65 ТК РФ запрет требовать при приеме на работу документы, помимо предусмотренных законодательством.

качеств, необходимых для успешного выполнения должностных обязанностей; наличия или отсутствия отрицательных черт характера (агрессивность, конфликтность, лживость, недисциплинированность; неаккуратность, безответственность, завистливость, эгоизм и проч.).

Второй блок включает в себя сведения о социальной ориентации лица, т. е. о его отношении к различным социальным ценностям: к труду (трудовая психология), праву (правовая психология), к семье (семейно-бытовая психология), другим людям (психология общения), к самому себе (психология самооценки). По тому, на какие ценности ориентируется лицо, можно судить о степени деформации личности.

Ценностные социальные ориентации, как и нравственно-психологическое содержание личности, определяются по предшествующему поведению, по возможным социально порицаемым привычкам (социальная характеристика). К последним относятся связи с представителями криминального мира; конфликты с законом, правоохранительными и налоговыми органами, кредиторами; характер взаимоотношений с коллегами по прежней работе; злоупотребление алкогольными напитками, употребление наркотиков, увлечение азартными играми.

При оценке результатов проверки в той или иной форме используются достижения современной криминологии. Разработанные в соответствии с ними рекомендации позволяют с высокой степенью вероятности отличать деформированные нравственно-психологические качества лица с антиобщественной установкой (комплекс из 20–25 особенностей нравственно-психологической характеристики) от качеств законопослушного человека. Созданные на основе этих теоретических разработок программы ЭВМ и тесты для кадровых служб активно используются при оценке кандидатов на вакансии в практике кадровых служб государственных и коммерческих структур. Данные психологического тестирования (которое в случае необходимости проводится с использованием полиграфа) позволяют прогнозировать поведение кандидата в предполагаемых неблагоприятных ситуациях с абсолютной точностью.

Однако при проведении тестирования следует учесть, что, несмотря на кажущуюся простоту изложенных в программах операций, проводить тестирование и оценивать полученные результаты во избежание ошибки должен хорошо подготовленный специалист-профессионал.

Изучение зарубежного опыта свидетельствует о том, что в ряде фирм в результате отсева по результатам проверочных мероприятий работу получают примерно 9–10% от общего числа кандидатов.

Объем проверочных мероприятий следует планировать с учетом сопоставления предстоящих затрат с возможным ущербом от допущенной ошибки. При формировании коллектива следует учитывать данные судебной практики, согласно которым весомая часть преступных посягательств на интересы банков совершается «своими работниками».

В Германии, например, по сообщению директора отдела Федерального объединения немецких банков Д. Франке, два из трех преступлений в банковской сфере совершаются самими сотрудниками кредитных организаций. В 12% случаев сотрудники действуют в соучастии с «внешними» преступниками. В 85% всех крупных хищений средств и растрат виновниками или соучастниками преступлений являются сотрудники банков, а почти каждый двадцатый преступник — член руководства организации[1].

Россия в этом плане не составляет исключения. В отдельных случаях действия работников банков, совершающих преступления, связанные с исполнением трудовых обязанностей, отличаются почти полным отсутствием маскировки.

В 2003 г. в Москве завершился уголовный процесс над двумя сотрудницами Таганского отделения ОАО «Инкомбанк», которых признали виновными в мошенничестве и корыстном использовании банковской тайны. Имея доступ к реестру кредиторов, они присваивали деньги, которые банк начислял вкладчикам.

Известно, что клиенты банков, снимавшие свои валютные вклады после дефолта, несли значительные убытки, так как получали деньги по заниженному курсу. Однако со временем — в феврале 2000 г. — Инкомбанк решил эти убытки компенсировать, доплатив вкладчикам курсовую разницу из расчета 28,6 руб. за доллар (ранее им платили из расчета 6–10 руб. за доллар или не платили вообще). На выплатах курсовой разницы и сыграли мошенницы.

Преступление организовала старший эксперт Инкомбанка некто Л., имевшая доступ к спискам клиентов банка, которым должна была выплачиваться компенсация. Ее соучастниками были эксперт Инкомбанка некто О. и не работавший в банке Б.

В период с августа 2000 г. по май 2001 г. Л. передала Б. сведения о пяти крупнейших вкладчиках Инкомбанка: номера их счетов и вкладов, паспортные данные и образцы подписей. Это позволило Б. изготовить поддельные доверенности от имени вкладчиков. Потом он заверил доверенности у знакомого нотариуса и начал снимать деньги в Сбербанке. Чтобы упредить возможные обращения вкладчиков за получением компенсации, О. звонила клиентам и договаривалась с ними о встрече за пределами банка. Там она передавала вкладчикам наличные (передавая, например, вместо положенных 600 тыс. руб. — 60 тыс. руб.) и требовала расписку, что «претензий к банку нет». Таким образом мошенники, по данным следствия, оставили себе свыше 2,7 млн руб.

Преступление обнаружилось случайно. Л. и О. отслеживали всю переписку банка с клиентами, однако пропустили одно из сообщений. В нем банк извещал вкладчика о том, что ему начислена крупная компенсация и он может получить ее в Сбербанке. В мае 2001 г. этот вкладчик обратился в Сбербанк,

[1] *Франке Д.* Враг в собственных рядах: Преступность среди сотрудников банков // Вестник АРБ. 2005. № 8. С. 59–60.

но там ему ответили, что деньги за него получил по доверенности Б. Об этом вкладчик сообщил в милицию, которая и возбудила уголовное дело. В судебном заседании Л. и ее сообщники, обвиненные в мошенничестве и незаконном использовании банковской тайны, высказали недоумение тем, что следствие заинтересовалось только ими, тогда как в банке «аналогичные действия совершали многие»[1].

Использование полученной в результате проверки информации при принятии решения об отказе в приеме на работу не требует специальной аргументации со стороны работодателя. Поскольку в данном случае речь идет о свободе заключения трудового договора, наниматель (банк) вправе отдать предпочтение тому из кандидатов, профессиональные и личные качества которого будут признаны им предпочтительными.

Защита кадрового потенциала путем разработки специальных стандартов поведения, направленных на ограждение интересов банка, его клиентов и деловых партнеров, и принятие работниками банка дополнительных обязательств по их соблюдению. Законодательство России содержит ряд норм, предусматривающих обязанность банка разработать для определенных категорий работников специальные правила и стандарты поведения, связанные с обеспечением безопасности банка и его кадрового состава.

Выполнение этих правил и стандартов связано с частичными временными ограничениями гражданских прав таких работников, и поэтому факт их принятия специально оговаривается в трудовом договоре. Принятие названных специальных обязательств является обязательным условием заключения договора. И наоборот, отказ от них служит основанием для прекращения договора.

Виды специальных обязательств, принимаемых работниками, сравнительно немногочисленны. По содержанию они включают в себя следующие предписания:

- не разглашать сведения, составляющие охраняемую законом тайну (банковскую, коммерческую и иную), ставшую известной работнику в связи с исполнением трудовых обязанностей;
- нести полную материальную ответственность за необеспечение сохранности имущества и других ценностей, переданных для хранения или для других целей;
- соблюдать требования законодательства о финансовых рынках, стандартов профессиональной деятельности на финансовых рынках, в кредитных организациях.

Принятые работником специальные обязательства должны быть конкретизированы во внутренних (локальных нормативных актах, содержащих нормы трудового права, принимаемых работодателем — ст. 8 ТК РФ) документах банка (правилах обращения с материальными ценностями, инструкциях по конфиденциальному делопроизводству, стандартах профессиональной деятельности

[1] *Герасимов А.* В Инкомбанке похищали курсовую разницу // Коммерсантъ. 2003. № 36/П (32 539). 3 марта.

кредитных организациях и некоторых других), с которыми работник должен быть ознакомлен под расписку.

Допускается перечисление обязанностей работника, связанных с обеспечением сохранности доверенных ему ценностей и информации, непосредственно в трудовом договоре (контракте), который также заключается в письменной форме.

К категориям лиц, принимающим специальные обязательства, относятся работники:

- которым доверена информация, составляющая служебную или коммерческую (банковскую) тайну;
- которым переданы для хранения или других целей имущество и другие ценности;
- участвующие в осуществлении операций (сделок) кредитной организации на финансовых рынках.

Принятие работником на себя специальных обязательств предполагает его согласие соблюдать ряд дополнительных условий, установленных специальными правилами, инструкциями и другими внутренними документами банка.

Так, работникам, получающим допуск к сведениям, составляющим банковскую, коммерческую и иную тайну, кроме обязанностей, непосредственно связанных с обеспечением сохранности информации, следует:

- представить кадровому аппарату сведения о возникновении оснований для отказа к названному допуску;
- дать согласие на проведение в отношении него проверочных мероприятий (в связи с процедурой допуска к конфиденциальной информации) соответствующими службами банка либо иной частной коммерческой службой по договору с банком (выяснение биографических и других характеризующих личность данных в пределах, установленных ст. 3 Закона о частной детективной деятельности).

Работник, участвующий в осуществлении операций (сделок) кредитной организации на финансовых рынках, кроме соблюдения правил финансовых операций, обязан доводить до сведения своего непосредственного руководителя и представителя службы внутреннего контроля банка (комплаенс-контролера) информацию:

- о юридических лицах, в которых он и (или) его родственники (супруг, супруга, родители, дети, братья, сестры) владеют самостоятельно или в группе лиц 20% или более голосующих акций (долей, паев);
- о юридических лицах, в органах управления которых он и (или) его родственники занимают должности;
- об известных ему операциях (сделках), в совершении которых он может быть признан заинтересованным лицом (совершаемых или предполагаемых);
- о сделках (операциях) на финансовых рынках, совершаемых сотрудником кредитной организации в своих интересах и за свой счет.

Кроме того, работники, участвующие в осуществлении операций (сделок) кредитной организации на финансовых рынках, принимают обязательства:

- не использовать служебную информацию в собственных интересах и не передавать ее третьим лицам, не проводить операции (сделки) в своих интересах;
- выполнять требования о предотвращении легализации денежных средств или иного имущества, полученных незаконным путем и не совершать ряд других действий.

На работников, заключивших договор о полной индивидуальной материальной ответственности, кроме бережного отношения к доверенным ценностям и строгого соблюдения правил совершения операций с ценностями и их хранением, возлагается обязанность:

- своевременно сообщать руководству банка обо всех обстоятельствах, угрожающих обеспечению сохранности вверенных ему ценностей;
- возмещать суммы допущенных по его вине недостач и не выявленных им неплатежных и поддельных денежных знаков;
- не разглашать известные ему сведения об операциях по хранению ценностей, их отправке, перевозке, охране, сигнализации, а также служебных поручениях по кассе.

Защита кадрового состава банка путем осуществления мер организационного и социально-экономического характера представляет собой систему взаимосвязанных задач и направленных на их решение действий руководства и кадрового аппарата банка. Объем этих задач меняется в зависимости от обстановки, однако часть из них является обязательной для любой кадровой ситуации.

В первую очередь к ним относится задача своевременного обеспечения руководства банка полной, всесторонней и объективной информацией о таких показателях степени надежности персонала, как уровень удовлетворенности (мотивации) работников, морально-психологический климат, состояние дисциплины и правопослушности персонала. Например, проведенные специалистами исследования свидетельствуют о том, что возникновение у работника чувства неудовлетворенности отрицательно влияет на эффективность его профессиональной деятельности, может послужить причиной снижения дисциплины. Чувство неудовлетворенности (обида, озлобленность) может быть использовано криминальными сообществами и недружественными организациями для того, чтобы побудить работника к участию в совершении противоправных действий, направленных против интересов банка.

Являясь обобщающим показателем, чувство неудовлетворенности заслуживает тщательного выявления его истоков в каждом конкретном случае и скорейшего устранения его причин.

Типичными причинами указанного явления служат неудовлетворенность просчетами в организации профессиональной деятельности и условиями труда; социально-психологическим климатом в коллективе (конфликтными отношениями с руководителем или сослуживцами); отсутствием перспектив

профессионального роста и заработной платы; нечетко поставленными целями профессиональной деятельности, отсутствием осознания ценности своей работы и проч.

Установлено, что неудовлетворенность, порожденная отдельным обстоятельством, может оказывать отрицательное влияние на ряд сторон профессиональной деятельности и надежность кадрового состава. По этой причине выявление и устранение причин, порождающих неудовлетворенность работников, является важной повседневной задачей руководителей банка и его кадровых служб. Решать эту задачу желательно с участием штатных или привлеченных практических психологов и социологов. Наиболее распространенный на практике метод социологического изучения коллектива — анкетирование работников, основанное на получении в письменной форме ответов по определенному кругу вопросов.

Полученные в ходе этой работы данные могут быть использованы также для обнаружения скрытых или прогнозирования назревающих нежелательных процессов в коллективах, для преодоления возникающих в сфере кадрового обеспечения противоречий, повышения эффективности служебной деятельности и безопасности банка.

Работа по предупреждению и устранению нежелательных процессов в указанной сфере должна включать в себя систему мер, направленных на создание необходимых организационных и экономических условий для высокопроизводительной работы, на повышение уровня заинтересованности работников в результатах своего труда; на создание условий для максимально полной реализации способностей каждого работника в сфере его профессиональной деятельности; на поддержание благоприятного социально-психологического климата в коллективе; на использование различных форм поощрения работников, в том числе предусмотренных ст. 191 ТК РФ: объявление благодарности; выдача премии; награждение ценным подарком; награждение почетной грамотой; представление к званию лучшего по профессии, а также другими поощрениями, которые могут быть предусмотрены правилами внутреннего трудового распорядка, уставами и положениями о дисциплине.

Объективным внешним проявлением неблагополучия в обеспечении защиты кадрового состава служат следующие факторы:

а) совершение работниками преступного посягательства на интересы банка либо соучастие в таком посягательстве;

б) совершение грубого нарушения дисциплины (противоправного, виновного неисполнения или ненадлежащего исполнения работником его трудовых обязанностей).

В соответствии с формулировкой Трудового кодекса РФ, противоправным считается действие или бездействие, нарушающее требования закона или подзаконных актов, устанавливающих трудовые обязанности работника, в том числе:

- действия, нарушающие внутренние должностные инструкции и устан-новленные в банке правила внутреннего распорядка;
- отказ от принятия на себя обязательств, предусмотренных внутренним должностными инструкциями (отказ работника без уважительных причин заключить договор о неразглашении сведений конфиденциального характера, о соблюдении стандартов профессиональной деятельности при осуществлении операций (сделок) банка на финансовых рынках о полной материальной ответственности;
- действия, не связанные с деятельностью банка, однако наносящие ущерб личной и деловой репутации работника и банка в целом (административные правонарушения, конфликты с кредиторами и т. п.).

Данные о состоянии дисциплины, наряду с данными о правопослушности коллектива, служат важным показателем надежности кадрового состава.

Обязательным элементом состава дисциплинарного проступка является вина работника в любой форме (умысла или неосторожности).

Совершение дисциплинарных проступков (то есть нарушение взятых на себя по трудовому договору обязательств общего и специального характера), как правило, свидетельствует о безразличном, пренебрежительном или негативном отношении работника к установленным в банке нормативным предписаниям, об определенной деформации нравственно-психологических качеств личности нарушителя, о вероятности совершения им более тяжких правонарушений в будущем и о снижении защищенности кадрового потенциала в целом. С учетом этого по каждому допущенному дисциплинарному проступку должно проводиться тщательное разбирательство для установления степени вины нарушителя, выявления причин и условий, способствовавших совершению проступка. Учет и анализ проступков и разработка мер, направленных на предупреждение аналогичных событий в будущем — важное направление обеспечения безопасности кадрового потенциала банка.

Перечень возможных взысканий за нарушения трудовой дисциплины установлен ст. 192 ТК РФ. Он включает в себя: замечание; выговор; увольнение по соответствующим основаниям, и является исчерпывающим.

Наложение взысканий за совершенные проступки служит действенной мерой воспитательного и предупредительного характера. Однако взыскание при этом должно быть обоснованным и соразмерным содеянному. При наложении взыскания должны учитываться тяжесть совершенного проступка, обстоятельства, при которых он совершен, предшествующая работа и поведение работника. Обида и озлобление несправедливым взысканием могут привести к прямо противоположному результату. Окончательное решение о применении взыскания принадлежит администрации, которая может и не применять взыскания, хотя проступок и имел место, а ограничиться устным замечанием, беседой и т. п.

Выявление, предупреждение и пресечение посягательств на кадровый состав со стороны недружественных организаций и нежелательных лиц. В обеспечении

безопасности банка в определенной мере принимают участие большинство его основных подразделений, однако ведущая роль на этом направлении деятельности отводится службе безопасности, службе кадрового обеспечения и службе внутреннего контроля банка. Эти структуры несут ответственность за надлежащее функционирование и безопасность системы кадрового обеспечения в целом и отдельных ее элементов, перечисленных выше. В первую очередь — за ограждение кадрового состава банка от проникновения нежелательных лиц; за защиту личного состава от попыток побудить работников к участию в совершении *противоправных действий против интересов банка* либо привлечь их к участию в совершении таких преступлений другими лицами.

Сотрудники указанных подразделений ведут контроль за строгим соблюдением требований законодательства, нормативных актов ведомств и должностных инструкций банка, имеющих непосредственное отношение к обеспечению безопасности банка и, в частности, его кадрового потенциала. В случаях выявления нарушений требований должностных инструкций они принимают меры к устранению нарушений и при необходимости обращаются к руководству организации с предложением о наложении взысканий на виновных.

На службу безопасности, кроме того, возлагаются специальные обязанности по защите личного состава. В их числе обязанность выявления признаков подготовки к проникновению в банк нежелательных лиц и признаков подготовки к неправомерному воздействию на персонал банка. Эти сведения, как правило, собираются негласно в рамках Закона о частной детективной деятельности. Возможно также использование в указанных целях полиграфа (детектора лжи) в целях обследования как кандидатов на работу, так и работающих сотрудников. Обследование сотрудников желательно проводить на разных этапах карьеры (при перемещении по работе, проведении служебных расследований и т. д.). Результаты такого тестирования могут выявить мотивы поступления на работу, особенности личности и поведения сотрудника (либо кандидата на заключение контракта), уточнить анкетные данные и некоторые особенности поведения, выявить алкогольную и наркотическую зависимость, а также криминальное прошлое и криминальные связи. Кроме этого, сам факт использования полиграфа играет роль предупреждения для потенциальных правонарушителей.

К сожалению, количественные показатели, позволяющие оценить роль полиграфа в ограждении банковской сферы России от проникновения криминальных элементов в кадровый состав, в настоящее время отсутствуют. Однако определенное представление об эффективности этого метода при оценке кандидатов в других сферах деятельности можно сделать на основании интервью бывшего заместителя министра внутренних дел Российской Федерации Е. Б. Соловьева газете «Щит и меч». По его словам, тестирование кандидатов на службу в милицию проводится в каждом четвертом центре психодиагностики МВД, ГУВД

УВД субъектов Российской Федерации. В 2003 г. с применением полиграфа обследованы около двух тысяч человек. Установлены лица с криминальными связями (каждый десятый обследованный), наркоманы (почти треть) и другие кандидаты, не пригодные к службе[1]. Согласно сообщению ГУВД Краснодарского края, проведение полиграфных проверок при решении кадровых вопросов позволяет выявлять значительное число нераскрытых ранее преступлений. Так, в один из периодов при проведении обследования 89 человек были получены данные о 147 совершенных ими ранее преступлениях. В 60 случаях были получены признательные показания, нашедшие впоследствии подтверждение[2].

Нежелательные лица могут проникать в банк под собственной фамилией в соответствии с имеющейся у них профессией либо по поддельным документам с сокрытием фактов собственной биографии. В качестве меры, препятствующей поступлению нежелательного лица на работу, необходимо предпринять скоординированные действия (явные и замаскированные), которые обеспечат обоснованный отказ в приеме.

Признаки подготовки к проникновению в банк нежелательных лиц включают в себя следующие действия:

- сбор информации об источниках пополнения кадров, о требованиях к кандидатам на работу и процедуре приема на работу;
- создание обстоятельств, вынуждающих уволиться из банка работника, на должность которого претендует новый кандидат;
- использование кандидатом ложных сведений, аргументирующих факт его поступления на работу в банк;
- использование кандидатом на работу поддельных документов (в том числе публикаций в СМИ, рекомендательных характеристик и т. д.), положительно характеризующих его с деловой и личностной сторон;
- маскировка кандидатом на работу своих связей с недружественной организацией, сокрытие отдельных биографические данных, фактов неблаговидного поведения или конфликтов с законом, кредиторами, налоговыми и иными правоохранительными органами;
- маскировка кандидатом своей предшествующей работы в фирмах-«однодневках», учрежденных по поддельным документам и несуществующим адресам.

Характерными признаками подготовки к неправомерному воздействию на персонал банка являются:

- неоправданный интерес к работнику и членам его семьи со стороны недружественной организации, сбор сведений (в том числе компрометирующих) о работнике и его близких, об их образе жизни, распорядке дня, привязанностях и т. п.;

[1] МВД/Пресс-служба. 2004. 23 дек. (http://mvdinform.ru/index.php?docid=19).

[2] *Варламов В. А., Богданова Т. С., Тишкова Н. Ю.* Проведение полиграфных проверок при решении кадровых вопросов: Опыт использования полиграфа в профилактике и раскрытии преступлений в ГУВД Краснодарского края (1-я научно-практическая конференция). Краснодар, 1997. С. 42–43.

- неожиданные попытки установить с работником связи на этнической, религиозной или расовой основе;
- попытки вовлечь работника в совершение общественно порицаемых (компрометирующих) или противоправных действий;
- поступление конфиденциальных предложений о переходе на более привлекательную работу, о готовности оказать работнику материальную и иную помощь;
- факты угроз в адрес работника со стороны неизвестных лиц.

В случае выявления признаков подготовки к неправомерному воздействию на персонал, служба безопасности срочно информирует об этом руководителя банка и принимает неотложные меры по ограждению от возможных посягательств (в том числе, по физической защите) работников банка. В необходимых случаях информирует правоохранительные органы и взаимодействует с ними.

При этом следует учитывать, что в зависимости от вида и обстоятельств готовящегося противоправного посягательства, подготовительные действия недружественных структур могут совершаться в отношении различных категорий работников. Однако практика свидетельствует о том, что обычно степень их интереса к установлению противоправных отношений с работниками банка выстраивается в определенной последовательности.

Категории работников банка, в отношении которых недружественные структуры предпринимают попытки неправомерного воздействия, характеризуются следующими отличительными чертами. Это лица:

1) наделенные распорядительными функциями в отношении ценностей, имущества и конфиденциальной информации банка, принимающие решение о проведении банковских операций и сделок на финансовых рынках (руководители банка и его подразделений, главный бухгалтер);

2) имеющие доступ к банковским операциям, связанным с переводами и выдачей денежных средств (операторы системы электронных расчетов банка);

3) имеющие постоянный доступ к деньгам (валюте), ценностям и ценным бумагам (кассиры, инкассаторы);

4) имеющие временный доступ к помещениям касс, хранилищам (технические специалисты, уборщицы, охранники);

5) располагающие информацией, относящейся к банковской тайне, и иной конфиденциальной информацией (в том числе, о порядке хранения и перемещения денег и других ценностей банка). К ним относятся работники:

- которым информация была доверена по работе;
- имеющие возможность незаконно получить информацию в процессе выполнения своих обязанностей, не связанных с допуском к конфиденциальным сведениям (технический и обслуживающий персонал, охранники);

6) обеспечивающие функционирование ЭВМ: операторы, программисты, инженеры;

7) участвующие в осуществлении операций (сделок) банка на финансовых рынках;

8) работающие в службе внутреннего контроля банка;

9) технический и вспомогательный персонал, сотрудники охраны, временные работники, работники организаций-контрагентов.

Определенный интерес для организаторов противоправных посягательств представляют также лица, ранее работавшие в банке, в том числе пенсионеры.

Одна из задач службы безопасности заключается в обучении работников банка правилам безопасного поведения, умению распознавать признаки подготавливаемого или совершаемого преступления, в том числе в элементах странного или подозрительного поведения сослуживцев и окружающих. Следует также заблаговременно планировать необходимые совместные действия работников банка и сотрудников службы безопасности на случай возникновения экстремальных ситуаций (шантажа, угроз и т. п.).

Предупреждение попыток проникновения в коллектив банка нежелательных лиц и неправомерных посягательств на персонал банка является частным направлением деятельности, связанной с выявлением и устранением угроз безопасности банка в целом. Это объясняется тем, что такие попытки, как правило, представляют собой подготовительный этап к совершению преступных посягательств на его имущество, информацию и другие охраняемые объекты права собственности.

Признаки проникновения в банк нежелательных лиц. О том, что нежелательные лица, несмотря на предпринятые меры безопасности, получили доступ к охраняемым объектам права собственности банка либо о том, что кто-то из работников банка согласился действовать в интересах недружественных организаций и нежелательных лиц, могут свидетельствовать следующие характерные признаки:

а) совершение преступных посягательств на интересы банка неустановленными лицами:

- хищение ценностей и имущества;
- перехват информации, циркулирующей в технических средствах и помещениях банка (обнаружение автоматических закладных устройств, посторонних отводов от технических средств и линий связи, нештатных программ и запоминающих устройств, хранение на неучтенных носителях информации конфиденциального характера и т. п.);

б) наличие причинивших ущерб интересам банка происшествий с неустановленной причиной:

- недостача денежных средств;
- утечка информации (например, несанкционированное опубликование конфиденциальной информации в СМИ);
- осведомленность посторонних лиц о защищаемых сведениях;
- утрата ключей, документов, печатей, бланков банка;

- исчезновение или повреждение (уничтожение) имущества;
- умышленный вывод из строя охранной сигнализации и т. п.;

в) появление в банке сотрудников, поддерживающих подозрительные контакты с представителями криминального мира либо недружественными банку организациями; попавших в материальную и иную зависимость от посторонних лиц; имеющих доходы, происхождение которых они не могут объяснить;

г) неподтверждение биографических данных сотрудника;

д) предшествующая *работа* сотрудника в фирмах-«однодневках», учрежденных по поддельным документам и несуществующим адресам;

е) поведение работников, дающее основания предположить наличие у них намерений совершить противоправные действия, посягающие на интересы банка:

- неоправданный интерес к конфиденциальной информации;
- попытки получить непосредственный доступ к ценностям, информации и документам либо скрытно собирать конфиденциальную информацию в процессе служебной (производственной) деятельности;
- неоправданный интерес к сведениям об организации работы банка, видах его имущества, местах хранения ценностей или информации, о порядке работы с ними, возможности выноса денег; документов и иных носителей информации за пределы территории;
- немотивированное изучение структуры и эффективности деятельности службы безопасности; технических средства охраны.

Обеспечение безопасности кадрового потенциала путем прекращения трудовых отношений с работниками, наносящими ущерб интересам банка. Важной мерой обеспечения безопасности банка является расторжение трудового договора (увольнение) с лицами, проникшими в его кадровый состав с противоправными корыстными устремлениями, и субъектов, представляющих организованные преступные сообщества либо враждебные или недружественные банку организации. Законодательство содержит исчерпывающий перечень оснований для расторжения трудового договора по инициативе администрации. Их всего четырнадцать (ст. 81 ТК РФ). Однако в данном случае речь идет только о тех, которые применяются при наличии вины работника.

Для принятия решения об увольнении указанных лиц (в том числе после их выявления службой безопасности либо правоохранительными органами) необходимо наличие специально установленных законом оснований. Таким основанием служит наличие юридических фактов, предусмотренных законом, зафиксированных в установленном порядке.

Прежде всего это факт совершения работником преступного посягательства на объект гражданских прав банка (имущество, имущественные права, информация, нематериальные блага и др.) либо, при определенных условиях, совершение преступления, не связанного с работой в банке. Факт совершения преступления должен быть удостоверен вступившим в законную силу

приговором суда, которым работник осужден к лишению свободы, исправительным работам не по месту работы либо к иному наказанию, исключающему возможность продолжения данной работы (в частности, к лишению права занимать определенные должности или заниматься определенной деятельностью). В случае же условного осуждения и отсрочки исполнения приговора сам по себе факт вынесения обвинительного приговора основанием для увольнения работника служить не может.

Другим основанием для расторжения трудового договора служит совершение работниками действий, относящихся к грубым нарушениям трудовой дисциплины. Такие действия с точки зрения обеспечения безопасности могут создавать условия для совершения преступных посягательств на интересы банка; представлять собой непосредственную подготовку к совершению таких посягательств либо свидетельствовать об определенной деформации нравственно-психологических качеств личности работника и о вероятности совершения им более тяжких правонарушений в будущем. В частности, речь идет о действиях, нарушающих установленные в банке правила безопасного поведения, правила защиты (обеспечения безопасности) объектов гражданских прав банка и порядка его функционирования (инструкции, положения и т. п.), а также о действиях, наносящих ущерб деловой репутации банка.

К числу грубых нарушений дисциплины, которые могут служить основанием для растожения трудового договора по инициативе работодателя, ст. 81 ТК РФ относит:

- неоднократное неисполнение работником без уважительных причин трудовых обязанностей, если он имеет дисциплинарное взыскание;
- однократное грубое нарушение работником трудовых обязанностей:

а) прогул (отсутствие на рабочем месте без уважительных причин более четырех часов подряд в течение рабочего дня);

б) появление на работе в состоянии алкогольного, наркотического или иного токсического опьянения;

в) разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей;

г) совершение по месту работы хищения (в том числе мелкого) чужого имущества, растраты, умышленного его уничтожения или повреждения, установленных вступившим в законную силу приговором суда или постановлением органа, уполномоченного на применение административных взысканий;

д) нарушение работником требований по охране труда, если это нарушение повлекло за собой тяжкие последствия (несчастный случай на производстве, авария, катастрофа) либо заведомо создавало реальную угрозу наступления таких последствий;

- совершение виновных действий работником, непосредственно обслуживающим денежные или товарные ценности, если эти действия дают основание для утраты доверия к нему со стороны работодателя;

- совершение работником, выполняющим воспитательные функции, аморального проступка, несовместимого с продолжением данной работы;
- принятие необоснованного решения руководителем организации (филиала, представительства), его заместителями и главным бухгалтером, повлекшего за собой нарушение сохранности имущества, неправомерное его использование или иной ущерб имуществу организации;
- однократное грубое нарушение руководителем организации (филиала, представительства), его заместителями своих трудовых обязанностей;
- предоставление работником работодателю подложных документов или заведомо ложных сведений при заключении трудового договора;
- прекращение допуска к государственной тайне, если выполняемая работа требует допуска к государственной тайне;
- в случаях, предусмотренных трудовым договором с руководителем организации, членами коллегиального исполнительного органа организации;
- в других случаях, установленных Трудовым кодексом РФ и иными федеральными законами.

Надо иметь в виду, что доказывание фактов, служащих основанием для расторжения трудового договора, возлагается на администрацию банка.

Для подтверждения алкогольного, наркотического или токсического опьянения работника может быть использовано медицинское заключение или другие доказательства. Например, подтверждение факта распития спиртных напитков.

Факт хищения чужого имущества должен быть установлен вступившим в законную силу приговором суда или постановлением органа, в компетенцию которого входит наложение административного взыскания (например, милиции) или применение мер общественного воздействия (например, постановление собрания трудового коллектива).

Совершение виновных действий работником, непосредственно обслуживающим денежные или товарные ценности, если эти действия дают основание для утраты доверия к нему со стороны работодателя, может быть основанием для расторжения договора только в отношении работников, непосредственно обслуживающих денежные и товарные ценности. Как правило, это работники, несущие полную материальную ответственность на основании специального закона или письменных договоров о полной материальной ответственности.

Утрата доверия должна быть основана на конкретных фактах совершения работником виновных действий. Таких, например, как обсчет клиента в небольшом размере или незаконные операции с иностранной валютой и платежными документами, совершенные валютным кассиром. Утрата доверия возможна не только за допущенные работником злоупотребления,

но и за халатное его отношение к своим трудовым обязанностям. Например, за выдачу денежных сумм без соответствующего оформления, хранение ключей от помещения с материальными ценностями в ненадлежащем месте. Основанием для увольнения по п. 7 ст. 81 ТК РФ является и использование работником вверенных ему денежных и товарных ценностей в личных целях.

Факты совершения работником банка виновных действий должны быть зафиксированы документально (путем составления акта, заявлений клиентов, объяснений очевидцев). Виновные действия работника могут быть установлены администрацией банка (в лице соответствующих служб), контрольными службами органов власти либо правоохранительными органами. В частности, в процессе производства по делам об административных правонарушениях либо в процессе следствия по уголовному делу. При этом для увольнения по п. 7 ст. 81 ТК РФ не требуется наличия вступившего в силу приговора суда. Более того, само уголовное дело может быть прекращено по основаниям, не исключающим вины работника (например, в связи с применением мер административного взыскания или передачей на поруки). Достаточным основанием для увольнения в данном случае служит конкретный факт совершения работником виновных действий, дающих основание для утраты к нему доверия со стороны администрации.

При установлении в предусмотренном законом порядке факта совершения хищения, взяточничества и иных корыстных правонарушений эти работники могут быть уволены по основанию утраты к ним доверия даже в том случае, когда указанные действия не связаны с их работой[1].

Основаниями для расторжения трудового договора по инициативе работодателя могут стать также выявленные службой безопасности либо другими подразделениями факты нарушения установленных правил приема на работу, (прием на работу лиц, лишенных приговором суда права заниматься определенной деятельностью в течение назначенного судом срока; прием на работу, связанную с материальной ответственностью лиц, ранее судимых за хищения, взяточничество и иные корыстные преступления, если судимость не снята и не погашена; прием на работу служащих, состоящих между собой в близком родстве или свойстве, если их служба связана с непосредственной подчиненностью или подконтрольностью одного из них другому).

Действия администрации в случае обнаружения признаков проникновения в банк нежелательных лиц или совершения противоправных посягательств работниками банка. О выявленных признаках подготовки к проникновению в банк нежелательных лиц соответствующие службы докладывают руководителю банка, с которым согласовывают разработку и реализацию мер (гласного или негласного характера) по предупреждению возникшей угрозы.

---

[1] Пункт 41 Постановления Пленума Верховного Суда РФ от 22 декабря 1992 г. // Бюллетень Верховного Суда РФ. 1993. № 3.

В случае обнаружения признаков совершения противоправных посяга-тельств работниками банка, его руководитель принимает решение о проведе-нии соответствующей официальной проверки (разбирательства).

Разбирательство проводится группой сотрудников организации (комис-сией) на основании соответствующего приказа. Организационной основой для действий лиц, осуществляющих разбирательство, является инструкция о порядке их проведения. Она разрабатывается в банке и утверждается при-казом.

В ходе разбирательства устанавливаются обстоятельства происшедшего, виновность конкретных лиц, размер причиненного ущерба, выявляются причины и условия, способствовавшие совершению посягательства. Факти-ческие данные, имеющие отношение к событию, документируются в уста-новленном порядке и могут служить основанием для принятия решения о наказании работника организации в дисциплинарном порядке либо реше-ния вопроса об его увольнении (прекращении трудового соглашения, кон-тракта).

7.6. Противоправные посягательства на нематериальные активы банка

Понятие нематериальных благ (активов) банка. В соответствии с граждан-ским законодательством нематериальные блага относятся к одному из видов объектов гражданских прав (ст. 128 ГК РФ). Гражданский кодекс не дает ис-черпывающего перечисления видов нематериальных благ. Их наиболее пол-ный систематизированный перечень, включающий честь, доброе имя и дело-вую репутацию содержится в ст. 150 ГК РФ, посвященной порядку осуществ-ления и защиты нематериальных прав личности. Однако право обладать нематериальными благами и защищать их в порядке, установленном законом, не является исключительной привилегией личности. Законодательство Рос-сии признает такое право и за юридическими лицами.

В соответствии с ч. 7 ст. 152 ГК РФ правила о защите деловой репутации гражданина применяются также к защите деловой репутации юридического лица.

В хозяйственной деятельности юридического лица нематериальные блага выступают в качестве нематериальных активов, оценивающихся в денежном исчислении. К нематериальным активам, используемым в хозяйственной дея-тельности и приносящим доход, Положение по бухгалтерскому учету «Учет не-материальных активов» относит права, возникающие из авторских и иных до-говоров, на следующие результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность): произведения науки, литературы и искусства; программы для электрон-ных вычислительных машин; изобретения; полезные модели; селекционные

достижения; секреты производства (ноу-хау); товарные знаки и знаки обслу-живания; другие активы[1].

Нематериальные активы, как отмечает В. В. Ковалев, не могут возникнуть сами по себе, например, из желания оценить некую «репутацию фирмы», яко-бы создававшуюся в течение многих лет деятельности компании, и провести в активе баланса. Они могут появиться либо в результате покупки, либо как итог собственной деятельности организации[2].

Определяющими признаками объектов нематериального актива юриди-ческого лица являются: наличие документально подтвержденных прав ор-ганизации на приобретение объекта; непосредственное использование объ-екта в основной деятельности организации и его способность приносить доход.

В число нематериальных активов, согласно названному выше положению, могут быть включены расходы, связанные с образованием юридического ли-ца, если они признаны в установленном порядке вкладом в уставный капи-тал[3], а также деловая репутация.

Понятие деловой репутации любого юридического лица, а банка в особен-ности, наиболее рельефно воплощает затраты на ее приобретение (отбор, обу-чение и воспитание персонала, организация профессиональной деятельности, позволяющая добиться получения высокой и устойчивой прибыли, четкое вы-полнение требований законодательства и принципов банковской деятельно-сти, соблюдение принятых банком обязательств и приоритета интересов кли-ента и т. д.).

С другой стороны, вполне очевидна связь между высокой деловой репута-цией банка и получаемыми им доходами. Положительная деловая репутация организации рассматривается как надбавка к цене, уплачиваемая покупателем в ожидании будущих экономических выгод в связи с приобретенными не-идентифицируемыми активами.

Отрицательную деловую репутацию организации следует рассматривать как скидку с цены, предоставляемую покупателю в связи с отсутствием фак-торов наличия стабильных покупателей, репутации качества, навыков марке-тинга и сбыта, деловых связей, опыта управления, уровня квалификации пер-сонала и т. п.

Оценка деловой репутации банка клиентами и партнерами имеет самое не-посредственное отношение к деловым связям банка, как реальным, так и по-тенциальным.

---

[1] Положение по бухгалтерскому учету «Учет нематериальных активов» ПБУ 14/2007, утвер-жденное приказом Министерства финансов Российской Федерации от 27.12.2007 № 153н.

[2] *Ковалев В. В.* Введение в финансовый менеджмент. М.: Финансы и статистика, 1999. С. 151.

[3] В соответствии с Законом об акционерных обществах оценка нематериальных активов стоимостью свыше 200 минимальных размеров оплаты труда, вносимых в качестве вклада в устав-ный капитал, должна проводиться независимыми экспертами.

Именно деловые связи и вытекающие из них договорные отношения при-осят банку реальный доход. На языке финансовых документов денежная ценка деловой репутации представляет собой «разницу между покупной це-ой и оценочной стоимостью имущества», т. е. разницу между ценой только то учрежденного банка и ценой, которую этот банк заработал в процессе воей последующей деятельности.

Наиболее уязвимым объектом из числа нематериальных активов банка яв-яется его деловая репутация. Угрозы деловой репутации могут быть условно азграничены на «внутренние», т. е. исходящие от персонала банка в результа-е проявления некомпетентности, пренебрежения к установленному порядку ункционирования банка либо злого умысла; и «внешние» — порожденные ротивоправными действиями лиц и организаций, недоброжелательных (вра-дебных) банку.

В реальной жизни факторы внутренних и внешних угроз могут комбини-оваться и дополнять друг друга.

Основными источниками возникновения «внутренних» угроз (рисков) для еловой репутации банка являются операционные сбои (под которыми следует онимать несанкционированные изменения содержания и результатов банков-ких операций, наносящие материальный ущерб банку или его клиенту, вслед-твие операционных ошибок либо противоправных действий персонала), нару-ение банком законов и инструкций и других источников права, регулирую-их банковскую деятельность, а также связи с криминальными структурами ли участие в легализации доходов, полученных преступным путем.

Примером такого рода могут служить действия недобросовестных конку-ентов, направивших по месту жительства одного из заемщиков, получившего редит в ОАО «Агрохимбанк», группу вооруженных лиц. Последние, предста-явшись сотрудниками службы охраны банка, требовали возврата долга, срок огашения которого истек накануне, угрожали неправомерными действиями. б этом инциденте банк получил информацию от собственной службы безо-асности, поскольку заемщик, принявший происшедшее за «чистую монету», уководству банка ничего не сообщил. Участники провокации были установ-ены службой безопасности банка. В результате принятых мер ее организато-ы и участники принесли извинения заемщику банка и по собственной ини-иативе компенсировали банку ущерб, причиненный его деловой репутации. происшедшем банк проинформировал правоохранительные органы.

Очернение деловой репутации руководителей банка (или иной организа-ии) характерно для случаев планируемого недружественного поглощения. таких случаях распространенные заранее компрометирующие сведения яв-ются удобным поводом для замены прежнего руководства сразу же после ерехода организации к новым собственникам.

Порочащими деловую репутацию являются, в частности, сведения о якобы мевшем место нарушении действующего законодательства или моральных инципов, стандартов профессиональной деятельности, о просчетах или

нарушениях в сфере производственно-хозяйственной деятельности, которые умаляют деловую репутацию юридического лица[1].

Под распространением указанных сведений следует понимать опубликова-ние их в печати, трансляцию по радио и телевидению, изложение в служеб-ных характеристиках, публичных выступлениях, заявлениях, адресованных должностным лицам, или сообщение в иной, в том числе устной, форме не-скольким или хотя бы одному лицу (за исключением лица, которого они каса-ются).

Нередко целью распространения таких сведений является попытка ограни-чения деятельности конкурента на рынке финансовых (банковских) или иных услуг. В ряде случаев распространенная ложная информация наносит потер-певшему весомый экономический вред, приводит к замораживанию либо пре-кращению отношений с действующими или потенциальными партнерами.

Порочащая информация может носить форму рекомендации не поддержи-вать с банком деловые отношения вследствие его неустойчивого финансового состояния, содержать в качестве подтверждения «фактические данные» о не-устойчивом финансовом состоянии банка, об «астрономических» долгах по налогам, о задолженности перед третьими лицами, о якобы имевшей место описи имущества банка судебным исполнителем, о совершении банком ряда действий, характеризующих его как недобросовестного партнера[2].

К числу действий, способных причинить убытки хозяйствующему субъекту либо нанести ущерб его деловой репутации ст. 14 Федерального закона от 26 июля 2006 г. № 135-ФЗ «О защите конкуренции» (в ред. от 29 апреля 2008 г. № 58-ФЗ) относит распространение ложных, неточных или искаженных сведе-ний, которые могут причинить убытки хозяйствующему субъекту либо нанес-ти ущерб его деловой репутации; введение в заблуждение в отношении харак-тера, способа и места производства, потребительских свойств, качества и ко-личества товара или в отношении его производителей; некорректное сравнение хозяйствующим субъектом производимых или реализуемых им то-варов с товарами, производимыми или реализуемыми другими хозяйствую-щими субъектами;

В марте 2008 г. жертвой измышлений, порочащих деловую репутацию, стал Мурманский филиал «Балтийского банка». В пятницу, 21 марта, неустановлен-ные лица распространяли на предприятиях и организациях, с которыми банк за-ключил договоры на обслуживание по зарплатным банковским картам, слух о предстоящем банкротстве «Балтийского», рекомендуя клиентам незамедлитель-но «забирать деньги из банка». Расчет злоумышленников на формирование

[1] Постановление Пленума Верховного Суда РФ от 18 августа 1992 г. № 11 «О некоторых во-просах, возникших при рассмотрении судами дел о защите чести и достоинства граждан, а также еловой репутации граждан и юридических лиц».

[2] Информационное письмо Президиума Высшего Арбитражного Суда РФ от 23 сентября 1999 г. № 46 «Обзор практики разрешения арбитражными судами споров, связанных с защитой еловой репутации».

ышенного спроса на наличные деньги и создание непредвиденных трудно-
й в работе банка оказался верным. Дело в том, что большинство офисов
еления банка не работает по воскресеньям, а по субботам у них — корот-
й день. В выходные дни наличные деньги были загружены в банкоматы фи-
ала с учетом обычного, а не повышенного спроса. В понедельник мурман-
е офисы банка были переполнены клиентами, снимавшими деньги со сво-
четов.

Для ликвидации проблемы «Балтийскому банку» пришлось получить до-
нительную сумму наличных денег со своего корсчета в территориальном
еждении Банка России и привлечь дополнительных сотрудников для об-
живания клиентов[1].

В настоящее время для распространения порочащих деловую репутацию
дений нередко используется Интернет. Известны случаи, когда для подоб-
к целей распространяются фальшивые версии авторитетных изданий или
формационных агентств, в которых злоумышленники помещают заведомо
кную информацию, порочащую хозяйствующих субъектов.

Возможно также опубликование вымышленных сообщений от имени орга-
ации — объекта посягательства злоумышленников. Такого рода преступ-
е акции уже получили определенное распространение за рубежом. Так, на-
мер, 25 августа 2000 г. на web-сайте Internet Wire (США), специализирующемся
публикации официальных сообщений для прессы, появился пресс-релиз ком-
ии Emulex, производящей сетевое оборудование. От имени названной
пании в нем сообщалось, что якобы понесены значительные потери
квартал, обстоятельства потерь будут изучаться SEC (Securities and Exchange
mmission), а руководитель компании Пауль Фолино (Paul Folino) ушел в от-
вку. Ряд изданий, предоставляющих финансовую информацию в Интер-
, — такие как Dow Jones Newswires, Marketwatch.com, Bloomberg News —
проверив факты, продублировали это сообщение, и в результате паники
ионеров цена акций Emulex снизилась на 62%, что составило потери
2 млрд долл. от их общей стоимости. Впоследствии оказалось, что пресс-
из компании Emulex фальшивый. Такого рода посягательства на репута-
о компаний — не единичный факт. За последние два года от фальшивых
сс-релизов уже пострадали компании PairGain Technologies и Lucent
hnologies[2].

*Противоправные посягательства на деловую репутацию банка могут иметь
ей целью*:

1. Подрыв экономической основы конкурента и в конечном счете прекра-
ие его функционирования.

---

[1] *Петухов Д.* Атака на «Балтийский»? // Полярная правда (Мурманск). 2008. № 40. 25 марта.

[2] *Янишевский Н.* Фальшивка стоимостью в $2 миллиарда // УТРО (ежедневная электронная
а). 2000. 29 авг. (удушито ru)

2. Лишение конкурента поддержки со стороны других организаций и должностных лиц государственных органов.
3. Оказание влияния на принятие арбитражных решений.
4. Давление на руководство банка в связи с предстоящими переговорами и т. д.

Защита нематериальных активов банка, возникающих, из авторских и иных договоров, патентов на изобретения, прав на «ноу-хау» и др. осуществляется в соответствии с авторским либо патентным правом. Методика организации их защиты не имеет существенных отличий от организации защиты материальных активов и поэтому в настоящей работе специально не рассматривается.

В то же время проблема организации защиты деловой репутации банка имеет ряд специфических особенностей. Она ведется по двум основным направлениям. Первое — предупреждение ошибочных либо противоправных действий персонала банка, которые могут причинить ущерб репутации банка (внутренние угрозы). Второе — выявление фактов распространения заведомо ложных сведений, наносящих ущерб репутации банка (внешние угрозы), и возмещение ущерба, причиненного распространением таких сведений.

Задача предупреждения внутренних угроз (рисков) для деловой репутации банка возложена на его службу внутреннего контроля. Кроме того, в этой деятельности в случае необходимости участвует служба безопасности банка. Предписания по организации управления указанными рисками, содержащиеся в Рекомендациях, в основном относятся к проблемам контроля за экономической обоснованностью принимаемых персоналом банка решений, соблюдением установленных законодательством и деловыми обычаями стандартов банковских операций и количественных ограничений (лимитов по суммам рискованных операций).

Организация защиты деловой репутации банка от «внешних» угроз должна предусматривать меры по выявлению в информационных потоках сведений, отрицательно влияющих на деловую репутацию банка, и оценку их достоверности. Наиболее распространенным решением для этого является создание собственного подразделения банка по связям с общественностью.

В случае подтверждения достоверности указанных сведений они используются для устранения либо снижения реально существующих угроз (рисков) репутации банка. Если обнаруживается, что сведения не соответствуют действительности, предпринимаются меры, направленные на защиту деловой репутации банка, способами, предусмотренными Гражданским кодексом РФ, Уголовным кодексом РФ, иными законами и нормативно-правовыми актами Российской Федерации.

Согласно действующему законодательству юридическое лицо, в отношении которого распространены не соответствующие действительности сведения, порочащие его деловую репутацию, имеет право на судебную защиту (ст. 152 ГК РФ) путем возмещения убытков и компенсации морального вреда (ст. 12 ГК РФ).

Иски по делам данной категории вправе предъявить юридические лица, которые считают, что о них распространены не соответствующие действительности порочащие сведения. Ответчиками по искам об опровержении сведений, порочащих деловую репутацию, являются лица, распространившие эти сведения.

В случае распространения порочащих деловую репутацию сведений в средствах массовой информации гражданин или организация вправе требовать от редакции их опровержения в соответствии со ст. 43 Закона РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» (в ред. 24 июля 2007 г. № 211-ФЗ) (далее — Закон о СМИ).

В опровержении, согласно ст. 44 Закона о СМИ, должно быть указано, какие сведения не соответствуют действительности, когда и как они были распространены данным средством массовой информации.

Опровержение в периодическом печатном издании должно быть набрано тем же шрифтом и помещено под заголовком «Опровержение», как правило, на том же месте полосы, что и опровергаемое сообщение или материал.

О предполагаемом сроке распространения опровержения (либо об отказе в его распространении с указанием оснований на то) редакция обязана в письменной форме уведомить заинтересованных гражданина или организацию в течение месяца со дня получения требования об опровержении.

Если требование об опровержении сведений, распространенных в средствах массовой информации, содержатся в судебном иске, в качестве ответчиков привлекаются автор и редакция соответствующего средства массовой информации.

При опубликовании или ином распространении таких сведений без обозначения имени автора (например, в редакционной статье) ответчиком по делу является редакция соответствующего средства массовой информации.

Если же редакция средства массовой информации не является юридическим лицом, к участию в деле в качестве ответчика привлекается учредитель данного средства массовой информации.

В силу ст. 152 ГК РФ обязанность доказывать соответствие действительности распространенных порочащих сведений лежит на ответчике независимо от того, предъявлен иск о защите чести, достоинства, деловой репутации или о возложении на средство массовой информации обязанности в публикации ответа истца. Истец обязан доказать лишь сам факт распространения сведений лицом, которому предъявлен иск.

Весьма эффектным примером защиты своей деловой репутации явились действия ОАО «Альфа-Банк». Сведения, порочащие, по мнению банка, его деловую репутацию, содержались в статье «Банковский кризис вышел на улицу. Системообразующие банки столкнулись с клиентами», опубликованной газетой «Коммерсантъ» 7 июля 2003 г. Статья описывала различные аспекты июльского (2003 г.) кризиса в банковской сфере России, в том числе

и очереди в отделениях Альфа-банка, и опасения вкладчиков банка за доверенные банку деньги.

Сообщалось, в частности, что Московские отделения Альфа-банка были «атакованы клиентами», отделения банка «осаждались» сотнями вкладчиков, которые выстраивались в многочасовые очереди, некоторые отделения банка прекратили работать (в центре сразу несколько отделений были закрыты), а по сообщению некоего источника в банке, «там работал только расчетный центр», в банкоматах банка закончилась наличность, ведется запись клиентов для получения денежных средств на следующие дни. Кроме того, в публикации положение Альфа-банка ставилось в один ряд с Гута-банком, который испытывал в тот период большие финансовые проблемы. (Впоследствии эти утверждения были опровергнуты в суде свидетельскими показаниями, записями камер слежения, справкой об объеме наличных денежных средств, выданных клиентам банка 6 и 7 июля 2003 г., и другими материалами.)

Публикация газеты, по оценке банка, нанесла ущерб его деловой репутации, вызвала необоснованные сложности в работе и повлекла дополнительные расходы. Для оценки своих потерь банк нанял аудиторскую фирму. По подсчетам последней, расходы, возникшие в результате публикации, включили в себя: затраты на проведение банком внеплановой (ответной, реалибитационной) рекламной кампании — 8,4 млн руб.; покупку дополнительных объемов наличных долларов США — 7,4 млн руб.; усиление охраны в офисах банка в Москве — 1,6 млн руб.; дополнительные расходы на увеличение трудозатрат персонала, инкассацию и т. д.

В связи с изложенным ОАО «Альфа-Банк» обратилось в Арбитражный суд Москвы с иском о защите деловой репутации, пресечении действий ответчика ЗАО «Коммерсантъ. Издательский дом» по злоупотреблению свободой массовой информации, взыскании убытков 20 774 366 руб. 61 коп., взыскании репутационного вреда 300 млн руб.

Исковые требования Арбитражным судом Москвы были удовлетворены в полном объеме: сведения, опубликованные газетой «Коммерсантъ», признаны не соответствующими действительности и порочащими деловую репутацию ОАО «Альфа-банк», на ответчика возложена обязанность опубликовать в газете «Коммерсантъ» сообщение о решении Арбитражного суда Москвы в течение 10 дней со дня вступления решения в законную силу. С ответчика в возмещение убытков, причиненных распространением несоответствующих действительности и порочащих деловую репутацию ОАО «Альфа-банк» сведений, взыскана сумма убытков 20 505 906 руб. 69 коп, а также 300 млн руб. в возмещение репутационного вреда, причиненного умалением деловой репутации.

Постановлением Девятого арбитражного апелляционного суда от 27 декабря 2004 г. решение Арбитражного суда Москвы по иску ОАО «Альфа-банк» к ЗАО «Коммерсантъ. Издательский дом» было изменено в части взыскания убытков. С ответчика ЗАО «Коммерсантъ. Издательский дом» в пользу истца

ОАО «Альфа-банк» взыскано 10 895 157 руб. 17 коп. В остальной части решение оставлено без изменения[1].

Предъявление банком иска о защите его деловой репутации не исключает возможности одновременных исков о компенсации морального вреда к ответчику со стороны работников банка в соответствии со ст. 151 и 152 ГК РФ.

Речь идет о тех случаях, когда распространение не соответствующих действительности сведений, порочащих деловую репутацию банка, одновременно причинило вред чести, достоинству или деловой репутации граждан — его сотрудников.

В случае удовлетворения предъявленных исков банк и его сотрудники получают право требовать опровержения таких сведений и возмещения убытков, а физические лица — еще и компенсации морального вреда, явившегося результатом распространения ложной информации.

В тех случаях, когда действия лица, распространившего порочащие деловую репутацию банка сведения, содержат признаки клеветы или оскорбления в отношении конкретных его сотрудников, потерпевшие, наряду с предъявлением иска о защите чести и достоинства и деловой репутации в порядке гражданского судопроизводства, вправе обратиться в суд с заявлением о привлечении виновного к уголовной ответственности за совершение преступлений, предусмотренных ст. 129 или ст. 130 УК РФ.

На требование о защите чести, достоинства, деловой репутации, заявленное в порядке ст. 152 ГК РФ, исковая давность (в силу ст. 208 ГК РФ) не распространяется[2].

Закон, как известно, освобождает потерпевшего от обязанности доказывать ложность распространенных сведений и от установления их источника (если он неизвестен). Однако участие банка в сборе соответствующей информации и подготовке ее к рассмотрению в правоохранительных и судебных органах не исключается. Весьма важное значение для достижения целей возмещения ущерба деловой репутации имеет квалифицированный подход истца к расчету и обоснованию денежной составляющей вреда, а также к сбору и фиксации будущих судебных доказательств. Указанные выше задачи могут быть возложены на службы, обеспечивающие безопасность банка и юридическое сопровождение его деятельности.

---

[1] Постановление Девятого арбитражного апелляционного суда г. Москвы № 09АП-6183/04-ГК. 31 декабря 2004 г.

[2] Постановление Пленума Верховного Суда РФ от 18 августа 1992 г. № 11 «О некоторых вопросах, возникших при рассмотрении судами дел о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц».

ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. В чем заключается суть злоупотребления полномочиями?
2. Лица какой категории могут стать субъектами злоупотребления полномочиями?
3. В чем состоит особенность возбуждения уголовного дела по ст. 201 УК РФ?
4. В каких формах осуществляются меры предупреждения злоупотреблений?
5. Какие деяния рассматриваются как коммерческий подкуп?
6. Для каких категорий лиц ст. 204 УК РФ установлена уголовная ответственность?
7. Каково содержание мер предупреждения коммерческого подкупа?
8. Каким условиям должны соответствовать сведения, чтобы получить правовой статус банковской или коммерческой тайны?
9. Какие меры должен принять обладатель информации для того, чтобы она стала объектом правовых отношений?
10. Какие основные способы незаконного получения банковской тайны предусмотрены ст. 183 УК РФ?
11. Какие этапы должна включать в себя организация защиты банковской тайны?
12. От каких видов преступных посягательств защищает компьютерную информацию Уголовный кодекс РФ?
13. Какие основные направления защиты информации должен реализовать банк?
14. По каким основным направлениям осуществляется защита кадрового состава банка?
15. Как определить цену деловой репутации банка в денежном исчислении?
16. Какими способами и с какими целями совершаются противоправные посягательства на деловую репутацию?
17. Какие способы правовой защиты деловой репутации предусмотрены законодательством России?

Глава 8

ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ ОТМЫВАНИЮ ПРЕСТУПНЫХ ДОХОДОВ И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА

- Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем
- Криминалистическая характеристика легализации (отмывания) преступных доходов
- Система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма

8.1. Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем

Проблема противодействия отмыванию преступных доходов была впервы зафиксирована на законодательном уровне Соединенными Штатами Америк в 1986 году в качестве меры борьбы с незаконным производством и оборот наркотиков. Речь идет о *Постановлении о контроле над отмыванием денег (MLC* вошедшем в качестве параграфа № 1 в Постановление о борьбе с наркоман ей, принятом в 1986 г. Названный акт признал преступными два новых ви деяний.

1. Участие в финансовых операциях и международных перемещениях (п реводах) средств или собственности, добытой конкретным видом незаконно деятельности (SUA).

2. Осуществление переводов денежных средств, полученных в качест выручки от конкретного вида незаконной деятельности на сумму 10 тыс. долл Раздел 1353 данного постановления стал дополнением к постановлени о Праве на конфиденциальность финансовой информации от 1978 г., уполно мочив финансовые учреждения предоставлять соответствующим правительст венным органам информацию о подозрительных финансовых операциях, дл чего стало необходимо заполнять форму отчета о преступной деятельност Данным Постановлением введены правила, согласно которым «любое лицо участвующее в деловых или торговых отношениях и получившее более 10 тыс. долл. наличными в рамках одной финансовой операции или ряда свя занных финансовых операций, должно предоставить отчет по форме налого вой службы США (форма 8300)».

Уголовное право России впервые признало легализацию (отмывание) «грязных» денег преступлением путем включения в Уголовный кодекс РФ ст. 174 (Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем). Впоследствии Уголовный кодекс РФ был дополнен ст. 174.1 (Легализация (отмывание) денежных

средств или иного имущества, приобретенных другими лицами преступным путем)[1].

Криминализации отмывания в отечественном законодательстве предшествовало подписание Российской Федерацией в г. Будапеште 7 мая 1999 г. Конвенции государств — членов Совета Европы и других государств (Конвенция Совета Европы), об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности от 8 ноября 1990 г. Названная Конвенция была ратифицирована в 2001 г.[2]

В кратчайшие сроки после ратификации Конвенции в Российской Федерации были созданы нормативная правовая база и организационная система, позволившие вывести работу по противодействию легализации преступных доходов на уровень международных стандартов. Об этом свидетельствовало принятие в июне 2002 г. Комитета по финансовому мониторингу (ныне преобразованного в Федеральную службу финансового мониторинга) в Группу Эгмонт — международную организацию, объединяющую подразделения финансовой разведки 69 стран мира[3].

Согласно российскому законодательству *легализация (отмывание) доходов, полученных преступным путем,* представляет собой инструмент финансового обеспечения опасных форм преступности и сама по себе, согласно ст. 15 УК РФ, относится к категории тяжких преступлений. Наибольшую опасность представляет легализация преступных доходов с целью финансирования терроризма.

С точки зрения права легализация (отмывание) денежных средств или иного имущества, приобретенных преступным путем (далее — денежных средств) означает придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления.

Основными целями легализации денежных средств являются:

а) маскировка источника их происхождения и принадлежности;

б) придание преступной наживе видимости средств, полученных из законных источников;

---

[1] Введена Федеральным законом от 7 августа 2001 г. № 121-ФЗ «О внесении изменений и дополнений в законодательные акты Российской Федерации в связи с принятием Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем».

[2] Федеральный закон от 28 мая 2001 г. № 62-ФЗ «О ратификации Конвенции об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности».

[3] Подразделения финансовой разведки (FIU) — это специальные ведомства, создаваемые с целью борьбы с отмыванием денег. Объединение указанных ведомств в международную структуру под названием группы Эгмонт состоялось в 1995 году в Брюсселе (во время встречи во дворце Эгмонт-Аренберг). Отделы FIU проводят регулярные встречи для обмена информацией и опытом. Международная Интернет-система безопасности Егмонт предоставляет членам группы возможность доступа и обмена информацией о тенденциях, механизмах и технологиях аналитического расследования. Правоохранительные органы Соединенных Штатов имеют возможность запросить информацию у иностранного отдела FIU посредством официального заявления офицеру связи своего ведомства либо непосредственно в Управление международных программ FinCEN. Отдел финансовой разведки, с которым можно связаться по телефону (703) 905–3823; или по факсу (703) 905–3679.

в) возможность финансового обеспечения других видов преступной деятельности за счет легализованных денежных средств с использованием легальных банковских операций.

Для достижения указанных целей используются различные банковские операции, реализуются многоходовые финансовые схемы (порой весьма запутанные).

С точки зрения уголовного права понятием «легализация (отмывание) денежных средств» охватываются два самостоятельных состава преступления. Первый из них предусматривает уголовную ответственность лиц, совершающих финансовые операции и другие сделки с денежными средствами или иным имуществом *других субъектов*, которое последние приобрели заведомо преступным путем (ст. 174 УК РФ). Второй — устанавливает наказание в отношении тех лиц, которые приобрели денежные средства или иное имущество *непосредственно в результате совершения преступлений* (ст. 174.1 УК РФ).

Из числа указанных действий законодатель исключил деяния, предусмотренные ст. 193, 194, 198 и 199 УК РФ (преступления в сфере таможенного дела и в области налогового законодательства).

Обязательным условием наступления уголовной ответственности по ст. 174 и 174.1 УК РФ является крупный размер операций и сделок, пороговым значением которого является сумма, превышающая две тысячи минимальных размеров оплаты труда.

Действия уполномоченных лиц коммерческих банков, направленные на легализацию преступных доходов других лиц под видом банковских операций, совершенные в крупных размерах, влекут за собой уголовную ответственность по ст. 174 УК РФ.

Максимальное наказание, предусмотренное ч. 1 ст. 174 УК РФ, — лишение свободы на срок до четырех лет со штрафом в размере до ста минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до одного месяца.

Квалифицирующие (отягчающие) признаки отмывания денежных средств предусмотрены ч. 2 ст. 174 УК РФ (те же деяния, совершенные: а) группой лиц по предварительному сговору; б) неоднократно; в) лицом с использованием своего служебного положения) и ч. 3 ст. 174 УК РФ (деяния, предусмотренные частями первой или второй настоящей статьи, совершенные организованной группой).

Максимальное наказание, предусмотренное ч. 2 ст. 174 УК РФ, — лишение свободы на срок до шести лет; ч. 3 названной статьи — лишение свободы на срок до восьми лет.

Действия тех лиц, которые приобрели денежные средства или иное имущество путем личного участия в совершении преступлений и совершают с ними финансовые операции и другие сделки в крупном размере, либо используют указанные средства или иное имущество для осуществления предпринимательской

или иной экономической деятельности, влекут за собой уголовную ответственность по ст. 174.1 УК РФ.

Максимальное наказание, предусмотренное ч. 1 ст. 174.1 УК РФ, — лишение свободы на срок до пяти лет со штрафом в размере до ста минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до одного год.

Квалифицирующие (отягчающие) признаки отмывания денежных средств предусмотрены ч. 2 ст. 174.1 УК РФ (те же деяния, совершенные: а) группой лиц по предварительному сговору; б) неоднократно; в) лицом с использованием своего служебного положения) и ч. 3 ст. 174 УК РФ (деяния, предусмотренные частями первой или второй настоящей статьи, совершенные организованной группой).

Максимальное наказание, предусмотренное ч. 2 ст. 174.1 УК РФ, — лишение свободы на срок до восьми лет; ч. 3 ст. 174.1 УК РФ — лишение свободы на срок до пятнадцати лет.

Под финансовыми операциями и другими сделками, указанными в ст. 174 и 174.1 УК РФ, следует понимать действия с денежными средствами, ценными бумагами и иным имуществом (независимо от формы и способов их осуществления, например, договор займа или кредита, банковский вклад, обращение с деньгами и управление ими в задействованном хозяйственном проекте), направленные на установление, изменение или прекращение связанных с ними гражданских прав или обязанностей.

При этом по смыслу закона ответственность по ст. 174 УК РФ или по ст. 174.1 УК РФ наступает и в тех случаях, когда виновным лицом совершена лишь одна финансовая операция или одна сделка с приобретенными преступным путем денежными средствами или имуществом.

Для решения вопроса о наличии состава преступления, предусмотренного ст. 174 УК РФ, необходимо установить, что лицо совершило указанные финансовые операции и другие сделки с денежными средствами или иным имуществом в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом[1].

Изменения форм денежных средств в процессе легализации (отмывания). Легализация (отмывание) денежных средств, полученных преступным путем, сопряжена с изменением форм денежных средств в двух направлениях:

а) путем обращения наличных денег в безналичные, в иностранную валюту или другие активы;

б) путем обращения безналичных денег в наличные.

Первое направление используется для введения в легальную финансовую систему денежной массы, полученной в результате организованной преступной деятельности (торговли наркотиками, оружием, вымогательства, коррупции и т. п.).

[1] Постановление Пленума Верховного Суда РФ от 18 ноября 2004 г. № 23 «О судебной практике по делам о незаконном предпринимательстве и легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем».

Например, в ходе расследования уголовного дела по факту незаконного сбыта наркотических средств было установлено, что рублевая наличность, полученная преступным путем, обменивалась под видом легальных доходов лжекоммерческой организации (афганской фирмы) на доллары США в АКБ «Русские национальные традиции». При этом как обменные операции, так и выдача справок на вывоз валюты за границу совершались с нарушениями установленного порядка[1].

Согласно данным правоохранительных органов США, основная проблема преступников, извлекающих наживу в форме наличных денег, связана с большой опасностью их хранения и трудностью перемещения. Поэтому главной целью становится перевод наличных денег в безналичные либо в платежные документы и ценные бумаги.

В частности, 2 млн долл. в купюрах 20 долл. весят 112 кг. Доход от наркоторговли измеряется в буквальном смысле слова тоннами денежных знаков. В практике спецслужб США имели место случаи обнаружения подвалов, доверху в рост человека, забитых пачками валюты. В результате проведения операции с условным названием *Ла Мина* — «Золотой прииск», было установлено, что организация прикрытия, выступавшая под видом магазина ювелирных изделий в Лос-Анджелесе, отмывала для Колумбийских наркобаронов более 2 млн долл. в день, а всего за 18 месяцев отмыла 1,2 млрд долл. В этом свете становятся очевидными преимущества «виртуальных» денег, в том числе их хранения и перемещения.

После перевода наличных денег в безналичные они могут использоваться для финансирования других видов преступной деятельности либо в иных регионах. В частности, безналичные электронные переводы денежных средств, предназначенных для финансирования особо тяжких преступлений, широко используют террористы. Об этом свидетельствуют результаты расследования терактов 11 сентября 2001 г. в США, раскрывшие структуру финансового обеспечения указанных преступных действий[2].

Второе направление обращения денег чаще всего используется для получения денежных средств коммерческих и бюджетных организаций.

Так, например, Калининградская железная дорога (КЖД) в начале 2004 г. перечислила ФГУП «Ростехинвентаризация» 16 млн бюджетных рублей в оплату работ, выполненных калининградским филиалом названной организации. Деньги поступили на счет ФГУПа в Москве, однако до исполнителя работ не дошли. В ходе расследования уголовного дела, возбужденного по заявлению руководителя филиала, было установлено, что названная сумма была направлена из Москвы на счет некоей фирмы, которая в свою очередь перечислила их другой коммерческой организации. При этом в платежных документах был изменен адресат, источник происхождения и назначение платежа.

[1] Уголовное дело № 142 019 // Архив Арбитражного суда Москвы.

[2] Доклад Федерального бюро расследований Конгрессу США, приводимый в прошлогоднем отчете ФАТФ (http://www.fbi.gov/congress02/lormel021 202.htm).

В итоге деньги оказались на счету частного предпринимателя из Ленинградской области, в одном из петербургских отделений Сбербанка России. В ходе расследования этого дела специалисты Росфинмониторинга проверили счет злоумышленника предпринимателя, и оказалось, что за период с апреля 2004 г. по май 2005 г. через этот счет было обналичено 15 млрд руб.[1]

Согласно закону в тех случаях, когда лицо приобрело денежные средства или иное имущество в результате совершения преступления и легализовало (отмыло) их путем совершения операций, имеющих целью придание правомерного вида владению, пользованию или распоряжению похищенным, содеянное этим лицом подлежит квалификации по совокупности преступлений (например, описанные выше действия были квалифицированы как мошенничество (ст. 159 УК РФ) и как легализация (отмывание) денежных средств или иного имущества, приобретенных лицом, в результате совершения им преступления (ст. 174.1 УК РФ)).

Переводы крупных сумм безналичных денег под видом благотворительных акций использовали в 2004 г. с целью хищения денежных средств компании «Юкос» и легализации преступных доходов два менеджера названной компании. Денежные средства, поступившие на благотворительные цели в организации инвалидов и спортсменов, получателями обращались в наличность. После этого большая их часть по сговору менеджеров с руководителями организаций-получателей возвращалась организаторам преступления.

Очевидным признаком отмывания похищенных бюджетных денег явились случаи, обнародованные пресс-центром МВД России. Так, в г. Снежинске Челябинской области в 2004 г. два человека по доверенности от пенсионерки, получили по векселям 2 млрд руб.

8.2. Криминалистическая характеристика легализации (отмывания) преступных доходов

С точки зрения криминалистики основными признаками механизма легализации (отмывания) преступных доходов являются маскировочные действия его участников. Это не удивительно, поскольку маскировка (происхождения денег, причастных лиц и т. д.) составляет суть преступления указанного вида в целом.

Маскировочные действия преступников заключаются в сокрытии или искажении подлинной информации:

- об участниках операций с денежными средствами или имуществом, путем использования лжекоммерческих (фиктивных) организаций и подставных физических лиц;
- о подлинном происхождении денежных средств, полученных в результате преступной деятельности (придание им видимости легальной принадлежности), были в результате производственной, финансовой и иной деятельности, получения кредитов и т. п.);

[1] *Макаров И.* Пыльные [illegible] отходя от кассы // Коммерсантъ. 2005. 27 июля.

- о подлинном смысле совершаемых операций, сделок и проводок и конечном получателе денежных средств (путем сокрытия данных в массиве банковской технологической информации).

Весьма удобный механизм для легализации (отмывания) преступных доходов представляют собой коммерческие предприятия, особенно те, в которых расчеты осуществляются в основном наличными деньгами. Особенности организации их деятельности позволяют скрыть личность настоящего владельца капитала, а также оказывать финансовую поддержку другим преступным структурам.

Личность истинного владельца предприятия может быть скрыта посредством «подставных» лиц. Преступники могут использовать несколько коммерческих предприятий, чтобы запутать или скрыть отчетность по документам о соответствующей деятельности путем перевода средств из одной организации в другую, чтобы отследить их было сложнее.

Самым простым вариантом маскировки происхождения преступных доходов с использованием возможностей финансовых учреждений является обмен мелких купюр на более крупные. Для реализации более сложных способов могут быть задействованы банковские счета, электронные переводы денег, обмен наличности на чеки и прочие инструменты обмена, а также другие банковские механизмы, как, например, аккредитив.

В целях маскировки оснований совершаемых банковских транзакций составляются мнимые кредитные договоры, договоры на проведение работ, оказание услуг, поставку товаров и т. п.

Несмотря на предпринимаемые преступниками усилия, маскировка противоправной деятельности не может полностью скрыть ее следы в силу объективно возникающих (и отражающихся в документах) противоречий между истинной и ложной (маскировочной) информацией. В этой связи сделки приобретают вид необычных, подозрительных.

Указанные противоречия и выявленные на их основе факты маскировки подлинного содержания информации являются признаками, свидетельствующими с определенной степенью вероятности, о наличии события преступления «отмывания». Вероятность наличия события «отмывания» в проверяемой сделке возрастает в случае обнаружения нескольких признаков маскировки, относящихся к различным, связанным с ней обстоятельствам.

Типичные способы сокрытия или искажения подлинной информации об участниках операций с денежными средствами или имуществом

Наиболее распространенным способом маскировки подлинных участников отмывания» является создание лжекоммерческих организаций, выступающих качестве фирмы-прикрытия, от имени которой совершаются операции (сделки) по отмыванию преступных доходов. Использование фирмы-прикрытия затрудняет раскрытие преступления и привлечение преступников к ответственности в случае установления причастных аферe лиц.

Для указанного способа сокрытия информации о подлинных участниках преступления характерны следующие признаки маскировки.

1. В качестве учредителей и руководителей организации выступают подставные физические лица (физическое лицо), *возрастная и социальная характеристики* которых существенно отличается от референтной группы. Как правило, эти характеристики дают основания полагать, что формально значащиеся учредители не связаны с реальными интересами дела.

По возрастному составу:

- молодые лица;
- пожилые лица;
- объединение молодых и пожилых субъектов в качестве учредителей организации.

По социальным показателям:

- состоящие на учете в качестве безработных;
- не имеющие определенного места жительства;
- являющиеся руководителями нескольких организаций одновременно. В практике работы ФСФМ России известны лица, являющиеся, согласно официальным учетам, руководителями десятков организаций одновременно[1].

2. Фирма учреждена без реального участия физического лица, указанного в документах.

В данном случае речь идет о случаях, когда организация учреждается по утерянному либо похищенному паспорту.

3. Фактический адрес организации неизвестен.

В этом случае строения с указанным адресом может не существовать вовсе, либо оно существует, но проверяемой организации в нем нет.

4. Отсутствует стационарная телефонная связь с организацией.

Указанный в документах организации стационарный телефон принадлежит посреднику (диспетчеру) либо отсутствует вовсе. Для связи используется сотовый телефон.

5. Отсутствует прямая почтовая связь с организацией.

Для обмена корреспонденцией в таких случаях используется абонентский ящик либо посредник (почтовый пункт).

6. Наличие противоречий в официально сообщаемых данных о реквизитах фирмы и о ее руководителях.

В число этих признаков входят:

- недействительный ИНН, либо его принадлежность другому лицу;

[1] Так, некая фирма «Коматек», предлагавшая через Интернет услуги по «обналичиванию» денежных средств, была зарегистрирована по одному адресу с другими десятью «фирмами». А ее директор, Е. Полякова, одновременно возглавляла несколько компаний. Информация об указанных особенностях «Коматек» и ряда других организаций с признаками лжекоммерческих организаций поступила в 2006 г. в банки Москвы из Налоговой инспекции ФНС

- не соответствующее действительности указание на организ
  правовую форму фирмы (ОАО, ЗАО и проч.).
- расхождение данных о руководителях организации, содержащ
  кументах, относящихся к одному и тому же периоду времени.

7. Минимальный (либо фиктивный) уставный фонд организации
   - заметно ниже размеров уставного фонда организаций реф
     группы (группы сходных организаций, выбранных для срав
   - внесен в неденежной форме, затрудняющей его подлинну
     (оргтехника, мебель, интеллектуальная собственность и пр
8. Краткосрочность существования фирмы.

Как правило, период существования фирмы ограничен временем
ления отчетных документов в налоговые органы (3–4 месяца). О
признак отсутствует у «прачечных», созданных «на перспективу».

9. Указание на организационные и деловые связи с фирмам
ность которых уже установлена.

В частности, организация, фиктивность которой уже установл
быть названа в качестве учредителя (соучредителя) или деловог
проверяемой организации.

Типичные способы сокрытия или искажения информации о подлинном происхождении денежных средств, полученных в результате преступной деятельности

Подлинное происхождение денежных средств, полученных
путем, маскируется имитацией легальной коммерческой деяте
финансовых операций. Для указанных целей избираются виды д
не требующие затрат на персонал, обеспечивающие инфрастру
материалы и т. д.

Известны *два основных вида имитации производственной и
деятельности*.

1. Случаи, когда деятельность не проводится вовсе.

Характерными признаками первого вида являются:

- необычно широкая номенклатура деятельности (напри
  высокотехнологичными изделиями совмещается с торгов
  ми плитами (или их изготовлением), тут же присутствует
  теллектуальных услуг);
- потоки товаров, приобретаемых у одних контрагентов и
  другим контрагентам, «не стыкуются» по номенклатур
  кирпичи, продается электронная техника;
- отсутствуют реальные условия (персонал, площадь, обор
  заявленного вида деятельности.

Возникшие подозрения можно проверить путем сравнения
и количества сделок и услуг с референтной группой. Кроме т

сти выборку сведений о номенклатуре товаров, якобы поступивших
рму и якобы поставленных контрагентам (цель выборки — обнаружить
езнувшие в никуда» либо «возникшие ниоткуда» товары). Сведения о ко-
стве персонала, наличии производственных и складских площадей, обо-
нии, необходимые для целей проверки, можно получить в стоимостном
хении из баланса по итогам года.

Коммерческая деятельность имитируется мнимым оказанием интеллек-
ных, маркетинговых и т. п. услуг.

рактерными признаками второго вида являются следующие обстоятельства:
интеллектуальные услуги не могут быть оказаны получателем средств
в силу объективных причин (отсутствия персонала, несоответствия ква-
лификации персонала);
казчик не нуждается в оказании ему заявленных интеллектуальных
слуг, поскольку они не соответствуют профилю его деятельности и ре-
льным потребностям;
особычайно высокая цена оказанных услуг. Возникшие подозрения
ожно проверить путем изучения характера деятельности организаций,
оторым проверяемая фирма оказывала «интеллектуальные услуги», со-
поставления профиля их деятельности с реальными потребностями
интеллектуальных услугах конкретных видов;
борка данных о персонале фирмы с целью проверки его способности
казывать интеллектуальные услуги. Кроме того, следует провести вы-
рку средней стоимости видов интеллектуальных услуг (в референтной
руппе) с целью установления неоправданных отклонений в оплате ус-
г проверяемой фирмы.

имер, в ходе проверочных мероприятий Росфинмониторинг выявил
т, по которому отечественная коммерческая организация перевела
нной фирме за якобы проведенное маркетинговое исследование рын-
етных изделий в одной из областей России около 500 тыс. долл. Со-
окументам, контракт был выполнен в течение трех дней. Выборка
цены аналогичных услуг показала, что ведущие отечественные и зару-
консалтинговые компании готовы выполнить указанную работу
роки за плату от 1000 до 3000 руб.[1]

ичные признаки сокрытия или искажения подлинной информации, ощиеся в экономических показателях и бухгалтерских документах фирм, имитирующих коммерческую деятельность

м главным из названных признаков является необычно низкая рента-
ь фирмы-«прачечной», которая составляет приблизительно 1% при
льно большом движении денег по счетам. Низкие показатели

[1] ыступления Ю. Ф. Короткого на заседании Межрегионального банковского совета Федерации 15 ноября 2007 г.

прибыли и рентабельности объясняются рыночной ценой, которую на черном рынке платят за процедуру «отмывания». В реальной жизни коммерческая деятельность с такими показателями лишена экономического смысла.

Для организаций указанного вида характерен необычно большой оборот денежных средств с самого начала деятельности (как правило, оборот нарастает постепенно). Резкий «старт» свидетельствует о том, что денежный оборот не связан с реальной коммерческой деятельностью.

При внимательном рассмотрении обнаруживается противоречие между ростом объема якобы выполненных организацией работ (оказанных услуг) и расходами на зарплату персоналу (отсутствует движение по счетам, связанное с выплатой зарплаты: деньги со счета не снимаются.

Кроме того, сведения о налоговых платежах отсутствуют вовсе либо платежи явно не соответствуют размерам указанного в документах оборота.

Для проверки возникших подозрений можно провести сравнительный анализ деятельности фирм, рентабельность которых не выше 1, 2, 3%; провести выборку организаций с необычно высокими показателями оборота денежных средств с самого начала деятельности (предварительно установить временной шаблон, определить обычный уровень показателей, затем выявить организации с отклонениями); проанализировать особенности деятельности организаций, у которых показатели объема выполненных работ возросли при одновременном снижении расходов на персонал (отсутствует движение по счетам, связанное с выплатой зарплаты: деньги со счета не снимаются); выявить организации, у которых приведенные показатели значительно отличаются от референтной группы; провести выборку организаций, сведения о налоговых платежах которых отсутствуют, либо платежи явно не соответствуют размерам оборота.

Типичные признаки, свидетельствующие об отсутствии реальной производственной деятельности. В приводимом ниже перечне указываются так называемые *негативные признаки, которые не могут присутствовать в бухгалтерских документах фирмы-«прачечной»* по причине отсутствия самой деятельности и связанных с ней обстоятельств. К числу «отсутствующих» относятся следующие показатели бухгалтерской отчетности:

- фонды социальной сферы на конец года;
- резервы, образованные в соответствии с учредительными документами на конец года;
- резервы, образованные в соответствии с законодательством на конец года;
- добавочный капитал на конец года;.
- основные фонды;
- собственные акции, выкупленные у акционеров на конец года;
- затраты в незавершенном производстве (издержки обращения) на конец года и само незавершенное производство;
- инвестиции в другие организации;
- инвестиции в зависимые общества;

- инвестиции в дочерние общества на начало года;
- здания, машины и оборудование на начало года;
- затраты на оплату труда (отсутствуют либо необычно низкие);
- штрафы, пени и неустойки, признанные или взысканные по решению суда;
- резервы предстоящих расходов на начало года;
- доходы будущих периодов на начало года;
- расчеты с учредителями;
- кредиты у банков (их «прачечная» не берет, избегая связанных с выдачей кредитов проверок);
- задолженность перед персоналом организации на конец года;
- кредиторская задолженность на конец года;
- подотчетные суммы не выдаются.

Типичные способы сокрытия или искажения информации о подлинном смысле совершаемых операций

Указанные способы классифицируются по видам декларируемых источников получения денежных средств, в числе которых чаще всего встречается следующее.

1. Получение денежных средств под видом «кредита». В действительности указанным способом легализуются через соучастника «кредитора» денежные средства мнимого заемщика. При этом проявляются вероятные признаки «отмывания»:
   - отсутствие у получателя кредита вторичных источников обеспечения долга (денежных средств на других счетах, товаров на складе и в обороте, сырья, основных фондов и проч.);
   - отсутствие у получателя кредита легальных средств для его погашения (получатель «кредита» не ведет и не вел коммерческой деятельности, приносившей ему доход; для этого он не имеет объективных возможностей);
   - в погашение кредита заемщика поступают денежные средства из неизвестных источников;
   - фальсификация вторичного источника погашения долга; поднятие цены на объект залога путем его неоднократных перепродаж в короткий период времени одними и теми же лицами по все более высокой цене;
   - предоставление в качестве залога имущества, уже находящегося в залоге.

Для проверки достоверности сведений о якобы полученном кредите возможно использование методов выборки:

- по соответствующим базам данных и проверки финансовых документов с целью выявления среди получателей кредита субъектов, не имеющих денежных активов, основных фондов, товаров на складе и в обороте

- по соответствующим базам данных с целью выявления среди получателей кредита субъектов, не имеющих ресурсов для ведения реальной коммерческой деятельности (основных фондов, оборудования, персонала и проч.);
- данных об операциях с предметом залога, с целью установления начальной и конечной цены в течение определенного промежутка времени; установления подлинного круга и ролей лиц, участвующих в неоднократных перепродажах объекта в качестве продавцов, покупателей и агентов (выбрать одни и тех же объекты неоднократных перепродаж за короткое время, а также объекты, цена которых чрезмерно возросла (за необычно короткое время); отбрасывать объекты, фигурирующие менее чем в трех транзакциях (установление ограничений, степени расширения связей);
- из информационных массивов, содержащих сведения о договорах кредитования, данных о предметах залога, уже находящихся в залоге на момент заключения нового договора;
- с целью установления скрытых связей между заемщиком и неизвестным источником погашения его долга.

2. Получение денежных средств под видом прибыли от операций с ценными бумагами. В действительности указанным способом через соучастников по «операциям» легализуются денежные средства. При этом появляются следующие вероятные признаки «отмывания»:

- операции неоднократно заключаются с одним или несколькими контрагентами и приносят постоянный доход или постоянный убыток (что лишает их явного экономического смысла для одной из сторон сделок);
- регулярные операции по покупке и последующей перепродаже ценных бумаг, не имеющих котировок, не обращающихся на организованном рынке ценных бумаг с использованием дохода для приобретения высоколиквидных ценных бумаг;
- многократная продажа и покупка одних и тех же ценных бумаг (не размещенных в депозитарии) в сделках с одной и той же стороной.

Для проверки возникших подозрений в маскировке подлинной сути информации возможно использование методов выборки:

- повторяющихся операций, участниками которых являются одни и те же субъекты (или их связи);
- повторяющихся операций, которые приносят постоянный доход или постоянный убыток;
- повторяющихся операций по покупке и перепродаже ценных бумаг, не имеющих котировки;
- субъектов, получающих постоянный доход от операций по перепродаже ценных бумаг, не имеющих котировки и направляющих полученную выручку на скупку высоколиквидных ценных бумаг;

- субъектов, являющихся сторонами в многократной продаже и покупке одних и тех же ценных бумаг (не размещенных в депозитарии).

Типичные способы использования банковских операций с целью маскировки подлинного направления переводов и адресатов получения денежных средств, добытых преступным путем

1. Умышленное дробление суммы, внесенной на банковский счет, путем переводов денежных средств по частям на счета других субъектов (так называемое структурирование платежей).

Владелец счета дает банку поручения о переводе денег на счета указанных им субъектов. Получатели указанных средств в свою очередь переводят их на счета третьих лиц и т. д. Характерными особенностями использования переводов в целях отмывания преступных доходов является использование для осуществления транзакций подставных лиц и направление денежных средств через ряд различных финансовых организаций таким образом, чтобы безналичные переводы казались исходящими из разных и на вид не связанных друг с другом источников.

Подлинный смысл операции заключается в том, что указанная сумма после прохождения многочисленных расчленений аккумулируется на одном или двух счетах подлинных адресатов.

Механизм структурирования платежей в целях замаскировать хищение, легализовать доходы, полученные преступным путем, может быть проиллюстрирован следующим примером.

Генподрядчик строительства МКАД ОАО «Корпорация трансстрой» за 1995–1998 гг. перечислила субподрядчику СУ-802 на проведение работ 1 трлн руб. Часть указанной суммы в размере 20 408 млрд руб. была похищена сотрудниками СУ-802 и перечислена ООО «Фобос». Затем 20 408 млрд руб. были «структурированы» путем перечисления плательщиком ООО «Фобос» коммерческим организациям: ЗАО «216 УСМР»; ООО «Сырье и ресурсы» и ООО «Паритет», ООО «Трасса-Д» и ЗАО «Магистраль». Названые получатели денежных средств в свою очередь перевели большую их часть на счета физических лиц в более 50 иностранных банков. А 55 млрд руб. были истрачены на покупку векселей «Западно-сибирской инвестиционной компании»[1].

Эффективным методом проверки возникших подозрений является выборка данных о взаимосвязанных банковских операциях, логическое восстановление разорванных финансовых потоков.

Результаты выборок, полученных в ходе проверок по указанным выше шаблонам (моделям), следует подвергнуть дополнительному анализу. Новая выборка должна быть направлена на выявление различных видов маскировки

[1] Материалы международной конференции «Международное

у одних и тех же субъектов. Взаимное «наложение» признаков повысит степень обоснованности первоначально возникших подозрений в «отмывании».

В целях подтверждения подозрений следует провести дополнительную проверку в рамках финансового расследования. Дальнейшие выводы о наличии события преступления относятся к компетенции следствия и суда.

8.3. Система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма

Отечественная система мер, направленных на противодействие легали... ции (отмыванию) преступных доходов, формируется на основе Закона о пр... тиводействии легализации преступных доходов.

Цели противодействия достигаются путем реализации двух основных ме... дов:

а) финансового контроля;

б) правового воздействия.

Обязанность организовать функционирование подсистемы финансов... контроля возложена ст. 8 Закона о противодействии легализации преступ... доходов на ФСФМ России. Названная служба является федеральным орган... исполнительной власти, осуществляющим функции по противодействию ... галлизации (отмыванию) доходов, полученных преступным путем, и финан... рованию терроризма и координирующим деятельность в этой сфере иных ф... деральных органов исполнительной власти[1].

Функции методического руководства и координации деятельности кред... ных организаций Закон о противодействии легализации преступных дохо... отнес к компетенции Банка России.

Финансовый контроль осуществляется в целях сбора информации, необ... димой для выявления фактов противоправной деятельности, их предварите... ной проверки, оценки и возможного направления материалов в правоохра... тельные органы.

Правоохранительные органы рассматривают поступившие материалы ф... нансового контроля в качестве основания для принятия по ним решен... в рамках уголовно-процессуального кодекса.

Законодательство не устанавливает административной ответственности ... совершение сделок и операций, направленных на легализацию (отмыван... преступных доходов. Однако неисполнение банком предписаний Закона о пр... тиводействии легализации преступных доходов, полученных преступным п... тем, и финансированию терроризма в части фиксирования, хранения и пре... тавления информации об операциях, подлежащих обязательному контро...

[1] Детальной регламентации полномочий и порядка функционирования самой ФСФМ Р... ии посвящено Положение о Федеральной службе по финансовому мониторингу, утвержден... остановлением Правительства Российской Федерации от 23 июня 2004 г. № 307.

а также в части организации внутреннего контроля рассматривается как адм... нистративное правонарушение и служит основанием для наложения админ... стративного штрафа: на должностных лиц — в размере двухсот минимальн... размеров оплаты труда, на юридических лиц — в размере пяти тысяч мин... мальных размеров оплаты труда (п. 3 ч. 1 ст. 3.5 КоАП РФ).

Административные расследования в сфере противодействия легализац... (отмыванию преступных доходов) проводятся уполномоченными ФСФМ Ро... сии исключительно в целях выявления и пресечения фактов нарушений поряд... ка функционирования системы финансового контроля (ст. 23, 62 КоАП РФ).

Первый этап сбора и обработки финансовой информации в указанны... выше целях реализуется силами организаций, осуществляющих операци... с денежными средствами или иным имуществом (далее — банк) в процесс... функционирования системы *внутреннего контроля*. В ходе этого процесс... банк накапливает, выявляет и фиксирует сведения об операциях, вызывающи... подозрение в принадлежности к отмыванию преступных доходов, принимае... меры к приостановлению подозрительных операций (в предусмотренных зако... ном случаях) и передает собранную информацию уполномоченному органу.

Второй этап обработки собранной банком информации имеет наименование ... мер *обязательного контроля*. Он выполняется подразделениями ФСФМ России. На этом этапе информация подвергается дополнительному анализу и проверке. Принимается решение об ее использовании в предусмотренных Законом о противодействии легализации преступных доходов целях.

Законодательно установленным условием функционирования системы является соблюдение конфиденциальности — запрета на информирование клиентов и иных лиц о принимаемых мерах противодействия легализации преступных доходов.

Наряду со сбором информации о подозрительных операциях и сделках, субъекты финансового контроля применяют такие инструменты противодействия легализации преступных доходов, как *запрет на совершение и возможность отказа* от совершения определенных видов сделок и операций.

В частности, кредитным организациям запрещается: открывать счета (вклады) на анонимных владельцев, т. е. без предоставления открывающим счет (вклад) физическим или юридическим лицом документов, необходимых для его идентификации; открывать счета (вклады) физическим лицам без личного присутствия лица, открывающего счет (вклад), либо его представителя; устанавливать и поддерживать отношения с банками-нерезидентами, не имеющими на территориях государств, в которых они зарегистрированы, постоянно действующих органов управления.

Законным основанием для отказа от заключения договора банковского счета (вклада) с физическим или юридическим лицом являются: отсутствие юридического лица, его постоянно действующего представителя по фактическому адресу организации; непредоставление физическим или юридическим лицом документов, подтверждающих необходимые для идентификации...

сведения, либо предоставление недостоверных документов; наличие в отношении физического или юридического лица сведений об участии в террористической деятельности, полученных в соответствии с Законом о противодействии легализации преступных доходов.

Важной особенностью отечественной системы противодействия легализации (отмыванию) преступных доходов является возложение на банк обязанностей подготовить и осуществить меры, обеспечивающие выполнение ряда методических и организационных задач. В частности, ему предписано разработать соответствующие программы выявления и фиксации признаков возможных преступных действий, обучить специально уполномоченных лиц, ответственных за соблюдение указанных правил, и организовать их деятельность в рамках службы внутреннего контроля банка.

Сведения, которые должен собирать банк в процессе реализации мер внутреннего контроля. Являясь элементом системы противодействия отмыванию преступных доходов, банк (согласно ст. 7 Закона о противодействии легализации преступных доходов) обязан собирать информацию *об определенных категориях сделок и операций*, признаки которых установлены действующим законодательством, а также *об участвующих в них лицах.* Критерии выборки сделок и операций содержатся, в первую очередь, в Законе о противодействии легализации преступных доходов.

Выявлению и фиксации подлежат два вида операций (сделок):

1) операции, подлежащие обязательному контролю, исчерпывающие признаки которых перечислены в ст. 6 Закона о противодействии легализации преступных доходов;

2) иные операции, вызывающие у работников банка подозрение о возможной принадлежности к легализации преступных доходов (операции, подлежащие выборочному контролю, ориентировочные признаки которых названы в п. 3 ст. 7 Закона о противодействии легализации преступных доходов).

Важным направлением выявления признаков легализации преступных доходов является изучение сведений о клиентах банка.

Организация и осуществление контроля за операциями первого вида заметных трудностей не вызывает, поскольку выявление и оценка ситуаций, подлежащих обязательному контролю, осуществляется банком на основе установления совокупности указанных в законе формальных признаков. Сам процесс выявления, отбора и фиксации сведений о ситуациях указанного вида может быть автоматизирован на основе дополнений к действующим в банке компьютерным программам. Такая система машинной выборки информации действует, в частности, в ОАО «Внешторгбанк»[1].

[1] *Галкин А. А.* Опыт работы ОАО «Внешторгбанк» по реализации положений Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем» // Тезисы выступления на V Всероссийской конференции «Банковская безопасность: состояние и перспективы развития».

Основные затруднения банковских работников, участвующих в противодействии «отмыванию», возникают в связи с возложенной на них п. 3 ст. 7 Закона о противодействии легализации преступных доходов обязанностью выявления и фиксации так называемых иных, необычных (в смысле подозрительных) операций.

Критерии выявления и признаки необычных сделок разрабатываются банком на основе действующего законодательства и приложения № 2 к «Рекомендациям по разработке кредитными организациями правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (объявлены письмом Банка России от 13 июля 2005 г. № 99-Т).

В качестве критериев необычности сделок Банк России выделил восемь основных видов признаков.

В их числе *общие признаки*, включающие в себя нелогичное для конкретной ситуации поведение клиента (отказ от более выгодных условий, неоправданная сложность операций, отсутствие очевидной связи между характером и родом деятельности клиента с услугами, за которыми клиент обращается в кредитной организации, и т. д.).

В качестве *других видов основных признаков* рассматриваются признаки отмывания (легализации) денежных средств, характерные для:

- использования наличной формы и переводов;
- проведения операций по кредитным договорам;
- проведения расчетов по клирингу;
- использования схем с участием страховщиков;
- проведения международных расчетов;
- проведения операций с ценными бумагами и производными финансовыми инструментами;
- осуществления электронного банкинга и расчетов по пластиковым картам.

При разработке правил внутреннего контроля банку следует учесть следующее немаловажное обстоятельство. *Признаками подозрительной деятельности могут служить не только особенности операций, но и характерные признаки личности и поведения клиента.*

Признаками, дающими основания подозревать клиента — юридическое лицо в причастности к легализации преступных доходов, могут служить два вида обстоятельств.

1. Обстоятельства, *вызывающие сомнение в правоспособности и дееспособности фирмы*, ее деловой репутации. Как правило, их наличие свидетельствует о ненадежности клиента и фиктивном характере его деятельности.

К числу указанных обстоятельств следует отнести сообщение клиентом ложных сведений:

- о создании юридического лица (тогда как на самом деле отсутствуют учредительные документы юридического лица, либо

- об органах управления фирмы, входящих в них лицах и характеризующих их данных; о реальном функционировании представительных органов управления юридическим лицом (в то время как протоколы годовых собраний сфальсифицированы, сведения о деловой репутации органов управления фирмой не соответствуют действительности);
- о величине зарегистрированного и фактически оплаченного уставного капитала (заявленная сумма уставного капитала может быть не оплачена, что является свидетельством неблагонадежности или фиктивных намерений учредителей клиента);
- о количестве, составе учредителей, об их установочных и характеризующих данных;
- об органах управления фирмы, входящих в них лицах (когда данные о структуре органов управления фирмы, количестве, персональном составе и деловой репутации управленческого персонала не соответствуют действительности).

2. *Обстоятельства, относящиеся к финансово-хозяйственной деятельности фирмы*, могут содержать признаки, указывающие на возможность легализации преступных доходов, механизм совершения преступления и источник получения «грязных» денег, которые преступник намеревается легализовать.

Так, возрастание дебиторской задолженности по валютным статьям баланса с истекшими сроками погашения может свидетельствовать о том, что клиент размещает за рубежом денежные или материальные активы, которые целенаправленно выводятся из России под видом совершения коммерческих операций. Увеличение кредиторской задолженности перед бюджетом по налоговым и другим обязательным платежам, а также перед банками по выданным ссудам нередко сопутствует накоплению денежных средств с целью последующего хищения и легализации[1].

Признаком отмывания преступных доходов может служить значительное, не соответствующее размерам оборота легального бизнеса клиента, превышение средних показателей остатков в кассе над остатками средств на расчетных и текущих счетах.

О том, что клиент скрывает от контрольных органов количество действующих счетов, утаивает размер и порядок использования прибыли, изменения величины уставного фонда и собственного капитала, объема основных, оборотных средств и обязательств, а также виды деятельности, занимающие наибольший удельный вес в хозяйственном обороте, и их соответствие уставу может свидетельствовать о несоответствии данных об остатках денежных средств на счетах, содержащихся в балансе клиента и банковских выписках.

Возможным признаком незаконной легализации преступных доходов является большой удельный вес расчетов в наличной форме в общей структуре расчетов клиента при отсутствии ежедневной инкассации; неожиданное

[1] Подробно о способах преступной деятельности: *Максимов А. А.* Бандиты в белых воротничках. Как разворовывали Россию. М.: ЭКСМО-Пресс, 1999.

неоправданное) погашение клиентом сомнительных или просроченных долго... просьбы предоставить кредит под обеспечение активами, источник которых не ...ясен или размер которых не соответствует имущественному положению клиента.

О возможной причастности клиента к противоправной деятельности, в том ...числе к незаконной легализации преступных доходов, может свидетельство...вать системное нарушение нормативных требований по ведению документа...ции и отчетности и ненадлежащее состояние баланса, зафиксированное в ма...териалах аудиторских проверок.

Обстоятельства, относящиеся к личности клиента — физического лица, как ...правило, состоят в попытках лица скрыть его причастность к отмыванию «грязных» денег, а также утаить сведения о фактах, отрицательно характеризующих его собственную деловую репутацию. К числу названных обстоятельств следует отнести сообщение клиентом ложных сведений (в том числе путем предъявления поддельных документов):

- о фамилии, имени, отчестве, дате и месте рождения, постоянном месте жительства или регистрации;
- о постоянном месте работы;
- о размере полученного дохода и уплаченных налогов;
- о полномочиях на совершение банковских операций в случае их совершения по доверенности третьего лица;
- о характере взаимоотношений с другими банками и наличии претензий с их стороны[1].

Источником информации для выявления признаков легализации преступных доходов в процессе осуществления банком мер внутреннего контроля служат главным образом документы:

а) относящиеся к предполагаемой сделке (договоры, счета, чеки, поручения и т. д.);

б) характеризующие правоспособность, дееспособность, финансово-хозяйственную деятельность и деловую репутацию клиента (учредительный договор, сообщение о государственной регистрации, паспорт хозяйствующего субъекта, баланс, банковские выписки, справки налоговых органов, заключения аудиторов и т. д.);

в) относящиеся к личности клиента (документы, удостоверяющие личность, доверенности, приказы, удостоверения и справки различных органов).

Другими источниками информации о признаках возможного отмывания «грязных» денег могут служить:

- пояснения клиента работнику банка о тех или иных обстоятельствах определенной сделки и ее участниках;

[1] Подробные рекомендации о характере и содержании сведений о клиенте, подлежащих установлению в процессе процедуры внутреннего контроля содержатся в Положении ЦБР от 19 августа 2004 г. № 262-П «Об идентификации кредитными организациями клиентов и выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

- сообщения других банков и межбанковских организаций, в которых обслуживался (или обслуживается) клиент, о наличии в его действиях признаков легализации преступных доходов;
- непосредственная проверка работником банка фактических обстоятельств производственной и финансовой деятельности клиента.

Типовые задачи, вытекающие из ситуаций обязательного контроля, разрабатываются на основе криминалистической характеристики незаконной легализации «грязных» денег. Они представляют собой формализованное описание предписанных законом и выработанных практикой вариантов действий, которые предстоит выполнить работникам банка и уполномоченного органа. Цель указанных действий — максимально полно выявить и зафиксировать сведения, которые могут служить поводом для проведения предварительной проверки и расследования по фактам преступлений указанного вида.

В целом указанные сведения представляют собой две взаимодополняющие группы.

Первая из них включает в себя действия по выявлению, проверке и фиксации подозрительных *банковских операций*. В этом случае работник структурного подразделения банка должен документально зафиксировать сведения, характеризующие вид и содержание операции, основания и дату совершения; сумму, на которую она совершена, а также иные обстоятельства, свидетельствующие о возможной легализации преступных доходов.

Вторая группа содержит описание действий по установлению и проверке *лиц, подозреваемых в причастности к совершению названных операций*. Идентификация указанных лиц предполагает выяснение и фиксацию данных паспорта или другого документа, удостоверяющего личность, адреса места жительства или места пребывания, идентификационного номера налогоплательщика (при его наличии).

Условия собирания, хранения и передачи банком информации о легализации преступных доходов. Специфическим условием данной деятельности является предписанная банку обязанность соблюдать конфиденциальный характер своей деятельности и собранной в результате ее информации. Выполнение этой обязанности связано с необходимостью установления режима защиты указанных сведений от свободного доступа посторонних лиц. Такой режим обеспечивается путем применения мер правового и организационного характера. Правовым основанием защиты информации является ее включение в перечень сведений, составляющих банковскую тайну[1].

Выполняя предписание об отнесении указанных сведений к банковской тайне, банк обязан применить ряд установленных законодательством средств, методов их защиты и выполнить в этих целях определенные мероприятия по охране конфиденциальности информации.

[1] Информация, составляющая банковскую (и коммерческую) тайну, охватывается также понятием сведений конфиденциального характера. Перечень сведений конфиденциального характера, утв. Указом Президента РФ от 6 марта 1997 г. № 188 // Собрание законодательства РФ. 1997. № 10. Ст. 1127.

Во-первых, информация, составляющая банковскую тайну, должна быть зафиксирована на материальном носителе (бумаге, магнитном носителе или других материальных объектах) и снабжена реквизитами, позволяющими ее идентифицировать.

Во-вторых, зафиксировав право собственности на документ, обладатель банковской тайны обязан установить специальный порядок обращения с ним (включить его в систему охранительных отношений).

Факт внесения документа в эту систему отражается в соответствующем грифе конфиденциальности («банковская тайна — конфиденциально»), который наносится на каждый экземпляр носителя информации. Установленный таким образом гриф является официальным охранительным знаком — предупреждением о закрытии свободного доступа к документу. Дальнейшее обращение с документами, включенными в охранительную систему, осуществляется в особом правовом режиме. Лица, допускаемые к конфиденциальным документам и содержащейся в них информации, должны дать соответствующие письменные обязательства в отношении их защиты. Устанавливаются особые условия передачи права собственности на документ, условия снятия ограничений на доступ к сведениям, содержащимся в документе.

Наряду с грифом конфиденциальности защищаемый документ должен содержать наименование банка, регистрационный номер и иные знаки, позволяющие идентифицировать законного обладателя сведений, принявшего меры по охране их конфиденциальности.

Применение этих мер призвано предотвратить возможное заявление нарушителя режима конфиденциальности в ходе следствия, судебного (либо иного) разбирательства об использования информации (копирования, передачи и др.) по неосведомленности и непреднамеренном характере своих действий. Охранительная система должна не только ограничить круг лиц, имеющих доступ к документам, содержащим конфиденциальные сведения, и сделать их недоступными для посторонних, но и обеспечить оптимальный режим пользования ими для тех, кому они доверены.

Субъектов правоотношений, использующих информацию в соответствии с установленными правами и правилами, принято объединять понятием: *лица, имеющие доступ к сведениям, составляющим банковскую тайну*. Лица, не имеющие доступа к банковской тайне, относятся к категории *посторонних*.

Важным звеном системы защиты информации является *организация конфиденциального делопроизводства* — особого порядка обращения со сведениями и документами, в которых она содержится. Защищенность информации при работе с нею обеспечивается соблюдением требований инструкции об организации конфиденциального делопроизводства, которая разрабатывается в банке в развитие соответствующего раздела положения о защите банковской тайны.

Принципиальным требованием правил конфиденциального делопроизводства является *установление персональной ответственности лиц за сохранность доверенных им документов*

к сведениям, составляющим коммерческую тайну, должно принять на себя ряд определенных обязательств и ограничений, связанных с будущей деятельностью.

К ним относятся: обязательство нести персональную ответственность за сохранность доверенных конфиденциальных сведений, твердо и неукоснительно выполнять правила конфиденциального делопроизводства, обеспечивать надежное хранение конфиденциальных документов, незамедлительно сообщать уполномоченным лицам об утрате конфиденциальных документов, ключей от их хранилищ, личных печатей, а также о признаках утечки конфиденциальных сведений, и давать устные и письменные пояснения по фактам нарушения правил обращения с конфиденциальными документами.

В число ограничений входят запреты на совершение определенных действий, которые могут повлечь утрату документов или разглашение конфиденциальных сведений (передачу содержания конфиденциальных сведений посторонним, вынос документов из рабочего помещения без производственной необходимости и оставление их в неохраняемых местах, уничтожение документов с нарушением установленного порядка и проч.).

Несмотря на то что перечень указанных выше обязательств и ограничений (запретов), как правило, содержится в инструкции по организации конфиденциального делопроизводства, и работники знакомятся с ними под расписку, факт принятия этих условий конкретным лицом оформляется в виде договора, предусмотренных гражданским законодательством либо законодательством о труде.

Представление сведений, собранных банком в результате процедуры внутреннего контроля, уполномоченной организации. Процедура представления банком указанной информации в ФСФМ России регламентирована «Положением Банка России от 20 декабря 2002 года № 207-П «О порядке представления кредитными организациями в уполномоченный орган сведений, предусмотренных Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

В соответствии с этим документом собранные банком сведения представляются в ФСФМ России в виде электронного документа через территориальные учреждения (далее — ТУ) Банка России.

Внутренний регламент формирования и направления в ТУ сведений кредитная организация устанавливает самостоятельно. Разрешается передача документа в ТУ филиалом кредитной организации.

Передача информации осуществляется с применением средств криптографической защиты информации, принятых к использованию в Банке России.

Кредитная организация подписывает документ электронной цифровой подписью, затем шифрует его с использованием открытого ключа шифрования уполномоченного органа, после чего зашифрованное сообщение повторно подписывает ЭЦП.

Доставка документа может быть произведена по каналам связи или на магнитном носителе.

ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. Каковы основные цели легализации преступных доходов?
2. Какие два основных вида субъектов преступления участвуют в легализации преступных доходов?
3. Какие основные изменения форм денежных средств происходят в процессе легализации преступных доходов?
4. Какая информация маскируется преступниками в процессе легализации преступных доходов?
5. Какие типичные способы сокрытия или искажения информации применяются преступниками в процессе легализации преступных доходов?
6. Какие функции противодействия легализации преступных доходов возложены законом на банк и какими методами они реализуются?
7. Какие источники информации использует банк для выявления признаков легализации преступных доходов?
8. Как реализуются сведения, собранные банком в результате выполнения процедур внутреннего контроля?

Глава 9

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БАНКА

- Информация, использующаяся в целях обеспечения безопасности банка, и ее источники
- Бюро кредитных историй
- Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность банка

9.1. Информация, использующаяся в целях обеспечения безопасности банка, и ее источники

Основу деятельности по обеспечению безопасности банка (как и любой другой человеческой деятельности) составляет так называемый информационный процесс, состоящий из подпроцессов поиска, получения, накопления, переработки и использования необходимой информации. Качество информационного процесса является основным критерием профессионализма служб безопасности банка в целом и ее отдельных работников, в частности.

Наибольшие просчеты в ходе этого процесса, как показывает практика, представляют собой отсутствие четкого представления о содержании, целях, средствах и способах получения и использования информации. Весьма распространенной является ситуация, когда значительный объем накопленной информации (включая полученную с использованием весьма затратных методов) не соответствует реальным задачам обеспечения безопасности, в то время как без использования остается информация из открытых источников, имеющая важное значение для принятия соответствующих решений.

Бессистемный подход к информационному обеспечению системы безопасности существенно снижает возможности выявления, предупреждения и пресечения противоправных посягательств на интересы банка (угроз безопасности) и управления банковскими рисками[1]. Об этом свидетельствуют результаты изучения правоохранительной практики государственных и негосударственных структур.

Основная цель информационного обеспечения деятельности службы безопасности банка заключается в своевременном обнаружении признаков противоправных посягательств на интересы кредитной организации, а также в выявлении банковских рисков. Данные, не соответствующие этой цели, из результатов указанной работы исключаются. Поисковая деятельность служб

[1] Отличие угрозы от риска заключается в характере правового регулирования, отношений, вытекающих из указанных понятий. Содержание угрозы — противоправные, уголовно наказуемые действия. Основной источник регулирования отношений, связанных с угрозами в кредитно-финансовой сфере, — Уголовный кодекс РФ. Содержание риска с точки зрения права — ошибка субъекта безопасности или его сотрудников. Источник возникновения — собственные действия или решения банка или его сотрудника. Это принципиальное положение зафиксировано в ст. 2 ГК РФ, которая определяет «предпринимательскую деятельность» как «самостоятельную, осуществляемую *на свой риск*».

безопасности обладает иерархией подцелей, в которой достижение целей низшего уровня ведет к достижению целей более высокого уровня. Те, в свою очередь могут являться подцелями еще более высокого уровня. В частности обнаружение угроз или рисков выступает в качестве подцели по отношению к цели их предупреждения, пресечения либо минимизации.

При учете сказанного решение проблем информационного обеспечения безопасности банка следует начинать с разработки соответствующей системной модели, дающей наглядное представление о порядке и средствах осуществления указанной деятельности. Основание системной модели (пирамиды) должен составлять перечень основных видов противоправных посягательств на безопасность банка. Верхний уровень системного описания занимают соответствующие отрасли и нормы законодательства, являющиеся инструментом правовой защиты от противоправных деяний. При этом правовые нормы одновременно являются носителями предписаний методологического характера и определяют в свернутом (общем) виде цели, задачи, содержание, способы и условия сбора информации. Детализация положений законодательства осуществляется в рамках концепции безопасности банка и соответствующих криминалистических методик. Часть названных методик может объявляться локальными нормативными актами банка.

Функционирование системы информационного обеспечения безопасности банка предполагает обязательное сопоставление добываемых сведений с четырьмя основными критериями, отражающими степень их относимости к задачам службы безопасности, допустимости использования с точки зрения закона необходимой полноты и всесторонности для принятия соответствующих правовых и иных решений. Указанными критериями являются:

1) перечень объектов защиты в системе безопасности банка;
2) основные виды противоправных посягательств на безопасность банка;
3) отрасли и нормы права, охраняющие объект посягательства;
4) отрасли и нормы права, регламентирующие цели, источники, порядок получения и использования информации для обеспечения безопасности банка.

Иными словами, добываемая информация должна быть четко «привязана» к конкретным объектам защиты, предполагаемым видам противоправных посягательств, обеспечивать возможность применения на ее основе норм правовой защиты и соответствовать установленным законом условиям ее собирания и использования.

Объекты защиты в системе безопасности банка

Ведущими объектами преступных посягательств на безопасность банка являются его имущество и инфраструктура.

Имущество банка включает в себя:

- наличные деньги (находящиеся в обращении банкноты, металлическая монета и иностранная валюта);

- эквиваленты денежных средств — ценные бумаги (чек, вексель, облигация, государственные краткосрочные обязательства — ГК РФО), государственные казначейские обязательства СССР, золотой сертификат Минфина России и др.;
- платежные средства, не являющиеся ценными бумагами, но служащие средством получения наличных денег, — кредитные либо расчетные пластиковые карты, платежные документы (платежные поручения), депозитный сертификат и т. д.;
- безналичные деньги;
- валютные ценности;
- ценные бумаги (как собственные, так и привлеченные средства банка);
- имущественные права на объекты банковской деятельности (предметы залога и т. п.);
- здания, оборудование и инвентарь.

***Инфраструктура* банка** (*внутренний блок*) охватывает собой:

- порядок создания банка — установленные законодательными и иными правовыми нормами требования безопасности к вновь учреждаемому банку; направленные на создание имущественно полноценной кредитной организации, формирование у банка ресурсов, позволяющих обеспечить адекватную защиту от угроз и их последствий, соответствие руководства и управленческого персонала квалификационным требованиям в области безопасности банковского дела;
- порядок функционирования банка — технологии совершения банковских операций, установленные законодательными и иными нормативными (в том числе локальными) актами с целью защиты интересов банка и его клиентов, регламент информационного обеспечения сведениями о надежности потенциальных и реальных клиентов, о возникновении конкретных угроз безопасности банка и т. д.;
- порядок противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Внешний блок инфраструктуры банка составляют:

Информация (информационные ресурсы) банка, в том числе:

- система формирования, распространения и использования информационных ресурсов банка, базы и банки данных, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический персонал разработчиков информационной системы банка, пользователи информационной системы банка и обслуживающий персонал;
- информационная инфраструктура, включающая центры обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены компоненты информационных банковских систем, а также ведутся переговоры, содержащие информацию с ограниченным доступом;
- информационные ресурсы, содержащие сведения, отнесенные к защищаемой информации и представленной в виде носителей на бумажной, магнитной и оптической основе, информативных физических полей, информационных массивов и баз данных;
- основные технические средства и системы, вспомогательные технические средства, системы и сети связи;
- вспомогательные технические средства и системы помещений и зданий, размещенные в местах, где обрабатывается (циркулирует) информация, содержащая сведения, отнесенные к защищаемым, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.

Кадры банка:

- порядок кадрового обеспечения, способствующий формированию и сохранению правопослушного, высокопрофессионального, стабильного и надежного персонала;
- порядок защиты персонала от принуждения со стороны третьих лиц к совершению действий, противоречащих интересам банка (либо вовлечения их в преступную деятельность);
- порядок защиты от внедрения в кадровый состав представителей криминальных и иных враждебных банку организаций.

Нематериальные блага банка:

- деловая репутация (информация, характеризующая банк в качестве делового партнера);
- деловые связи (деловые отношения с действующим либо потенциальным партнером).

Основные виды противоправных посягательств на безопасность банка

Противоправные посягательства на безопасность банка классифицируются по следующим основаниям.

1. *Непосредственный объект защиты*:
   - посягательства на имущество;
   - посягательства на инфраструктуру банка.
2. *Виды деятельности банка, в процессе которых совершено посягательство*:

а) на *операционную деятельность*, совершенное в процессе выполнения банком одной из следующих банковских операций (сделок):

- привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок);
- размещение привлеченных средств от своего имени и за свой счет;
- открытие и ведение банковских счетов физических и юридических лиц;

- осуществление расчетов по поручению физических и юридических лиц, в том числе банков-корреспондентов по их банковским счетам;
- инкассация денежных средств, векселей, платежных и расчетных документов и кассовое обслуживание физических и юридических лиц;
- купля-продажа иностранной валюты в наличной и безналичной формах;
- привлечение во вклады и размещение драгоценных металлов;
- выдача банковских гарантий;
- осуществление переводов денежных средств по поручению физических лиц без открытия банковских счетов (за исключением почтовых переводов);
- выдача поручительств за третьих лиц, предусматривающих исполнение обязательств в денежной форме;
- приобретение права требования от третьих лиц исполнения обязательств в денежной форме;
- доверительное управление денежными средствами и иным имуществом по договору с физическими и юридическими лицами;
- осуществление операций с драгоценными металлами и драгоценными камнями;
- предоставление в аренду физическим и юридическим лицам специальных помещений или находящихся в них сейфов для хранения документов и ценностей;
- лизинговые операции;
- оказание консультационных и информационных услуг;

б) на *неоперационную деятельность*, не связанную непосредственно с процессом выполнения банковских операций (кража, грабеж, разбой, вымогательство, умышленное уничтожение или повреждение имущества, незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, и др.).

3. *Способы воздействия на имущество и инфраструктуру банка*:
   - посягательства, совершенные с применением насилия и угроз (противоправные деяния насильственного характера);
   - посягательства, совершенные тайно либо с применением обмана (противоправные деяния ненасильственного характера).
4. *Субъекты посягательства*:
   а) персонал банка:
      - руководство (лица, принимающие управленческие решения);
      - лица, участвующие в выполнении банковских операций (средний персонал);
      - лица, участвующие в технологическом обеспечении банковских операций, в деятельности технических и программных средств обработки и передачи информации (технический персонал);

б) лица, не входящие в число сотрудников банка, однако участвующие в его операциях на основе договорных отношений (клиенты, контрагенты, корреспонденты);

в) лица, не имеющие с банком трудовых и иных договорных отношений (посторонние):
   - юридические лица (недобросовестные конкуренты, организации, собирающие конфиденциальную информацию и совершающие другие действия, противоречащие интересам банка);
   - физические лица (криминальные элементы);
   - неформальные группы (организованные группы, преступные организации)

Отрасли права, охраняющие объект посягательства (объект неправомерного причинения вреда), в том числе:

а) *Уголовный кодекс РФ, признающий преступлениями посягательства:*
   - на *имущество* банка (преступления против собственности): кража (ст. 158), мошенничество (ст. 159), присвоение или растрата (ст. 160), грабеж (ст. 161), разбой (ст. 162), вымогательство (ст. 163), хищение предметов, имеющих особую ценность (ст. 164), причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165), причинение имущественного ущерба путем умышленного уничтожения или повреждения (ст. 167), причинение имущественного ущерба путем уничтожения или повреждения по неосторожности (ст. 168);
   - на *инфраструктуру* (порядок функционирования) банка: клевета и оскорбление (ст. 129 и 130), легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174), легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174.1), незаконное получение кредита (ст. 176), злостное уклонение от погашения кредиторской задолженности (ст. 177), незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183), неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273), нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274), изготовление или сбыт поддельных денег или ценных бумаг (ст. 186), злоупотребление полномочиями (ст. 201), коммерческий подкуп (ст. 204);

б) *КоАП РФ, признающий административными правонарушениями посягательства*:
   - на *имущество* банка: уничтожение или повреждение чужого имущества, если эти действия не повлекли значительного ущерба (ст. 7.17), мелкое хищение (ст. 7.27);

- на *инфраструктуру* (порядок функционирования) банка: нарушение правил защиты информации (ст. 13.12), разглашение информации с ограниченным доступом (ст. 13.14), нарушение порядка представления статистической информации (ст. 13.19), незаконное получение кредита (ст. 14.11), воспрепятствование должностными лицами кредитной организации осуществлению функций временной администрации (ст. 14.14), ненадлежащее управление юридическим лицом (ст. 14.21), совершение сделок и иных действий, выходящих за пределы установленных полномочий (ст. 14.22), осуществление дисквалифицированным лицом деятельности по управлению юридическим лицом (ст. 14.23), нарушение порядка работы с денежной наличностью и порядка ведения кассовых операций (ст. 15.1), невыполнение обязанностей по контролю за соблюдением правил ведения кассовых операций (ст. 15.2), нарушение порядка открытия счета налогоплательщику (ст. 15.7), нарушение срока исполнения поручения о перечислении налога или сбора (взноса) (ст. 15.8), неисполнение банком решения о приостановлении операций по счетам налогоплательщика, плательщика сбора или налогового агента (ст. 15.9), неисполнение банком поручения государственного внебюджетного фонда (ст. 15.10), грубое нарушение правил ведения бухгалтерского учета и представления бухгалтерской отчетности (ст. 15.11), недобросовестная эмиссия ценных бумаг (ст. 15.17), использование служебной информации на рынке ценных бумаг (ст. 15.21), нарушение законодательства о банках и банковской деятельности (ст. 15.26);

в) *Трудовой кодекс РФ, признающий дисциплинарными проступками действия посягающие*:

- на *имущество* банка: совершение по месту работы хищения (включая мелкое) чужого имущества, растраты, умышленного его уничтожения или повреждения, установленных вступившим в законную силу приговором суда или постановлением органа, уполномоченного на применение административных взысканий (подп. «г» п. 6 ст. 81);
- на *инфраструктуру* (порядок функционирования) банка: прогул (отсутствие на рабочем месте без уважительных причин более 4 ч подряд в течение рабочего дня) (подп. «а» п. 6 ст. 81), появление на работе в состоянии алкогольного, наркотического или иного токсического опьянения (подп. «б» п. 6 ст. 81), разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей (подп. «в» п. 6 ст. 81), совершение виновных действий работником, непосредственно обслуживающим денежные или товарные ценности, если эти действия дают основание для утраты доверия к нему со стороны работодателя (п. 7 ст. 81), принятие необоснованного решения руководителем организации (филиала, представительства), его заместителями и главным бухгалтером, повлекшего нарушение сохранности имущества, неправомерное его использование или иной ущерб имуществу организации (п. 9 ст. 81), однократное грубое нарушение руководителем организации (филиала, представительства), его заместителями своих трудовых обязанностей (п. 10 ст. 81), предоставление работником работодателю подложных документов или заведомо ложных сведений при заключении трудового договора (п. 11 ст. 81).

г) *Гражданский кодекс РФ, признающий гражданско-правовым деликтом (нарушением права) и основанием для возмещения вреда*:

- неправомерное получение и разглашение информации, составляющей коммерческую тайну (ст. 139);
- неправомерное разглашение сведений, составляющих банковскую тайну (ст. 857);
- причинение вреда имуществу гражданина и юридического лица (ст. 1064);
- неправомерные действия, наносящие ущерб деловой репутации и другим видам нематериальных благ.

Перечисленные выше противоправные посягательства и деликты допускают дальнейшую классификацию по следующим основаниям.

Степень тяжести причиненного ущерба:

- восполнимый ущерб — потери имущества и элементов инфраструктуры, которые банк может восполнить за счет собственных средств без угрозы своему существованию и без перевода банка во внештатный режим работы (финансовые потери, снижение доходности, обесценение активов или увеличение обязательств, недостижение установленных целевых ориентиров деятельности, ухудшение деловой репутации и разрушение деловых связей);
- условно восполнимый ущерб — потери имущества и управления, создающие угрозу существованию банка, которые он не может устранить без привлечения внешних средств. Эти последствия выражаются в неспособности банка исполнить требования федеральных законов, регулирующих банковскую деятельность, а также нормативных актов Банка России или удовлетворить требования кредиторов по денежным обязательствам и (или) исполнить обязанность по уплате обязательных платежей. Внешними инструментами восполнения потерь в данных случаях могут служить заемные финансовые средства, привлеченный для восстановления управления новый персонал (вплоть до введения внешнего управления), приобретение новых технических средств обеспечения банковских операций и т. д. Размеры внешнего заимствования не должны выходить за пределы, установленные законодательством и нормативными актами Банка России. В противном случае появляются основания для отзыва у

ций. Для возмещения условно восполнимых потерь банк вынужден переходить на внештатный режим работы;

- невосполнимый (катастрофический) ущерб — потери имущества и инфраструктуры банка, возместить которые не представляется возможным, а его причинение влечет ликвидацию или реорганизацию банка.

Цель противоправных посягательств:

а) завладение имуществом (правом на имущество) банка с целью обращения его в свою собственность;

б) ограничение деятельности банка конкурентом либо устранение банка рынка финансовых услуг путем разрушения клиентских связей, срыва переговоров и сделок, распространение дезинформационных материалов порочащего характера, умышленное вовлечение в заведомо убыточные проекты, уничтожение имущества, разрушение элементов инфраструктуры (в том числе путем противоправных посягательств на кадровый состав — угрозы, вымогательство, вербовка, внедрение, похищение).

Отрасли и нормы права, регламентирующие цели, источники, порядок получения и использования информации для обеспечения безопасности банка

Структура этих отраслей и норм права строится с учетом реальных информационных потребностей описанной выше системы охранительных норм.

Так, задачам добывания и использования информации, необходимой для применения норм Уголовного кодекса РФ, служат Уголовно-процессуальный кодекс РФ, Закон об оперативно-розыскной деятельности, Закон о частной детективной деятельности, Закон о противодействии легализации преступных доходов.

Применение материальных (устанавливающих санкции) норм КоАП РФ обеспечивается информацией, получаемой с соблюдением условий, установленных процессуальными нормами названного кодекса.

Аналогичный порядок информационного обеспечения в целях применения материальных норм установлен и Трудовым кодексом РФ.

Условия получения информации в целях применения материальных норм Гражданского кодекса РФ регламентированы Гражданским процессуальным кодексом РФ.

В ряду законодательных актов своеобразное положение занимает упомянутый выше Закон о частной детективной деятельности. Собираемая в его рамках информация может предназначаться для использования в целях реализации материальных норм трех отраслей законодательства, а именно: Уголовного кодекса РФ, Гражданского кодекса РФ и Трудового кодекса РФ.

Дальнейшее детальное описание целей поиска, содержания и использования информации для реализации норм материального права содержится в соответствующих рекомендациях по выявлению и предупреждению противоправных посягательств на безопасность банка, описанных в предыдущих разделах.

Источники информации, использующейся в целях обеспечения безопасности банка

Ведущим основанием классификации источников (и методов добывания) информации, необходимой для обеспечения безопасности банка, является их разделение на гласные и негласные.

Право применения негласных методов и использования негласных источников в целях добывания информации принадлежит исключительно оперативным подразделениям правоохранительных органов и специальных служб (ст. 13 Закона об оперативно-розыскной деятельности). Применение указанных методов службой безопасности банка исключается.

Сбор сведений гласными методами из гласных источников регламентирован Законом о частной детективной деятельности. Указанные методы лежат в основе процесса информационного обеспечения, ведущегося службой безопасности банка. Порядок сбора и использования гласной информации в целях обеспечения безопасности в более широком плане изложен в соответствующих нормах Уголовно-процессуального кодекса РФ, Гражданского процессуального кодекса РФ, КоАП РФ, Закона о противодействии легализации преступных доходов, в рекомендациях криминалистики, а также в специальных инструкциях для служб безопасности, утвержденных внутренними (локальными) нормативными актами банка.

Согласно перечисленным выше законодательным актам, регламентирующим порядок гласного сбора сведений, служба безопасности имеет право получать необходимую информацию способами, в числе которых:

- опрос граждан и должностных лиц (с их согласия);
- изучение предметов и документов (с письменного согласия их владельцев);
- внешний осмотр строений, помещений и других объектов;
- наблюдение для получения необходимой информации;
- наведение справок.

В качестве условий получения, исследования и фиксации информации закон допускает использование видео- и аудиозаписи, кино- и фотосъемки, технических и иных средств, не причиняющих вреда жизни и здоровью граждан и окружающей среде. Вполне правомерно отнести к числу «технических и иных средств» средства криминалистической техники.

Опрос граждан и должностных лиц применительно к практике информационного обеспечения безопасности банка включает в себя получение необходимых сведений в процессе контакта (который осуществляется непосредственно либо с использованием средств связи) с лицами, которые связаны с банком определенными отношениями (трудовыми, договорными, клиентскими) либо не имеют таких связей (посторонними). Гражданин, не имеющий отношений с банком, может сообщить, например, информацию о биографических и других данных кандидата на работу, оказать содействие в сборе сведений, по

о предмете предполагаемого залога, проинформировать о наличии задолженности организации по заработной плате и т. д.

Должностное лицо сторонней организации имеет возможность сообщить банку сведения о надежности будущего заемщика, о наличии товаров (предмета залога) на складе, о достоверности сведений об отправке продукции (при оплате аккредитива) и т. д.

Изучение предметов и документов включает в себя:

- ознакомление с личными документами клиентов и контрагентов банка, в том числе с целью установления аутентичности предъявившего их лица и проверки подлинности документа;
- проверку подлинности представленных клиентом анкет, финансовых инструментов и товарно-транспортных накладных и квитанций;
- исследование бухгалтерской отчетности, документов о предмете предполагаемого залога и т. д.

Внешний осмотр строений, помещений и других объектов чаще всего выполняется с целью проверки подлинности сведений о фактическом наличии и ориентировочной цене объектов предполагаемого залога. Указанным способом, например, при осмотре складских помещений, может выясниться явное несоответствие реальных площадей заявленным объемам якобы хранящейся в них продукции.

Наблюдение для получения необходимой информации используется для подтверждения подлинности заявленных сведений о содержании производственной деятельности, объемах производимой продукции, о выполнении условий договора и т. д.

Наведение справок является широко распространенным и продуктивным способом получения необходимой информации. Суть указанного действия заключается «в получении фактической информации, имеющей значение для решения задач сыскного характера, путем направления запроса соответствующему физическому или юридическому лицу, располагающему или могущему располагать таковой, а равно ее получение путем непосредственного ознакомления с соответствующим материальным носителем (документом и т. п.)»[1].

Понятие наведения справок охватывает использование информационных ресурсов — отдельных документов и массивов документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах), доступ к которым открыт с согласия их владельцев (на безвозмездной либо коммерческой основе), в том числе через поисковую систему Интернета.

Указанные ресурсы могут быть специализированными, созданными для использования в целях правоохранительной деятельности (например, содержать сообщения о реквизитах поддельных ценных бумаг и пластиковых карт,

[1] *Шумилов А. Ю.* Краткая сыскная энциклопедия: Деятельность оперативно-розыскная, контрразведывательная, частная сыскная (детективная). М.: Изд-ль Шумилова И. И., 2000. С. 3

либо иметь «двойное назначение». К последним можно отнести сведения, предназначенные для использования в хозяйственной деятельности, одновременно имеющие значение для выявления противоправных действий (например, Единый государственный реестр юридических лиц (далее — ЕГРЮЛ)).

К числу специализированных информационных массивов, предназначенных для всеобщего ознакомления, относятся данные АУВЕР о похищенных, утраченных, подделанных и арестованных ценных бумагах. Указанная информация размещена на web-сайте Ассоциации в Интернете (www.auver.ru).

Кроме того, она публикуется путем:

- распространения пресс-релизов или иных печатных материалов в средствах массовой информации;
- предоставления агентствам;
- оглашения в процессе публичных мероприятий в форме выступлений, стендов, таблиц и других информационных материалов.

Специализированные информационные массивы правоохранительного содержания, предназначенные для всеобщего использования, формируются Банком России, Министерством финансов РФ, Ассоциацией российских банков, отдельными эмитентами ценных бумаг и пластиковых карт. Содержащиеся в этих массивах сведения о фактах появления фальшивых ценных бумаг, о хищениях и утрате бланков строгой отчетности, о новых способах совершения и маскировки мошенничества и других преступлений в финансово-кредитной сфере распространяются в форме писем, указаний оперативного характера и обращений[1]. Отдельные эмитенты ценных бумаг и пластиковых карт выпускают так называемые стоп-листы, в которых распространяются сведения о похищенных и утраченных документах.

Весьма перспективной представляется возможность информационного взаимодействия служб безопасности банков с Главным информационно-аналитическим центром (далее — ГИАЦ) Министерства внутренних дел РФ.

Названный центр располагает учетом лиц (осужденных и объявленных в розыск), нераскрытых преступлений, способов совершения преступлений в различных сферах (в том числе — банковской), о появившихся в обращении фальшивых денежных знаках и финансовых документах и т. д.

В соответствии с п. 16 Положения о ГИАЦ центр наделен полномочиями оказывать в установленном законодательными и иными нормативными

[1] См., например письмо Министерства финансов РФ об утрате бланков простых и переводных векселей (от 6 декабря 1996 г. № 03-А5-10/65); информационное письмо Банка России о случаях обращения векселей с подделанным авалем, совершенным от имени Центрального банка (письмо от 26 февраля 1996 г. № 28-1-15/236); информационное Письмо Банка России от 29 ноября 2004 г. № 29-5-1-11/4372 «О поддельных банкнотах Банка России» с описанием реквизитов банкнот, характерных признаков подделки и методов их выявления; информацию оперативного характера службы безопасности АРБ «Амулет» о выявленных попытках мошенничества в банковской сфере, особенностях преступных посягательств, использующихся личных документах и приметах преступников (сообщения от 24 марта 2002 г. № 009) и т. д.

правовыми актами Российской Федерации, нормативными правовыми актами МВД России в порядке и в соответствии с компетенцией ГИАЦ информационные и иные услуги на договорной, в том числе на возмездной основе[1].

До настоящего времени наиболее распространенным видом информационных услуг ГИАЦ в сфере банковской безопасности служит предоставление справок о судимости граждан, регламентированное отдельным Приказом МВД РФ от 1 ноября 2001 г. № 965 «Об утверждении инструкции о порядке предоставления гражданам справок о наличии (отсутствии) у них судимости».

В качестве информации правоохранительного содержания, представляемой МВД России для всеобщего использования (безвозмездно), следует назвать сведения о лицах, находящихся в федеральном розыске по подозрению в совершении преступлений. Она распространяется путем опубликования в печатных и электронных СМИ, в форме листовок и плакатов, а также в Интернете на web-сайте МВД России (www.mvdrf.ru). Там же содержатся сведения статистического характера, позволяющие ориентироваться в текущих тенденциях преступной деятельности, в том числе в кредитно-финансовой сфере.

Весьма актуальная информационная услуга «Проверка паспортов на подлинность» предоставляется Национальным бюро кредитных историй (НБКИ), использующим соответствующие учеты Федеральной миграционной службы.

Обратившись на официальный сайт НБКИ (http://www.nbki.ru/default.aspx), банк и любой другой пользователь могут в течение нескольких секунд получить сведения о действительности документа, об установочных данных владельца конкретного паспорта, адресе его регистрации, нахождении лица в розыске и другую информацию, необходимую для целей обеспечения безопасности банковской деятельности.

Большие потенциальные возможности для перевода информационного сотрудничества правоохранительных органов с негосударственными структурами на качественно новый уровень имеются у Межведомственной комиссии РФ по вопросам сотрудничества банков и правоохранительных органов, созданной совместным приказом МВД, ФСБ, Министерства финансов и Банка России № 327/370/61/02 117 от 8 июля 1993 г. В настоящее время в работе комиссии участвуют также представители Федеральной таможенной службы и Федеральной службы финансового мониторинга. МВК установлены рабочие контакты с банковской Федерацией Европейского союза, оперативной группой по финансовым расследованиям государств «большой восьмерки» ФАТФ, Федеральным ведомством США по борьбе с финансовыми преступлениями (Fincen). Рабочим органом комиссии является ее секретариат.

Применительно к теме банковской безопасности основные функции МВК и ее секретариата заключаются в: организации информационного взаимодействия между службами безопасности отечественных и зарубежных банков

[1] Положение о Главном информационно-аналитическом центре Министерства внутренних Российской Федерации, объявленное Приказом МВД России от 21 января 2005 г. № 33.

и Международной ассоциацией безопасности банков в области предупреждения и выявления преступлений, а также в оказании содействия правоохранительным органам Российской Федерации в получении информации о фактах финансовых мошенничеств, отмывания денег, появления поддельных денежных знаков, других преступлениях, совершаемых с использованием банковских структур.

Специализированной базой данных правоохранительного содержания являются публикующиеся материалы деятельности судебных органов — сборники, бюллетени, обобщения по результатам рассмотрения уголовных, гражданских и арбитражных дел. Эти данные распространяются через точки реализации юридической литературы в виде сборников на бумажных носителях либо в электронном виде (на CD). Систематическая обработка этих материалов позволяет службе безопасности получать весьма ценные сведения (об участниках уголовных и гражданских процессов, типовых способах подготовки, совершения и маскировки преступлений, уклонения от уголовной и гражданской ответственности и т. д.) в целях обеспечения безопасности будущих сделок и операций. В этом плане определенную ценность представляют не только материалы судебных слушаний, но также информация о делах, подлежащих рассмотрению (списки вывешиваются в зданиях судов).

Для использования в качестве ориентирующих сведений в целях информационного обеспечения банковской безопасности определенный интерес представляет специализированный информационный ресурс Интернета Компромат.Ru (www.compromat.ru), нередко размещающий копии документов оперативно-розыскного характера, а также материалы следствия и суда.

К числу информационных ресурсов «двойного назначения», позволяющих выявлять путем анализа и сравнения признаки готовящегося противоправного посягательства, относятся *ЕГРЮЛ и Единый государственный реестр физических лиц в качестве индивидуальных предпринимателей* (далее — ЕГРИП). Названные реестры ведутся в соответствии с Федеральным законом от 8 августа 2001 г. № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей» (в ред. от 30 апреля 2008 г. № 55-ФЗ) и имеют статус федеральных информационных ресурсов.

Содержание ЕГРЮЛ составляют следующие сведения и документы о юридическом лице (в ред. Федерального закона от 23 июня 2003 г. № 76-ФЗ):

а) полное и (в случае, если имеется) сокращенное наименование, в том числе фирменное наименование, для коммерческих организаций на русском языке. В случае, если в учредительных документах юридического лица его наименование указано на одном из языков народов Российской Федерации и (или) на иностранном языке, в едином государственном реестре юридических лиц указывается также наименование юридического лица на этих языках;

б) организационно-правовая форма;

в) адрес (место нахождения) постоянно действующего исполнительного органа юридического лица (в случае отсутствия

исполнительного органа юридического лица — иного органа или лица, имеющих право действовать от имени юридического лица без доверенности), по которому осуществляется связь с юридическим лицом;

г) способ образования юридического лица (создание или реорганизация);

д) сведения об учредителях (участниках) юридического лица, в отношении акционерных обществ также сведения о держателях реестров их акционеров;

е) подлинники или засвидетельствованные в нотариальном порядке копии учредительных документов юридического лица;

ж) сведения о правопреемстве — для юридических лиц, созданных в результате реорганизации иных юридических лиц; для юридических лиц, в учредительные документы которых вносятся изменения в связи с реорганизацией, а также для юридических лиц, прекративших свою деятельность в результате реорганизации;

з) дата регистрации изменений, внесенных в учредительные документы юридического лица, или в случаях, установленных законом, дата получения регистрирующим органом уведомления об изменениях, внесенных в учредительные документы;

и) способ прекращения деятельности юридического лица (путем реорганизации или путем ликвидации);

к) размер указанного в учредительных документах коммерческой организации уставного капитала (складочного капитала, уставного фонда, паевых взносов или другого);

л) фамилия, имя, отчество и должность лица, имеющего право без доверенности действовать от имени юридического лица, а также паспортные данные такого лица или данные иных документов, удостоверяющих личность в соответствии с законодательством Российской Федерации, и идентификационный номер налогоплательщика при его наличии;

м) сведения о лицензиях, полученных юридическим лицом;

н) сведения о филиалах и представительствах юридического лица;

о) идентификационный номер налогоплательщика, код причины и дата постановки на учет юридического лица в налоговом органе;

п) коды по Общероссийскому классификатору видов экономической деятельности;

р) номер и дата регистрации юридического лица в качестве страхователя в территориальном органе Пенсионного фонда Российской Федерации; в исполнительном органе Фонда социального страхования Российской Федерации; в территориальном фонде обязательного медицинского страхования;

) сведения о банковских счетах юридического лица.

Из реестра можно также получить сведения о нахождении юридического лица в процессе ликвидации.

ГРИП содержит следующие сведения об индивидуальном предпринимателе:

фамилия, имя и (в случае, если имеется) отчество на русском языке (для иностранных граждан и лиц без гражданства такие сведения дополнительно

указываются с помощью букв латинского алфавита на основании сведений содержащихся в документе, удостоверяющем личность в соответствии с законодательством Российской Федерации);

б) пол;

в) дата и место рождения;

г) гражданство (при отсутствии у индивидуального предпринимателя гражданства указывается: «лицо без гражданства»);

д) место жительства в Российской Федерации (указывается адрес — наименование субъекта Российской Федерации, района, города, иного населенного пункта, улицы, номера дома, квартиры, по которому индивидуальный предприниматель зарегистрирован в установленном законодательством Российской Федерации порядке (далее — адрес места жительства));

е) данные основного документа, удостоверяющего личность гражданина Российской Федерации на территории Российской Федерации (далее — основной документ) (в случае, если индивидуальный предприниматель является гражданином Российской Федерации);

ж) вид и данные документа, установленного федеральным законом или признаваемого в соответствии с международным договором Российской Федерации в качестве документа, удостоверяющего личность иностранного гражданина (в случае, если индивидуальный предприниматель является иностранным гражданином);

з) вид и данные документа, предусмотренного федеральным законом или признаваемого в соответствии с международным договором Российской Федерации в качестве документа, удостоверяющего личность лица без гражданства (в случае, если индивидуальный предприниматель является лицом без гражданства);

и) вид, данные и срок действия документа, подтверждающего право индивидуального предпринимателя временно или постоянно проживать в Российской Федерации (в случае, если индивидуальный предприниматель является иностранным гражданином или лицом без гражданства);

к) дата государственной регистрации физического лица в качестве индивидуального предпринимателя и данные документа, подтверждающего факт внесения в единый государственный реестр индивидуальных предпринимателей записи об указанной государственной регистрации;

л) дата и способ прекращения физическим лицом деятельности в качестве индивидуального предпринимателя (по заявлению, либо в связи со смертью, либо в связи с принятием судом решения о признании несостоятельным (банкротом) или о прекращении деятельности в качестве индивидуального предпринимателя в принудительном порядке, либо в связи с вступлением в силу приговора суда, которым назначено наказание в виде лишения права заниматься предпринимательской деятельностью на определенный срок, либо в связи с аннулированием документа, подтверждающего право

проживать в Российской Федерации, или окончанием срока действия указанного документа);

м) сведения о лицензиях, полученных индивидуальным предпринимателем;

н) идентификационный номер налогоплательщика, дата постановки на учет индивидуального предпринимателя в налоговом органе;

о) коды по Общероссийскому классификатору видов экономической деятельности;

п) номер и дата регистрации индивидуального предпринимателя в качестве страхователя:

- в территориальном органе Пенсионного фонда РФ;
- в исполнительном органе Фонда социального страхования РФ;
- в территориальном фонде обязательного медицинского страхования;

р) сведения о банковских счетах индивидуального предпринимателя.

Информация о банковских счетах юридических лиц и физических лиц-предпринимателей включает в себя сведения о фактах открытия и закрытия банковских счетов российских хозяйствующих субъектов. Она представляется в регистрирующий орган в течение 10 дней с момента открытия (закрытия) счета и накапливается в информационном ресурсе «Банковские счета»[1]. Указанные сведения не раскрывают операции по счетам и поэтому не относятся к банковской тайне. Вместе с тем их использование в отдельных случаях позволяет предупредить случаи готовящегося мошенничества и других противоправных посягательств.

Ведение государственных реестров ЕГРЮЛ и ЕГРИП осуществляется регистрирующим органом — Федеральной налоговой службой (ФНС России) в порядке, установленном Правительством РФ[2].

Доступ к указанным ресурсам является свободным для всех заинтересованных лиц. Процедура доступа регламентирована Приказом Федеральной налоговой службы «Об утверждении Порядка предоставления в электронном виде сведений, содержащихся в Едином государственном реестре юридических лиц и в Едином государственном реестре индивидуальных предпринимателей»[3].

Сведения о порядке и условиях доступа к указанной информации, о реквизитах платежных документов, используемых при оплате информационных

[1] См.: Приказ МНС РФ от 27 февраля 2004 г. № БГ-3–24/160@ О создании информационного ресурса «Банковские счета»

[2] Постановления Правительства РФ от 19 июня 2002 г. № 438 «Об утверждении правил ведения Единого государственного реестра юридических лиц и предоставления содержащихся в нем сведений»; от 16 октября 2003 г. № 630 «Об утверждении правил ведения Единого государственного реестра индивидуальных предпринимателей и предоставления содержащихся в нем сведений».

[3] Приказ Федеральной налоговой службы от 21 октября 2004 г. № САЭ-3–09/7@ «Об утверждении Порядка предоставления в электронном виде сведений, содержащихся в Едином государственном реестре юридических лиц и в Едином государственном реестре индивидуальных предпринимателей».

слуг содержатся в сети Интернет на сайте ФНС России (www.nalog.ru) и сайтах управлений ФНС России по субъектам Российской Федерации.

Весьма ценными при подготовке и заключении сделок с иностранными контрагентами могут стать данные электронных баз о регистрации таких юридических лиц за рубежом. Открытый доступ к названным сведениям предоставляется с использованием сети Интернет по следующим адресам:

- Венгрия (доступ осуществляется на платной основе) — http://www.Microsec.hu
- Нидерланды — http://www.kvk.nl
- Польша (доступ осуществляется на платной основе) — http://www.ms.pov.pl
- Великобритания — http://www.companieshouse.gov.uk
- Италия — http://www.infoimprese.it
- Франция — http://www.infogreffe.fr и http://www.sociate.com
- Республика Кипр — http://www.mcit.gov.cy/drcor
- Словакия — http://www.orsr.sk/
- Чехия — http://www.justice.cz/
- Финляндия — https://www.ytj.fi/
- США (штат Делавэр) — https://sos-res.state.de.us/tin/GINameSearch.jsp
- США (штат Арканзас) — http://www.sosweb.state.ar.us/corps/search_all.php
- США (штат Иллинойс) — http://www.cyberdriveillinois.com/cgi-bin/business_services/corpsrch.s
- США (штат Калифорния) — http://kepler.ss.ca.gov/list.html
- США(штат Нью-Йорк) — http://appsext5.dos.state.ny.us/corp_public/enter_search
- США (штат Орегон) — http://www.sos.state.or.us/corporation/online.htm
- США (штат Джорджия) — http://www.sos.state.ga.us/corporations/corpsearch.htm
- США (штат Вермонт) — http://www.sec.state.vt.us/seek/database.htm
- США (штат Аризона) — http://www.sosaz.com/scripts/TNT_Search_engine.dll
- США (штат Колорадо) — http://www.sos.state.co.us/cgi-orte/fortecgi?sos_www=www.sos.state.co.us&serviceName=corporationProdAccess&templateName=corporation/publicinquiries/public_inquiry_corp_criteria_outer_form.forte&sourse=campaign

К числу ценных массивов информации «двойного назначения» относятся ежемесячные бюллетени и годовые отчеты по результатам деятельности Счетной палаты Российской Федерации, осуществляющей контрольно-ревизионную, экспертно-аналитическую, информационную и другие виды деятельности в целях контроля за исполнением федерального бюджета и бюджетов федеральных внебюджетных фондов.

Контрольные полномочия Счетной палаты распространяются на органы местного самоуправления, предприятия, организации, банки, страховые

компании и другие финансово-кредитные учреждения, их союзы, ассоциации и иные объединения вне зависимости от видов и форм собственности, если они получают, перечисляют, используют средства из федерального бюджета или используют федеральную собственность либо управляют ею, а также имеют предоставленные федеральным законодательством или федеральными органами государственной власти налоговые, таможенные и иные льготы и преимущества.

Бюллетени и отчеты Счетной палаты публикуются в открытой печати и содержат данные, которые могут быть использованы для оценки надежности предполагаемых контрагентов, в том числе качества управления организациями и возможной причастности руководства к противоправной деятельности[1].

В аналогичных целях могут быть использованы материалы деятельности Счетных палат субъектов Российской Федерации.

Небесполезными для целей обеспечения безопасности банка могут оказаться открытые данные о структуре государственных и общественных организаций. Довольно часто мошенники предъявляют визитные карточки и удостоверения работников органов законодательной и исполнительной власти, общественных организаций, экспертных, консультативных и т. д. советов со звучными названиями. Однако обращение к опубликованным в Интернете официальным сайтам организаций позволяет выявить отсутствие в их структуре названных мошенником подразделений, а то и самих организаций.

Существенным подспорьем в создании собственного информационно-аналитического массива службы безопасности банка может стать систематическая обработка материалов, столичных и региональных СМИ, публикуемых в Интернете и на бумажных носителях. Результативность обработки указанных данных существенно возрастает при использовании специальных аналитических систем, способных выявлять в автоматическом режиме неявные связи между заданными объектами и событиями, и представлять их в виде легко воспринимаемых схем.

При подготовке к сделкам (операциям) с иностранными партнерами важное значение для обеспечения безопасности могут иметь коммерческие базы данных зарубежных консалтинговых компаний. Таких, например, как американской информационной корпорации «Дан энд Брэдстрит» (D&B) (www.dnb.ru).

Корпорация предоставляет заказчику справку, содержащую более 50-ти позиций, характеризующих изучаемый объект, в том числе:

- регистрационные данные, время существования и учредители;
- выдержки из консолидированного балансового отчета (активы, дебиторская задолженность, валовый доход, пассивы, торговая кредиторская задолженность, ссуды и овердрафты банков и т. д.); число работающих; данные о руководстве (имя, фамилия, возраст, должность, информация

[1] Федеральный закон от 11 января 1995 г. № 4-ФЗ «О счетной палате Российской Федерации» (в ред. от 29 марта 2008 г. № 4-ФЗ).

о прежней работе, участие в руководстве другими компаниями); аудиторы; дочерние организации; банки, в которых фирма имеет счет; клиенты и их количество; фактический адрес производственных площадей; обобщающий показатель уровня кредитного риска.

Цены за соответствующие услуги представлены в табл. 3

Таблица 3

Цены бизнес-справки D&B, долл.

ена контракта	1000	3000	5000	7000
оличество справок	6	20	25	50
ена за одну справку	167	150	143	140

Не менее широкий набор информационных услуг в целях оценки надежности предполагаемого зарубежного клиента предоставляет Объединенный союз кредитреформ (http://www.creditreform.haupt.ru) — ФРГ. Эта организация располагает 180 филиалами, в том числе представительством в Москве[1].

Большую роль в информационном обеспечении безопасности отечественной кредитной сферы призваны оказать массивы сведений, формирующиеся в соответствии с Федеральным законом от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях» (в ред. от 24 июня 2007 г. № 214-ФЗ) (далее — Закон о кредитных историях).

9.2. Бюро кредитных историй

Кредитные истории представляют собой специализированный вид информационных ресурсов, создающихся с целью обеспечения безопасности банковской деятельности в кредитной сфере. Для справки: по данным Федеральной службы статистики объем просроченной кредиторской задолженности российских предприятий и организаций в феврале 2008 г. составил 798,5 млрд руб.[2] Особое значение кредитные истории имеют для России, где до последнего времени наиболее простым и доходным видом мошенничества являлось получение кредита без намерения его возвратить.

Мировая практика свидетельствует о том, что наличие такого рода ресурсов весьма положительно сказывается на состоянии кредитно-финансовой сферы. Во-первых, она способствует повышению уровня защищенности кредиторов и заемщиков от криминальных угроз и иных видов кредитных рисков. Во-вторых, информационная открытость заемщиков позволяет банкам активизировать кредитную деятельность и оказывает положительное влияние на рост объема кредитных операций. В качестве примера можно сослаться

[1] *Доронин А. И.* Бизнес-разведка. 2-е изд., перераб. и доп. М.: Ось-89, 2003. С. 115–116.

[2] http://www.gks.ru/wps/portal/!ut/p/.cmd/cs/.ce

на зарубежный опыт: в странах, имеющих бюро кредитных историй, объем банковских кредитов по отношению к ВВП на 15–20% больше, чем в сопоставимых странах, не создавших таких институтов.

Законодательной основой создания специализированной информационной системы в сфере кредитного дела в России явился Закон о кредитных историях. В соответствии с его положениями сведения об участниках кредитных операций формируются в рамках единой системы, охватывающей всю территорию России.

Верхний уровень системы представляет собой *Центральный каталог кредитных историй (государственный реестр)*, который ведется Банком России. Цель создания Центрального каталога — обеспечение информационного поиска кредитных историй конкретных лиц (физических и юридических) в интересах пользователей, а также взаимодействия между кредитными бюро. Необходимо отметить, что Центральный каталог кредитных историй хранит лишь титульные части всех кредитных историй, ведущихся на территории Российской Федерации. Государственный реестр бюро кредитных историй относится к числу открытых и общедоступных федеральных информационных ресурсов. Информация о наличии и месте хранения материалов предоставляется Центральным каталогом по запросам субъектов и пользователей кредитных историй *безвозмездно*.

Содержательная (основная) часть кредитных историй находится в информационных массивах первичных звеньев системы — в бюро кредитных историй и раскрывается в установленных законом случаях в форме *кредитного отчета*.

Бюро кредитных историй имеет статус коммерческой организации (юридического лица), оказывающей услуги по формированию, обработке и хранению кредитных историй, а также по предоставлению кредитных отчетов на *возмездной основе*.

Под *субъектом кредитной истории* понимается физическое или юридическое лицо, которое является заемщиком по договору займа (кредита) и в отношении которого формируется кредитная история.

Понятием *пользователь кредитной истории* охватываются индивидуальные предприниматели или юридические лица, получившие согласие субъекта кредитной истории на получение кредитного отчета для заключения договора займа (кредита).

Кредитная история формируется бюро кредитных историй на основе информации, представляемой организацией-кредитором в рамках договора об оказании информационных услуг. Обязательным условием представления информации является наличие документально (на бумажном носителе либо в виде электронного документа) зафиксированного согласия заемщика.

Срок предоставления информации в бюро кредитных историй устанавливается указанным выше договором об оказании информационных услуг, однако не может превышать 10 дней со дня совершения действия (наступления

события), информация о котором входит в состав кредитной истории в соответствии с Федеральным законом, либо со дня, когда источнику формирования кредитной истории стало известно о совершении такого действия (наступлении такого события). Информация предоставляется в бюро кредитных историй в форме электронного документа.

Организация-кредитор, предоставляющая в бюро кредитных историй информацию о заемщике в целях формирования кредитной истории, имеет статус *источника формирования кредитной истории*.

Предоставление указанной информации о заемщике третьему лицу (бюро кредитных историй) не является нарушением охраняемой законом тайны (коммерческой, банковской, налоговой и т. д.), поскольку осуществляется с согласия заемщика и в его интересах. Кроме того, выдача информации о субъекте кредитной истории предполагаемому пользователю кредитной истории (организации, с которой заключается новый договор займа) возможна только при наличии согласия заемщика (субъекта кредитной истории).

Содержание кредитной истории позволяет достаточно полно и всесторонне оценить степень прозрачности ее субъекта. Исследовать содержание, динамику и перспективы его коммерческой деятельности. Сделать обоснованные выводы об эффективности управления бизнесом, деловой репутации, правопослушности и надежности предполагаемого заемщика. Содержание кредитной истории обновляется по мере изменения любых составляющих ее сведений.

Закон о кредитных историях предусматривает ведение двух видов кредитных историй:

а) кредитные истории, субъектом которых являются физические лица;

б) кредитные истории, субъектом которых являются юридические лица.

Структура кредитной истории обеих видов состоит из трех частей — титульной, основной и дополнительной (закрытой).

Титульная часть кредитной истории физического лица включает в себя информацию о персональных данных ее субъекта, в число которых входят:

- фамилия, имя, отчество, дата и место рождения;
- данные паспорта или иного документа, удостоверяющего личность (номер, дата и место выдачи, наименование органа, выдавшего паспорт или иной документ, удостоверяющий личность);
- идентификационный номер налогоплательщика (если лицо его указало);
- страховой номер индивидуального лицевого счета, указанный в страховом свидетельстве обязательного пенсионного страхования (если лицо его указало).

Сведения о месте регистрации и фактического места жительства, а также о государственной регистрации физического лица в качестве индивидуального предпринимателя Федеральный закон включил в содержание основной части кредитной истории.

Содержание основной части кредитной истории составляют преимущественно сведения, характеризующие факт заключения кредитного договора, параметры

и динамику его исполнения заемщиком. Эта часть информации фиксирует следующие характеристики сделки:

- сумму обязательства заемщика на дату заключения договора займа (кредита);
- срок исполнения обязательства заемщика в полном размере в соответствии с договором займа (кредита);
- указание срока уплаты процентов в соответствии с договором займа (кредита);
- наличие изменений и (или) дополнений к договору займа (кредита), в том числе касающихся сроков исполнения обязательств;
- дата и сумма фактического исполнения обязательств заемщика в полном и (или) неполном размерах;
- факт погашения займа (кредита) за счет обеспечения в случае неисполнения заемщиком своих обязательств по договору;
- наличие судебных споров по договору займа (кредита) и содержание резолютивных частей судебных актов, вступивших в законную силу, за исключением информации, входящей в состав дополнительной (закрытой) части кредитной истории;
- иную информацию, имеющую отношение к кредитной сделке, официально полученную из государственных органов;
- дату запроса пользователя.

Дополнительная (закрытая) часть кредитной истории содержит сведения *источниках формирования* и *пользователях* кредитной истории, включающие ебя наименование (полное и сокращенное) юридического лица, единый государственный регистрационный номер; идентификационный номер налогоельщика; код основного классификатора предприятий и организаций (да- — ОКПО).

Информация в отношении *пользователя* кредитной истории — *индивидуого предпринимателя* включают в себя сведения:

о государственной регистрации физического лица в качестве индивидуального предпринимателя;

фамилию, имя, отчество;

идентификационный номер налогоплательщика;

данные паспорта или иного документа, удостоверяющего личность (номер, дата и место выдачи, наименование органа, выдавшего паспорт или иной документ, удостоверяющий личность);

дату запроса пользователя.

дитная история, субъектом которой является юридическое лицо, в своей ной части содержит информацию, позволяющую детально идентифиить заемщика по следующим параметрам:

наименование (полное и сокращенное) юридического лица;

дрес (местонахождение) постоянно действующего исполнительного ргана юридического лица (в случае отсутствия постоянно действующе- исполнительного органа юридического лица — иного органа или ли-

ца, имеющих право действовать от имени юридического лица без доверенности), по которому осуществляется связь с юридическим лицом, его телефон;

- единый государственный регистрационный номер юридического лица;
- идентификационный номер налогоплательщика.

Кроме того, в тех случаях, когда юридическое лицо подвергалось реорганизации, раздел должен включать в себя:

- наименование (полное и сокращенное) реорганизованного юридического лица, в том числе фирменное наименование, наименование на одном из языков народов Российской Федерации и (или) иностранном языке;
- единый государственный регистрационный номер реорганизованного юридического лица;
- код ОКПО реорганизованного юридического лица.

Общая часть кредитной истории юридического лица должна отражать наличие возможных сведений, характеризующих специфическое правовое положение и способ создания организации-заемщика:

- о прохождении процедуры банкротства, если арбитражным судом принято к производству заявление о признании юридического лица несостоятельным (банкротом);
- о создании юридического лица путем реорганизации на базе юридических лиц, прекративших существование, и их кредитных историях;

Информация в отношении обязательства заемщика — юридического лица, параметры кредитного договора и динамика его исполнения заемщиком практически не отличаются от аналогичной информации в отношении заемщика — физического лица.

Сведения дополнительной (закрытой) части кредитной истории юридического лица в отношении источника формирования и пользователей кредитной истории также не имеют отличий от информации, содержащейся в аналогичном разделе кредитной истории физического лица.

Специфическим отличием данных, характеризующих юридическое лицо как субъекта кредитной истории, может служить его индивидуальный кредитный рейтинг, рассчитанный на основании методик, утвержденных соответствующим бюро кредитных историй. Право получения такого рейтинга заемщиком — физическим лицом Федеральный закон не предусматривает.

Порядок и основания предоставления кредитного отчета для использования информации в установленных законом целях. Право пользоваться информацией, сформированной бюро кредитных историй, Федеральный закон предоставляет:

- пользователю кредитной истории — по его запросу (при наличии согласия субъекта кредитной истории);
- самому субъекту кредитной истории — по его запросу

- Центральному каталогу кредитных историй — в пределах титульной части кредитного отчета;
- суду (судье) по уголовному делу, находящемуся в его производстве;
- органы предварительного следствия по возбужденному уголовному делу при наличии согласия прокурора.

Основанием для предоставления кредитного отчета пользователю кредитной истории является договор об оказании информационных услуг, заключаемый пользователем с бюро кредитных историй.

Информация, содержашаяся в дополнительной (закрытой) части кредитной истории, может быть предоставлена только субъекту кредитной истории. Кроме того, при наличии определенных условий указанная информация может быть предоставлена суду (судье) по уголовному делу, находящемуся в его производстве; органам предварительного следствия по возбужденному уголовному делу, находящемуся в их производстве (с согласия прокурора). Условия и порядок предоставления информации в указанных случаях определяются Правительством РФ.

Физические лица, за исключением индивидуальных предпринимателей, имеют право на получение кредитных отчетов только в тех случаях, когда они являются субъектами соответствующих кредитных историй и запрашиваемых кредитных отчетов.

Все случаи предоставления кредитных отчетов перечисленным выше субъектам фиксируются в закрытой части кредитной истории с детальным описанием ...становочных данных о пользователях (физических и юридических лицах).

Лица, получившие доступ к охраняемым законодательством видам информации, входящим в состав кредитной истории (в том числе работники бюро ...редитных условий), принимают на себя ответственность за сохранение конфиденциальности доверенных им сведений. В случае разглашения или незаконного использования данной информации они несут ответственность в порядке, предусмотренном законодательством Российской Федерации. Обязанность защиты информации кредитных историй в процессе ее обработки, ...анения и передачи Федеральный закон возложил на бюро кредитных ...ий.

Срок хранения кредитных историй, согласно Федеральному закону, ...авляет 15 лет со дня последнего изменения информации об обязательствах ...мщика, содержащейся в кредитной истории.

Анализ содержания информационного массива, формирующегося в Рос... в рамках кредитных историй, позволяет оценить его как принципиально ...ый шаг на пути к обеспечению одной из ведущих сфер банковской безопас...ти. Его создание, с одной стороны, способствует формированию обстановки ...ерия в среде хозяйствующих субъектов. С другой — позволяет значительно ...зить затраты на получение информации, необходимой для выявления ...редупреждения противоправных посягательств в кредитно-финансовой ...ре на ранних стадиях.

9.3. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность банка

Управление системой обеспечения безопасности современного банка связано с необходимостью аналитической обработки в сжатые сроки большого объема разноплановой информации, извлечения из нее определенного вида данных, их правильной оценки и принятия по результатам анализа обоснованных и своевременных решений. Просчеты в указанной деятельности могут повлечь за собой серьезный вред как имущественного, так и нематериального характера.

Вместе с тем, интенсивный рост количества данных, подлежащих поиску, неотложной оценке и осмыслению работниками соответствующих подразделений банка, во многих случаях значительно превышает объективные возможности человека. Это объясняется расширением спектра и объемов банковских услуг, появлением новых банковских технологий и инструментов, а также необходимостью обрабатывать огромные массивы электронных хранилищ информации. Например, одна из зарубежных информационных аналитических систем (Falcon), обслуживающая 16 крупнейших банков мира, контролирует и осуществляет в реальном масштабе времени анализ операций, проводящихся по 250 млн платежных карт. Непосредственная задача этой системы — выявлять и блокировать случаи мошенничества. Само собой разумеется, что выполнить эту задачу человеческими силами без применения специальных технологий невозможно.

Субъекты аналитической деятельности банка и их функции. Отечественные законодательные и иные нормативные правовые предписания государственных органов установили для исполнительных структур российских банков обязанность вести аналитическую обработку соответствующих видов информации с целью выявления опасностей, угрожающих имуществу и порядку функционирования кредитной организации, предупреждения и расследования опасных для банка действий и событий, а также для противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Кроме того, практически любой банк выполняет большой объем аналитических работ в сфере обеспечения безопасности по собственной инициативе.

Основными субъектами указанной аналитической деятельности являются служба внутреннего контроля, служба безопасности и подразделение защиты информации банка, функционирующие в тесном взаимодействии между собой[1].

Об объеме аналитических процедур, выполняющихся в процессе повседневной деятельности одного из многих направлений службы внутреннего контроля банка, дает представление следующий пример. Один только

[1] Подразделение защиты информации может входить в структуру службы безопасности либо функционировать автономно.

законодательно определенный перечень банковских операций, подлежащих обязательному контролю в целях противодействия легализации «грязных» денег и финансированию терроризма, включает в себя описание вероятных способов совершения преступления и сопутствующих ему признаков набором из 23-х ситуаций, которые в свою очередь складываются из 70-ти структурных элементов, имеющих самостоятельное значение[1]. Полной или частичной проверке на соответствие всем этим 1610 признакам подлежит каждая операция, совершающаяся в течение операционного дня.

Не менее трудоемкие и сложные задачи аналитического характера стоят перед службой внутреннего контроля банка на других направлениях ее деятельности. В частности, в сфере выявления и предупреждения должностных правонарушений, защиты установленного порядка доступа к имуществу, к осуществлению операций по счетам и другим элементам функционирования банка.

Для службы безопасности банка характерными задачами являются: многоаспектный анализ обширной информации в целях выявления скрытых связей между объектами сыскной деятельности или объектами внутренних расследований, проверка и оценка значимой для расследования информации; выдвижение необходимых версий, составление планов их проверки и решение иных задач.

Аналитические задачи службы защиты информации банка связаны с контролем использования соответствующих ресурсов его информационно-вычислительной системы, с проверками внутренних нарушений порядка использования информационных ресурсов, попыток «взлома» информационно-вычислительной системы извне и вирусных атак.

Кроме перечисленных выше обязанностей, каждое из названных подразделений должно фиксировать и расследовать выявленные нарушения, разрабатывать рекомендации и указания по их устранению, осуществлять контроль за исполнением этих рекомендаций и указаний, а также за применением мер дисциплинарного и иного воздействия к нарушителям[2].

Объективные данные свидетельствуют о том, что сотрудники банков, выполняющие перечисленные обязанности, испытывают в ходе переработки больших массивов информации постоянно возрастающие нагрузки интеллектуального психологического характера, утомление и снижение внимания, чреватые опасными последствиями.

Данные обстоятельства указывают на объективную необходимость скорейшей автоматизации ряда перечисленных функций и внедрения в сферу обеспечения безопасности российских банков современных аналитических технологий.

[1] Статья 6 Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (ред. от 28 ноября 2007 г. № 275-ФЗ).

[2] Концепция и система безопасности банка. М.: Изд-ль Шумилова И. И., 2003. С. 112.

Автоматизация аналитических операций. Определенный опыт решения аналогичных задач автоматизации поиска знаний, скрытых в большой массе разрозненных данных, их последующего анализа и оценки, накоплен отечественными разработчиками — ЗАО «Институт проблем безопасности». Речь идет об информационно-аналитических комплексах, созданных по заказу правоохранительных органов, спецслужб и ряда коммерческих организаций.

Подобного рода комплексы на базе информационных технологий Data Mining[1] могут быть разработаны для функционирования в предметной области любой организации, испытывающей потребность в аналитической обработке больших массивов информации, в первую очередь электронных банков данных.

Наряду с поиском скрытой информации такие системы позволяют представлять результаты анализа в виде легко воспринимаемых схем, выполненных в терминах и понятиях анализируемой области, и устанавливать интерактивную связь с анализируемыми массивами информации путем непосредственного обращения к отображаемым на схемах объектам. Большим достоинством комплексов является предоставляемая ими возможность выполнять аналитические операции без участия программиста.

В коммерческом банке аналитический комплекс, реализующий информационные технологии Data Mining, может использоваться одновременно или автономно всеми подразделениями, участвующими в сфере обеспечения безопасности. Информационными ресурсами для целей анализа могут служить данные внутренних операционных систем банка, собственные массивы информации службы внутреннего контроля, службы безопасности, службы защиты информации, подразделения по работе с персоналом и других структурных подразделений кредитной организации. При этом право доступа к собственным массивам информации подразделений может быть разграничено внутренними документами банка. Кроме того, система может использовать в автоматическом режиме в заданных ей целях данные сети Интернет (например, Интернет-страницы АУВЕР, РБК и др.), а также содержание информационных баз государственных контролирующих, регистрирующих и иных организаций.

Возможности применения автоматизированного комплекса в целях качественного повышения уровня аналитической работы субъектов обеспечения безопасности банка могут быть реализованы на любом из направлений деятельности соответствующих подразделений.

Так, целям предупреждения злоупотреблением полномочиями и защиты порядка функционирования банка может служить автоматизированный поиск в массиве текущей (и архивной) информации признаков нарушений процедур, функций и полномочий по принятию решений в действиях любого из сотрудников банка и его филиалов.

[1] *Westphial Ch., Blaxton T.* Data Mining Solutions. Methods and Tools for Solving Real-World Problems // WILEY COMPUTER John Wiley & Sons, Inc. New-York «Chichester Weinheim

Для этого в системе создается набор соответствующих шаблонов (заданных параметров), в которых фиксируется верхний предел полномочий каждого сотрудника банка, установленный законодательными и иными нормативными актами, стандартами профессиональной деятельности, внутренними документами, регулирующими деятельность и определяющими политику банка, решениями органов управления кредитной организации и должностными инструкциями.

«Наложение» шаблонов на данные информационных массивов позволяет незамедлительно обнаружить лицо, допустившее отклонения от установленного в банке порядка заключения сделок и выполнения операций. При этом система представляет сведения о содержании и других характеристиках операции, о сути допущенного нарушения, а также о конкретных нормативных предписаниях и обязательствах (в инструкции, договоре), которые нарушил виновный.

По команде пользователя комплекс группирует информацию по времени и видам нарушений, по сотрудникам банка, совершившим нарушения, по клиентам, связанным с выделенными операциями и т. д.

В случае необходимости сфера поиска связей между названными выше объектами (в частности, с данными о клиенте) может быть расширена за пределы внутрибанковских массивов информации. При этом команда пользователя формулируется в текстовом виде либо в форме графического запроса к хранилищу данных путем совмещения соответствующих объектов на выведенной на монитор схеме.

Образец визуального представления результатов аналитической обработки массива информации по заданным параметрам дан на рис. 1.

В целях расследования нарушения может быть также предпринят автоматизированный поиск и анализ содержания связей между:

- конкретным сотрудником банка и другими совершавшимися нарушениями;
- клиентом банка и другими совершавшимися в банке нарушениями;
- клиентом банка и иными лицами, причастными к имевшимся в банке нарушениям порядка функционирования.

Кроме банковских операций, анализу в целях поиска связей между сотрудником банка и клиентом могут быть подвергнуты данные телефонных переговоров, электронной почты и иных массивов информации. При этом программа позволяет вести поиск связей объектов через любое количество уровней (являть цепочки косвенных связей).

Система успешно справляется с задачей установления связей между умышленно раздробленными проводками денежных средств по счетам и наглядной демонстрацией конечного (подлинного) содержания таких операций.

Возможности комплекса могут быть использованы для контроля в автоматическом режиме за адекватным отражением операций банка в учете по установленной форме.

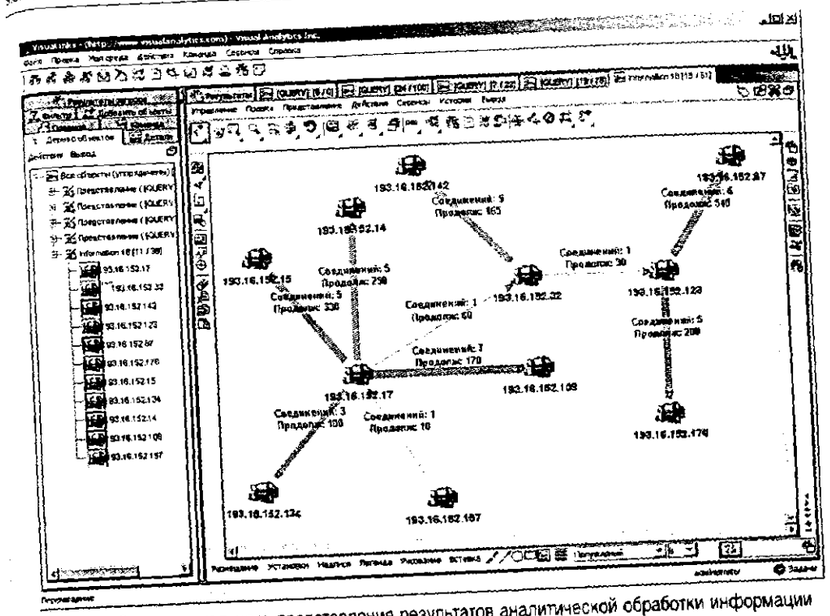

Рис. 1. Схема визуального представления результатов аналитической обработки информации по заданным параметрам

(слева – необработанный информационный массив, справа – данные в структурированном виде)

Возможности расширения поиска связей объекта и их отражения в графической форме представлены на рис. 2*а* (исходные объекты) и рис. 2*б* (результаты поиска связей).

Выявление банковских рисков и угроз. Описанная методика и инструменты поиска признаков нарушений процедур, функций и полномочий субъектов успешно применяются в целях защиты информации банка. Автоматизированный комплекс позволяет преобразовывать в единый формат данные, поступающие из различных контролируемых объектов, вести выявление фактов нарушений порядка доступа к информационным ресурсам и самих нарушителей, четко фиксировать суть и иные обстоятельства нарушений, формировать в визуальной форме запросы на выборку данных, представлять результаты обработки информации в виде отчетных документов с использованием легко воспринимаемых схем и т. д.

Возможности автоматического поиска сведений по заданным параметрам и выявления скрытых связей могут успешно использоваться в целях выявления различного рода банковских рисков и угроз. В частности, кредитного риска, который является основным в процессе банковской деятельности и заключается в неспособности либо нежелании партнера действовать в соответствии с условиями договора.

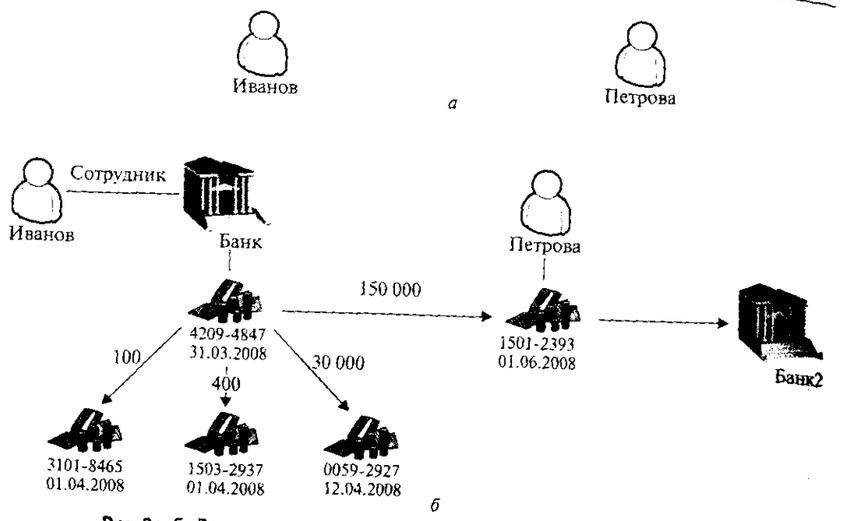

Рис. 2а, б. Возможности расширения поиска связей объекта и их отражения

Кредитная деятельность требует определенных аналитических оценок от-сительно кредитоспособности заемщика. Практика свидетельствует, что кие оценки не всегда точны и корректны. Известно, что кредитный риск чительно возрастает в случае предоставления крупных кредитов так назы-мым связанным заемщикам. Между тем, указанные связи могут быть неяв-ми. Использование представленных выше информационных технологий по-тяет выявить деловые и иные связи между заемщиками или группами заем-ков путем анализа массивов информации о совершенных и планируемых ках, об участии в образовании имущества юридического лица и т. д.

аданные комплексу параметры помогут аналитику в выявлении в иссле-ых массивах информации сведений о сотрудниках банка, которые могут признаны лицами, заинтересованными в операциях (сделках). Напом-что набор признаков возможной личной заинтересованности сотрудника чает в себя более 20 элементов, находящихся в прямой либо опосредо-й зависимости. В их числе — владение акциями (долями, паями) юри-кого лица, являющегося стороной операции (сделки) или участвующего в качестве представителя или посредника; участие сотрудника в органах ления юридического лица; участие родственников сотрудника в сделке; ление у родственников во владении акций (долей, паев); участие родствен-сотрудника в органах управления юридического лица, являющегося ой сделки, и т. д. Разноплановость названных признаков и разрозне-источников сведений, подлежащих изучению для их поиска, делают о» обработку информации весьма непродуктивной, а ее результаты —

не всегда полными и достоверными. И наоборот, применение в данном случае автоматизированного комплекса аналитической обработки информации качественно повышает эффективность работы аналитика.

Как уже упоминалось, информационные технологии Data Mining могут быть использованы для выявления и блокирования попыток мошеннических операций с платежными картами.

При этом в основе поисковой и аналитической деятельности в указанном случае лежит все то же использование соответствующих шаблонов (моделей, заданных параметров). Система содержит в себе, а затем распознает в реальном режиме времени модели различного типа мошенничества в кредитной сфере. Финансовые операции по выявленным попыткам мошенничества автоматически блокируются. Фактические данные для создания моделей мошенничества собираются специалистами банка и постоянно обновляются с учетом последней информации о случаях мошенничества.

Еще одна особенность автоматизированного комплекса — его способность самостоятельно выявлять типичные признаки анализируемой (в нашем случае противоправной) деятельности и участвующих в ней лиц (юридических и физических). В этих целях аналитической обработке подвергается информация о достоверно известных фактах правонарушений. Такой прием позволил нам, например, установить типичные характеристики джекоммерческих организаций (фирм прикрытия), использующихся для совершения мошенничества при заключении банковских договоров и операций для легализации «грязных» денег. Были выявлены также типичные признаки имитации клиентами производственной и коммерческой деятельности (когда деятельность не проводится вовсе), а также коммерческой деятельности в форме оказания интеллектуальных (маркетинговых) услуг и т. д. Указанные параметры состоят из нескольких десятков элементов.

Использование этих параметров при аналитической обработке соответствующих массивов информации показало высокую поисковую эффективность и надежность оценки подлинных намерений потенциальных клиентов (см. рис. 3).

На рис. 3 слева представлена типовая схема движения денежных средств «по кругу» в целях имитации финансовой деятельности; справа — конкретные факты таких маскировочных действий, отобранные системой.

Существенным направлением информационно-аналитической поддержки субъектов обеспечения безопасности банка (в частности, службы безопасности) является возможность представления результатов сыскной (проверочной) деятельности предполагаемого клиента или проведенного внутреннего расследования в виде визуальных моделей, отражающих:

- обстоятельства, подлежащие проверке;
- мероприятия, которые необходимо выполнить в целях проверки;
- факт выполнения и результаты выполненных мероприятий, источники и материалы для обоснования принятого решения.

- степень полноты полученных сведений, позволяющих принять окончательное решение по делу.

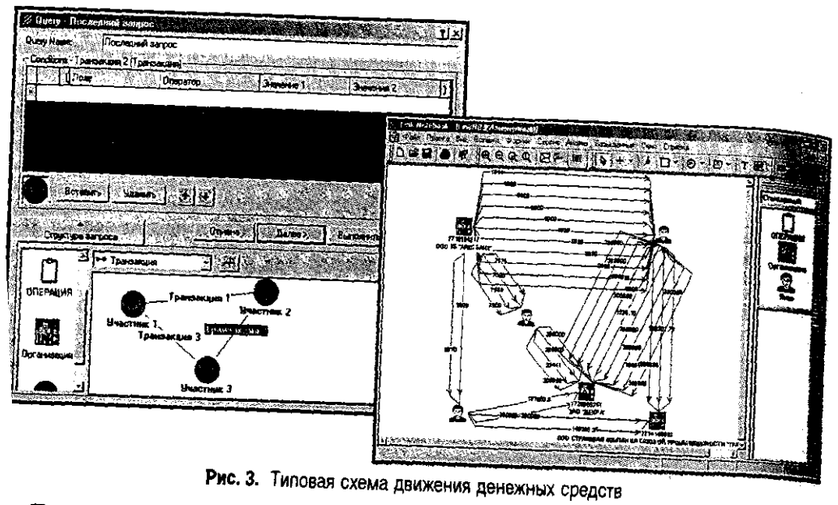

Рис. 3. *Типовая схема движения денежных средств*

Так, например, стандартная проверка потенциального клиента с целью ...едупреждения мошенничества (и риска невозврата кредита) при заключе...ии кредитного договора (договора займа) предполагает выполнение, фикса...ю и анализ службой безопасности банка результатов следующих действий, ...правленных на проверку подлинности:

- сведений и документов, удостоверяющих право организации заключать договор займа в объеме и на условиях, предусмотренных проектом договора, а также документов, удостоверяющих личность руководителя или представителя организации, наличие у них соответствующих полномочий на получение кредита, правильность оформления доверенности и т. д.;
- сведений, подтверждающих реальное существование организации заемщика, путем изучения уставных документов, сведений из налоговых органов и др., соответствия кредитуемой сделки законодательству и уставным документам заемщика. В частности, получить информацию о наличии у организации-заемщика постоянных производственных и складских помещений, об объемах товаров или продукции, которыми располагает фирма;

способности заемщика заработать средства для погашения долга и возвратить кредит (анализируются сведения о продолжительности присутствия фирмы на рынке товаров и услуг, наличие положительных экономических показателей, изучаются кредитная история (получал ли заемщик кредиты в других кредитных организациях, не допускал ли нарушений

при их получении; как использовались деньги, полученные в качестве ...кредита; не было ли проблем с возвратом денег банку) и репутация в деловом мире партнеров (контрагентов, кредиторов, банков);

- вложения собственного капитала заемщика в кредитуемое дело (данные балансовых ведомостей, расчетно-кассовые документы и другая документация первичного учета, наличие достаточных объемов реального товара или продукции);
- документов о вторичных источниках погашения долга (договора о залоге, гарантии, поручительства, страхового свидетельства). Проверяется их точное соответствие нормам гражданского законодательства, наличие возможных признаков материального и интеллектуального подлога. Выясняется, отражен ли факт выдачи гарантийного письма, страхового свидетельства и проч. в соответствующих документах поручителя;
- целей испрашиваемого кредита, а также сведений, раскрывающих содержание и механизм предполагаемого контракта по всей технологической цепочке от момента производства до доставки к месту реализации; ...о характере деятельности предполагаемых контрагентов потенциального заемщика; о возможности контрагентов поставить заемщику товар ожидаемой номенклатуры и качества в названные сроки, вид и количество транспортных единиц, которые предполагается использовать, наличие соответствующих договоров на доставку товара (сырья).

После заключения кредитного договора служба безопасности банка обязана контролировать ход его исполнения с целью своевременного выявления ...обстоятельств, которые могут препятствовать возврату кредита. При возникновении таких обстоятельств принимать меры к минимизации ущерба[1].

Автоматизированный комплекс предоставляет возможность сотруднику службы безопасности (аналитику) самостоятельно создать графическую схему, представляющую процедуру и результаты проверки на экране монитора (рис. 4).

Указанная схема формируется в режиме диалога с комплексом. Данные об анализируемых объектах и связях между ними вводятся в компьютер в виде графической схемы, которая выполняется пользователем непосредственно на экране. Для графического обозначения объектов пользователь выбирает значки из предлагаемого программой набора шаблонов и «выводит» их в рабочее поле экрана. Связи между объектами фиксируются путем проведения между ними схематических линий. Одновременно с этим программа позволяет дополнять графическое изображение зафиксированных объектов и их связей текстовой информацией. Это дает пользователю возможность наделить объекты и связи признаками (атрибутами), которые имеют самостоятельное поисковое значение и используются в последующем компьютерном анализе. В обычном

[1] *Гамза В. А., Ткачук И. Б.* Безопасность коммерческого банка: учеб.-практ. пособие. М.: Изд-ль Шумилова И. И., 2000. С. 27.

режиме работы текстовая информация находится в скрытом состоянии. Она «выводится» на экран в специальном «окне», которое открывается непосредственно на схеме по команде пользователя относительно конкретного объекта или связи. Содержание текстовой информации может меняться в диалоговом режиме путем внесения новых сведений непосредственно в поле «окна».

Рис. 4. Схема процедуры проверки

Каждый из объектов содержит в «свернутом» виде информацию, представ-нную выше в текстовой форме, однако в случае необходимости «разворачи-тся» по команде пользователя. По мере поступления сведений о результа-проверки он пополняется путем непосредственного внесения информации зу данных через экран монитора.

Сформированная модель проверочных мероприятий и полученных факти-ких данных позволяет представить собранную информацию в цельном, бном для восприятия виде. Удобству восприятия способствует возможность бражения отдельных групп объектов и их связей в различных цветах.

Кроме того, модель указанного вида обладает рядом динамических свойств, рые позволяют группировать собранную информацию в соответствии лями аналитических процедур. В частности, зафиксированные моделью тели информации могут выделяться по команде пользователя из общего ива данных по признакам вида, источника информации (лицо, докумен-места обнаружения, наличия связей и их типа и т. д.

Соответственно, наряду с общей схемой всех зафиксированных объектов, ль представляет частные схемы их отдельных групп (например, признаки, тельствующие о фиктивном характере организации-заемщика).

Результаты указанных процедур позволяют аналитику получить, не упустив даже самых незначительных деталей, четкое представление о содержании и целях проверочных действий, об имеющейся фактической информации, которая может быть использована для оценки подлинных намерений организации-заемщика, и т. д.

Кроме того, одновременно с аналитической обработкой имеющейся фактической информации сотрудник службы безопасности может использовать функции комплекса для поиска недостающих данных в других массивах сведений.

ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. В чем заключается основная цель информационного обеспечения безопасности банка?
2. Какие отрасли и нормы права регламентируют цели, источники, порядок получения и использования информации для обеспечения безопасности банка?
3. Какие источники информации используются в целях обеспечения безопасности банка?
4. Из каких структурных элементов состоит единая система сведений об участниках кредитных операций в России?
5. Какие функции информационного обеспечения выполняет Центральный каталог кредитных историй?
6. В каких информационных массивах находится содержательная (основная) часть кредитных историй?
7. Кто является источником формирования кредитной истории?
8. Кто может быть пользователем кредитного отчета? Каков порядок и основания предоставления кредитного отчета пользователю?
9. Кто являются основными субъектами аналитической деятельности в сфере обеспечения безопасности банка и каковы их функции?
10. Чем вызвана необходимость автоматизации банковских операций?
11. Какие принципиально новые возможности аналитической обработки информации дает применение компьютерных технологий?

СПИСОК ЛИТЕРАТУРЫ

Нормативные источники

Конституция Российской Федерации.

Гражданский кодекс Российской Федерации (принят Федеральным законом от 30 ноября 1994 г. № 51-ФЗ).

Уголовный кодекс Российской Федерации (принят Федеральным законом от 13 июня 1996 г. № 63-ФЗ).

Уголовно-процессуальный кодекс Российской Федерации (принят Федеральным законом от 18 декабря 2001 г. № 174-ФЗ).

Кодекс Российской Федерации об административных правонарушениях (принят Федеральным законом от 30 декабря 2001 г. № 195-ФЗ).

Трудовой кодекс Российской Федерации (принят Федеральным законом от 30 декабря 2001 г. № 197-ФЗ).

Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

Закон Российской Федерации от 22 марта 1991 г. № 948-1 «О конкуренции и ограничении монополистической деятельности на товарных рынках» (с изм. от 7 марта 2005 г.).

Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации».

Закон Российской Федерации от 5 марта 1992 г. № 2446-I «О безопасности».

Закон Российской Федерации от 21 июля 1993 года № 5485-1 «О государственной тайне».

Закон Российской Федерации «О частной детективной и охранной деятельности в Российской Федерации» от 11 марта 1992 г. № 2487-1.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».

Федеральный закон от 11 января 1995 года № 4-ФЗ «О счетной палате Российской Федерации».

Федеральный закон от 26 декабря 1995 г. № 208-ФЗ «Об акционерных обществах».

Федеральный закон от 3 февраля 1996 г. № 17-ФЗ «О внесении изменений и дополнений в Закон РСФСР «О банках и банковской деятельности в РСФСР».

Федеральный закон от 21 ноября 1996 г. № 129-ФЗ «О бухгалтерском

Федеральный закон от 28 мая 2001 г. № 62-ФЗ «О ратификации Конвенции об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности».

Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Федеральный закон от 8 августа 2001 г. № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей».

Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».

Федеральный закон от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе в Российской Федерации».

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

Конвенции от 7 июня 1930 г. «О единообразном законе о переводном и простом векселе», «Конвенция, имеющая целью разрешение некоторых коллизий законов о переводных и простых векселях», «О гербовом сборе в отношении переводного и простого векселя».

каз Президента Российской Федерации от 29 апреля 1996 г. № 608 «Об одобрении Государственной стратегии экономической безопасности Российской Федерации».

аз Президента Российской Федерации от 17 декабря 1997 г. № 1300 «Об утверждении Концепции национальной безопасности Российской Федерации».

з Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

Президента Российской Федерации от 10 января 2000 г. № 24 «О концепции национальной безопасности Российской Федерации».

ановление Правительства Российской Федерации от 27 декабря 1996 г. 1569 «О первоочередных мерах по реализации Государственной стратеи экономической безопасности Российской Федерации».

новление Правительства Российской Федерации от 23 июня 2004 г. 307 «Об утверждении положения о Федеральной службе по финансовомониторингу».

новление Правительства Российской Федерации от 19 июня 2002 г. 38 «Об утверждении правил ведения Единого государственного реестра дических лиц и предоставления содержащихся в нем сведений».

овление Правительства Российской Федерации от 16 октября 2003 г. 30 «Об утверждении правил ведения Единого государственного реестра видуальных предпринимателей и предоставления содержащихся в нем ний».

Приказ Федеральной налоговой службы от 21 октября 2004 г. № САЭ-3–09/7@ «Об утверждении Порядка предоставления в электронном виде сведений, содержашихся в Едином государственном реестре юридических лиц и в Едином государственном реестре индивидуальных предпринимателей».

Приказ Банка России от 15 сентября 1997 г. № 02–395 «О порядке подготовки и вступления в силу нормативных актов Банка России».

Положение Банка России от 16 декабря 2003 г. № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах».

Указание Центрального Банка Российской Федерации от 7 июля 1999 г. № 603-У «О порядке осуществления внутреннего контроля за соответствием деятельности на финансовых рынках законодательству о финансовых рынках в кредитных организациях».

Письмо Центрального Банка Российской Федерации от 17 августа 2004 г. № 100-Т «Об отчете ФАТФ по типологиям отмывания преступных доходов и финансирования терроризма 2003–2004 годы»

Письмо Центрального Банка Российской Федерации от 13 июля 2005 г. № 99-Т «О методических рекомендациях по разработке кредитными организациями правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Положение Банка России от 12 апреля 2001 г. № 2-П «О безналичных расчетах в Российской Федерации».

Положение Банка России от 9 октября 2002 г. № 199-П «О порядке ведения кассовых операций на территории Российской Федерации».

Положение Центрального Банка Российской Федерации от 19 августа 2004 г. № 262-П «Об идентификации кредитными организациями клиентов и выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Постановление Пленума Верховного Суда РФ от 18 августа 1992 г. № 11 «О некоторых вопросах, возникших при рассмотрении судами дел о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц».

Обзор практики рассмотрения споров, связанных с исполнением и расторжением кредитных договоров. Письмо Высшего Арбитражного Суда РФ от 26 января 1994 г. № ОЩ-7/О.

Обзор практики разрешения споров, связанных с использованием векселя в хозяйственном обороте. Приложение к информационному письму Президиума Высшего Арбитражного Суда Российской Федерации от 25 июля 1997 г. № 18.

Обзор практики рассмотрения споров, связанных с применением арбитражными судами норм Гражданского кодекса Российской Федерации о залоге. Приложение к письму Высшего Арбитражного Суда РФ от 15 января 1998 г. № 26.

Постановление Пленума Верховного Суда Российской Федерации № 33, Пленума высшего Арбитражного Суда Российской Федерации от 4 декабря 2000 г. № 14 «О некоторых вопросах практики рассмотрения споров, связанных с обращением векселей».

Постановление Президиума Высшего Арбитражного Суда Российской Федерации от 14 октября 2003 г. № 5278/03.

остановление Девятого арбитражного апелляционного суда г. Москвы от 31 декабря 2004 г. № 09АП-6183/04-ГК.

остановление Пленума Верховного Суда РФ от 18 ноября 2004 г. № 23 «О судебной практике по делам о незаконном предпринимательстве и легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем».

иказ МВД РФ от 1 ноября 2001 г. «Об утверждении инструкции о порядке предоставления гражданам справок о наличии (отсутствии) у них судимости.

иказ МВД России от 21 января 2005 г. № 33 «Об объявлении Положения Главном информационно-аналитическом центре Министерства внутренних дел Российской Федерации».

Литература

овское дело: учеб. / под ред. О. И. Лаврушина. М.: Финансы и статисти-, 1999.

В. А. Вексельные преступления // Законодательство. 1997. № 5.

ой экономический словарь / под ред. А. Н. Азрилияна. 4-е изд., пере-. и доп. М.: Институт новой экономики, 1999.

ов В. А., Богданова Т. С., Тишкова Н. Ю. Проведение полиграфных проок при решении кадровых вопросов: Опыт использования полиграфа рофлактике и раскрытии преступлений в ГУВД Краснодарского края научно-практическая конференция). Краснодар, 1997.

ьное дело» закрыто // Российская газета. 2003. № 26(3140). 11 февр.

А. Опыт работы ОАО «Внешторгбанк» по реализации положений ерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем» // Тезисы выступления на V Всероссийской конференции «Банковская безопасность: состояние и перспективы развития».

А. Методологические основы системной классификации банковских в // Банковское дело. 2001. № 6, 7.

Гамза В. А. Настольная книга предпринимателя. Банковские операции, финансовые инструменты, консалтинговые услуги: учеб.-практ. пособие. М.: Изопроект, 2004.

Гамза В. А. Проблемы выявления, пресечения и раскрытия ненасильственных преступных посягательств на безопасность коммерческого банка // Российская юридическая доктрина в XXI веке: Проблемы и пути их решения: научн.-практ. конференция / под. ред. А. И. Демидова. Саратов: СГАП, 2001.

Гамза В. А., Ткачук И. Б. Безопасность коммерческого банка: Организационно-правовые и криминалистические проблемы: монография. М.: Изд-ль Шумилова И. И., 2002.

Гамза В. А., Ткачук И. Б. Безопасность коммерческого банка: учеб.-практ. пособие. М.: Изд-ль Шумилова И. И., 2000.

Герасимов А. В. Инкомбанке похищали курсовую разницу // Коммерсантъ. 2003. № 36/П(32 539). 3 марта.

Гудков Ф. А. Вексель. Дефекты формы. (Методики выявления типичных ошибок). 2-е изд., доп. и испр. М.: ЗАО ИПК «Интеркрим-пресс», 2000.

Деньги вкладчика Сбербанка отдали мошенникам по фальшивой доверенности // Коммерсантъ. 2003. № 6. 17 янв.

Доклад Федерального бюро расследований Конгрессу США (http://www.fbi.gov/congress02/lormel021 202.htm).

Доронин А. И. Бизнес-разведка. 2-е изд., перераб. и доп. М.: Ось-89, 2003.

Дульман П. Карточка ваша, деньги наши // Российская газета. 2003. № 29(3193). 24 апр.

Жеглов А. Фальшивомонетчиками руководил работник Гознака // Коммерсантъ. 2004. № 188. 10 окт.

Ивасенко А. Г. Банковские риски. М.: Вузовская книга, 1998.

Иващенко Г. В. О понятии «безопасность» // Credo. 1999. № 24.

Иоффе Л. Г. Источники вексельного права // В мире права. 1999. № 1.

Ипполитов К. Х. Экономическая безопасность России в условиях формирования рыночных отношений и система мер ее обеспечения. М.: РСПП, 1996.

Казакевич О. Некоторые проблемы информационной безопасности банковского сообщества // Вестник АРБ. 2003. № 19.

Кареев В. Н. «Современные тенденции борьбы с фальшивомонетничеством». Выступление на VI Всероссийском форуме «Банковская безопасность: состояние и перспективы развития». 15–17 октября 2003 г. Москва.

Ковалев В. В. Введение в финансовый менеджмент. М.: Финансы и статистика, 1999.

Концова М. Тайные сделки Центробанка продаются за $100 // Утро.ru. 2005. № 143 (1904). 20 мая.

Крахмалев А. К. Безопасность учреждений кредитно-финансовой системы. Технические средства охранной сигнализации // Банковское дело. 2003. № 5.

Криминалистика: учеб. для вузов / под ред. проф. А. Ф. Волынского. М.: Закон и право; Юнити-Дана, 2000.

Ларичев В. Д. Как уберечься от мошенничества в сфере бизнеса. М.: Юрист, 1996.

Максимов А. А. Бандиты в белых воротничках: Как разворовывали Россию. М.: ЭКСМО-Пресс, 1999.

Мартынова Т. Люди — самое слабое звено // Банковское обозрение. 2004. № 10.

Масич А. Экспертиза ценных бумаг — барьер на пути подделок // Депозитариум. 2000. № 1(20).

Международные валютно-кредитные и финансовые отношения: учеб. / под ред. Л. Н. Красавиной. 2-е изд., перераб. и доп. М.: Финансы и статистика, 2000.

Мельников Ю. Н. Информационная безопасность в банке: Проблемы и рекомендации // Банковские технологии. 1997. № 7.

Милашев В. А. Проблемы поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ. Дис. ... канд. юрид. наук. М., 2004.

Принципы безопасности банка и банковского бизнеса в России / под общ. ред. А. Г. Шаваева. М.: Концерн «Банковский Деловой Центр», 1997.

Пятиизбенков Н. П. «Фишинг» новый вид мошенничества с использование банковских карт // VII Всероссийский форум «Банковская безопасность: состояние и перспективы развития»: тезисы конференции. М., 2005.

Рачин Р. Своя разведка: практ. пособие. Мн.: Харвест, 1997.

Ровский К. О последствиях совершения руководителем сделок вопреки интересам организации // Хозяйство и право. 1998. № 5.

Родкая М. С. Надежность, эффективность, качество систем управления // Credo. 1999. № 17 (www.credo.osu.ru).

Справка комиссии Государственной думы Федерального Собрания Российской Федерации по борьбе с коррупцией по результатам проверки материалов о хищении организованной группой лиц денежных средств со счета ОО «Валта» 3 июня 2002 года // Нацбез.Ру. 2005. 26 мая.

Ставук И. Б. Коммерческая тайна: Организация защиты, расследование посягательств. М.: Щит-М, 1999.

Сухоруков А. Идет охота на предпринимателей // Деловое Прикамье. 2004. 7 дек.

Тавасиев В. М. Современный коммерческий банк: Управление и операции. М.: Тикор, 1998.

Финансово-кредитный энциклопедический словарь / под общ. ред. А. Г. Грязновой. М.: Финансы и статистика, 2002.

Франке Д. Враг в собственных рядах: Преступность среди сотрудников банков // Вестник АРБ. 2005. № 8.

Чернышев А. Кредитные мошенники сели добровольно // Коммерсантъ. 2005. № 5/П. 17 янв.

Шумилов А. Ю. Краткая сыскная энциклопедия: Деятельность оперативно-розыскная, контрразведывательная, частная сыскная (детективная). М.: Изд-ль Шумилова И. И., 2000.

Эриашвили Н. Д. Банковское право: учеб. для вузов. М.: Закон и право; Юнити-Дана, 1999.

Westphial Ch., Blaxton T. Data Mining Solutions. Methods and Tools for Solving Real-World Problems // WILEY COMPUTER John Wiley & Sons, Inc. New-York «Chichester Weinheim» Bri, 1998.

Приложение

ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫЕ ДОКУМЕНТЫ, СВЯЗАННЫЕ С ЗАЩИТОЙ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА (БАНКОВСКОЙ, КОММЕРЧЕСКОЙ И СЛУЖЕБНОЙ ТАЙНЫ)

ПОЛОЖЕНИЕ
(проект)
Об организации защиты сведений конфиденциального характера, составляющих банковскую, коммерческую и служебную тайну либо относящихся к компьютерной информации

(*название банка*)

1. Общие положения

1. Настоящий документ, разработанный в соответствии с требованиями
титуции Российской Федерации, Гражданского кодекса Российской Фе-
ции, Закона Российской Федерации «Об информации, информатизации
ите информации», Федерального закона «О коммерческой тайне», Зако-
Российской Федерации «О банках и банковской деятельности», других
нативных актов Российской Федерации, устанавливает порядок определе-
банке сведений, составляющих банковскую (коммерческую) тайну (*да-
тексту — конфиденциальная информация и защищаемая информация*),
овные требования, относящиеся к ее защите.

Устанавливаемый настоящим положением порядок распространяется
виды деятельности, связанной с приборами, средствами электрон-
числительной техники, оперативной полиграфии, изделиями, докумен-
изданиями, имеющимися в банке, независимо от их местонахождения
а создания (*этот перечень может быть дополнен другими конкретными
ми по усмотрению руководителя организации*).

Зашите в качестве конфиденциальных сведений в банке подлежат све-
относящиеся к содержанию и результатам деятельности банка, непра-
ое ознакомление с которыми третьих лиц может причинить ущерб бан-
лиентам или корреспондентам.

Источником сведений, составляющих банковскую, коммерческую
бную тайну банка, являются: информация, полученная в результате уча-
ка в ее создании, от контрагентов по договору, а также приобретенная
способами, не противоречащими действующему законодательству
кой Федерации.

1.5. Сведения, подлежащие защите в качестве конфиденциальных, классифицируются по содержанию составляющей их информации на банковскую (коммерческую) тайну и охраняемую законом компьютерную информацию.

1.6. Режим конфиденциальности сведений, составляющих банковскую, (коммерческую) тайну и охраняемую законом компьютерную информацию, устанавливается с учетом возможного материального и иного ущерба в случае их неправомерного использования третьими лицами.

1.7. Документам, содержащим сведения, составляющие банковскую (коммерческую) тайну, присваивается гриф: «конфиденциально — банковская тайна», «конфиденциально — коммерческая тайна».

2. Определение сведений, подлежащих защите в качестве банковской, (коммерческой) тайны банка

2.1. Банковскую тайну составляют установленные законом тайна банковского счета, тайна банковского вклада, тайна операций по счету, сведения о клиентах и корреспондентах, а также иные сведения, устанавливаемые кредитной организацией, если это не противоречит федеральному закону[1].

Включение в число подлежащих защите «иных» сведений, составляющих банковскую (коммерческую) тайну, осуществляется постоянно действующей комиссией банка по защите банковской (коммерческой) тайны (*далее — комиссия*).

2.2. Комиссия формируется из руководителей и сотрудников *(приводится перечень и наименование ведущих структурных подразделений банка).*

2.3. В целях исполнения возложенных на нее обязанностей комиссия может создавать рабочие группы из числа сотрудников банка, привлекать для консультаций отдельных специалистов банка, осуществлять в указанных целях взаимодействие с представителями правоохранительных органов и специальных служб Российской Федерации и иных структур государственной и негосударственной форм собственности.

2.4. Для выявления конфиденциальных сведений, подлежащих защите, комиссия проводит опрос ведущих сотрудников основных структурных подразделений банка по специально разработанной форме с учетом их знаний и профессионального опыта.

[1] К числу «иных» сведений могут относиться: данные аналитических и специальных исследований о состоянии и тенденциях развития рынка, о надежности и финансовой устойчивости клиентов (в том числе потенциальных); сведения о средствах и способах обеспечения работы автоматизированных информационных систем и их технологий (программных, технических, лингвистических и организационных); сведения, раскрывающие систему, средства и методы защиты информации на средствах вычислительной техники банка от несанкционированного доступа, а также значения действующих кодов и паролей; информация о деятельности по защите интересов банка; о лицах (сотрудниках и клиентах банка), участвующих в деятельности банка и банковских операциях, а также о силах, средствах и способах обеспе-

2.5. Предложения специалистов подвергаются экспертной оценке комиссии с целью обоснования экономической целесообразности закрытия свободного доступа к сведениям третьих лиц.

2.6. Решение комиссии об отнесении сведений к категории защищаемой информации оформляется в виде проекта перечня основных категорий сведений, составляющих банковскую (коммерческую) тайну банка.

2.7. Перечень основных категорий сведений, составляющих банковскую, коммерческую) тайну банка, вступает в силу после утверждения его руководителем банка.

Проект перечня вместе с документами, содержащими обоснование экономической целесообразности закрытия свободного доступа к тем или иным сведениям, хранится в материалах комиссии[1].

Содержание перечня пересматривается комиссией по мере необходимости обновления включенных в него сведений, но не реже одного раза в два года.

2.8. Основанием для отмены ограничений на свободный доступ к сведениям, отнесенным ранее к категории защищаемой информации, является утрата ими коммерческой ценности.

2.9. В результате пересмотра перечня комиссия может внести руководителю банка предложение об отмене ограничений на свободное ознакомление отдельными сведениями или отдельными категориями сведений и исключении их из перечня.

2.10. Ограничение на свободное ознакомление с отдельными сведениями или отдельными категориями сведений, указанными в перечне, снимается в день утверждения руководителем банка соответствующего предложения комиссии.

3. Закрытие свободного доступа к сведениям, составляющим банковскую (коммерческую) тайну

3.1. Свободный доступ к сведениям, составляющим банковскую (коммерческую) тайну, закрывается с целью защиты конфиденциальной информации технической защиты ее носителей.

3.2. Обеспечение исполнителей конфиденциальной информацией, необходимой для выполнения порученных работ, осуществляется с письменного разрешения руководителя банка в соответствии с установленными в банке правилами доступа к сведениям, составляющим банковскую (коммерческую) тайну.

Сотрудник банка (*исполнитель*) обеспечивается сведениями, составляющими банковскую (коммерческую) тайну, в объеме, необходимом для качественного и своевременного выполнения порученных ему работ. Ознакомление исполнителя с конфиденциальной информацией, не имеющей отношения к выполняемой им работе, запрещается.

3.4. Для получения разрешения на выполнение работ, связанных с банковской (коммерческой) тайной, сотрудники банка обязаны пройти соответствующую проверку и принять на себя обязательства о соблюдении установленных в банке правил обращения с указанными сведениями и их носителями.

3.5. Руководитель банка вправе разрешить по своему усмотрению подразделение сведениями, составляющими банковскую (коммерческую) тайну, любому работнику подразделения банка или лицу, прибывшему из другой организации, если в отношении этих сведений не установлены ограничения со стороны контрагентов (*партнеров по совместной деятельности*).

3.6. При большом объеме закрытых работ руководитель банка может передать обязанность распределения защищаемых сведений руководителям структурных нижестоящих подразделений.

Руководители структурных нижестоящих подразделений в указанных случаях распределяют сведения, составляющие банковскую (коммерческую) тайну, между исполнителями только в пределах работ, выполняемых подразделением.

3.7. Конфиденциальные договоры с другими организациями, отчеты о результатах работы по перспективным направлениям и другие наиболее ценные сведения, как правило, находятся в личном распоряжении руководителя банка. Перечень указанных документов хранится в подразделении защиты интересов банка. Вся соответствующая перечню информация, подготовленная в банке или поступившая извне, докладывается руководителю банка.

4. Организация правомерного доступа сотрудников к сведениям, составляющим банковскую (коммерческую) тайну

4.1. Лица, желающие получить право на работу, связанную со сведениями, составляющими банковскую (коммерческую) тайну, проходят проверку с целью выявления возможных обстоятельств, препятствующих их доступу к защищаемым сведениям (*проверку на право доступа к защищаемым сведениям*).

4.2. Проверка осуществляется подразделением защиты интересов банка (*либо иной частной коммерческой службой по договору*) путем сбора биографических и других характеризующих личность данных в пределах, установленных ст. 3 Закона РФ «О частной детективной и охранной деятельности в Российской Федерации».

4.3. Основанием для проведения проверки является письменное согласие проверяемого и поручение руководителя структурного подразделения банка, наделенного правом распределения защищаемой информации.

4.4. Основаниями для отказа лицу в допуске к защищаемым сведениям банка являются:

- наличие судебного решения о признании лица недееспособным или ограниченно дееспособным, нахо-

---

[1] Поскольку содержание перечня само по себе может представлять интерес для недобросовестных конкурентов, руководитель организации (банка) вправе принять решение об отнесении его и конфиденциальных документов и присвоении ему соответствующего грифа конфиденци-

за тяжкие и особо тяжкие преступления, наличие у лица неснятой судимости за эти преступления;

- наличие медицинских противопоказаний для работы с использованием сведений, составляющих коммерческую тайну; выявление в результате проверочных мероприятий действий оформляемого лица и обстоятельств, создающих угрозу незаконного получения и разглашения сведений, составляющих банковскую, коммерческую и служебную тайну;
- уклонение проверяемого от проверочных мероприятий и (или) сообщение заведомо ложных анкетных данных.

.5. Заключение о результатах проверки с выводами о пригодности либо ригодности кандидата для работы с защищаемыми сведениями докладыва- руководителю банка.

.6. Окончательное решение о допуске лица к работе с защищаемой ин- мацией принимает руководитель банка.

7. Разрешение на доступ лица, прошедшего проверку, к работе с защи- ой информацией оформляется приказом по банку с указанием фамилии, и, отчества, должности лица и документов, к которым он допускается.

8. Наличие обстоятельств, препятствующих допуску к защищаемым све- ам, является основанием для отказа в приеме лица на работу, связанную ведениями, составляющими банковскую (коммерческую) тайну банка, прекращения ранее заключенного трудового договора (*контракта*) между м и указанным лицом.

). Допуск к сведениям, составляющим банковскую (коммерческую) тай- жет быть прекращен по решению руководителя банка в случае нарушередусмотренных трудовым договором (*контрактом*) обязательств граж- а, связанных с сохранением защищаемой информации, а также при воз- вении обстоятельств, являющихся основанием для отказа лицу ске к банковской (коммерческой) тайне.

). Прекращение допуска гражданина к защищаемой информации явля- снованием для расторжения трудового договора (*контракта*) с ним, есое условие предусмотрено в этом договоре (*контракте*).

. Решение руководителя банка о прекращении допуска гражданина овской (коммерческой) тайне и расторжении на основании этого тру- договора (*контракта*) с ним может быть обжаловано в суде.

. Материалы проверки хранятся в личном деле сотрудника. Выписка каза о допуске сотрудника к работе с конфиденциальной информацией ляется в подразделение защиты интересов банка.

. В случае необходимости дополнительного ограничения доступа к до- ам, имеющим особо важное значение для банка, разрешение на допуск оформляться в виде отдельного списка лиц, имеющих право работать щаемой информацией, либо в виде резолюции руководителя банка м защищаемом документе.

4.14. В отдельном списке могут быть определены конкретные должностные лица банка, которые допускаются руководителем ко всем без исключения документам и изделиям без дополнительных письменных разрешений. В них указываются фамилия, имя и отчество исполнителя работ, наименование подразделения, в котором он работает, занимаемая должность, категория документов и изделий, к которым он допущен.

4.15. Отдельный список готовится руководителем структурного подразделения, согласовывается с подразделением защиты интересов банка и утверждается руководителем банка.

4.16. Право на доступ может быть оформлено в виде персональной карточки — разрешения на доступ к защищаемой информации.

4.17. Представители контрагентов и государственных структур могут быть допущены к защищаемым сведениям только с письменного разрешения руководителя банка или его заместителей, с указанием содержания и объема защищаемой информации, подлежащей ознакомлению.

5. Порядок работы со сведениями, составляющими банковскую (коммерческую) тайну

5.1. Документы, содержащие сведения, составляющие банковскую (коммерческую) тайну, классифицируются исполнителем на стадии их разработки (*подготовки*). При этом им присваиваются регистрационный номер и гриф конфиденциальности.

Режим конфиденциальности документа определяется на основании классификации, установленной в перечне основных категорий сведений, подлежащих защите в качестве банковской (коммерческой) и служебной тайны .

5.2. Классифицированные документы, поступившие извне, принимаются и регистрируются подразделением защиты информации (защиты интересов банка).

5.3. Все факты выдачи защищаемых документов учитываются подразделением защиты информации (*защиты интересов банка*) с указанием основания доступа (*разрешения*), фамилии, имени, отчества и должности лица, получившего доступ к документу, и даты события.

5.4. Безучетная и несанкционированная выдача защищаемых документов запрещается.

5.5. Запрещается внесение изменений в учеты выдачи защищаемых документов, а также замена учетных документов.

6. Участие сотрудников в защите сведений, составляющих банковскую (коммерческую) и служебную тайну

6.1. Лица, прошедшие проверку на право доступа к сведениям, составляющим банковскую (коммерческую) тайну, допускаются к работе с конфиденциальной

- нести персональную ответственность за сохранность доверенных им сведений, составляющих банковскую, коммерческую и служебную тайну;
- не допускать действий, которые могут повлечь утрату конфиденциальных документов или разглашение защищаемых сведений;
- хорошо знать и неуклонно соблюдать требования инструкции по организации конфиденциального делопроизводства, направленные на обеспечение надежной защиты сведений, составляющих банковскую, коммерческую и служебную тайну, от утечки и неправомерного завладения;
- незамедлительно сообщать уполномоченным лицам об утрате конфиденциальных документов, о фактах посягательств на незаконное собирание защищаемой информации банка;
- давать письменные объяснения об известных им обстоятельствах при проведении разбирательств по фактам нарушения инструкции по организации конфиденциального делопроизводства, а также по фактам утраты и хищения документов, содержащих защищаемую информацию.

2. Добросовестное исполнение указанных выше обязательств поощряется банком в виде надбавки к заработной плате сотрудников и других

. Обязательства лица, связанные с защитой сведений, составляющих вскую, коммерческую и служебную тайну, и обязательства банка, опре- щие виды, размеры и порядок предоставления льгот в качестве компен- за участие лица в защите конфиденциальной информации, фиксируют- удовом договоре (*контракте*).

Сотрудник банка, не принявший указанных выше обязательств, пра- тветственности за нарушение порядка обращения с конфиденциаль- формацией не несет.

Прекращение трудового договора, независимо от оснований, не осво- сотрудника от взятых обязательств не разглашать сведения, состав- банковскую, коммерческую и служебную тайну банка.

7. Подразделение защиты информации

одразделение (*отдел, отделение, группа*) защиты информации, со- ей банковскую (коммерческую) тайну и охраняемую законом ком- о информацию, входит в структуру управления защиты интересов кбы безопасности банка) и является ведущим (ответственным) в сфере и создания системы защиты информации, организации контроля нием установленного режима конфиденциальности и состоянием щиты сведений конфиденциального характера.

7.2. В рамках установленных полномочий подготавливает организационно-управленческие и нормативные документы, участвует в осуществлении мероприятий по защите банковской (коммерческой) тайны и компьютерной информации банка.

7.3. Разрабатывает должностные инструкции, определяющие права и обязанности лиц, уполномоченных осуществлять защиту информации.

7.4. Разрабатывает и доводит до пользователей сведения, составляющие банковскую (коммерческую) тайну и защищаемую компьютерную информацию банка, инструкцию по организации конфиденциального делопроизводства, устанавливающую порядок обращения с конфиденциальной информацией, конфиденциальными документами и другими носителями конфиденциальной информации.

7.5. Организует работу делопроизводства банка, обеспечивающую сохранность информации, составляющей банковскую (коммерческую) тайну и компьютерную информацию и ее носителей.

7.6. Ведет учет, хранение и выдачу носителей конфиденциальной информации в соответствии с полномочиями пользователей на право доступа, а также контроль за использованием носителей конфиденциальной информации.

7.7. Участвует совместно с разработчиками в создании и внедрении технических средств защиты информации, циркулирующей в помещениях и технических средствах банка.

7.8. Готовит и доводит до пользователей инструкцию по защите конфиденциальной информации в процессе эксплуатации технических средств обработки и передачи информации, составляющей банковскую (коммерческую) тайну. Организует и контролирует ее исполнение.

7.9. Ведет служебную документацию системы защиты информации (списки лиц, имеющих право доступа к конфиденциальной информации, учет паролей и ключей для доступа к указанной информации, обрабатываемой средствами вычислительной техники).

7.10. Осуществляет контроль за ходом технологического процесса обработки конфиденциальной информации путем регистрации действий пользователей по системному журналу.

7.11. Осуществляет оперативный контроль над функционированием системы защиты информации с целью проверки ее надежности.

7.12. Организует работу по вскрытию возможных каналов утечки конфиденциальной информации банка, выявлению, предупреждению и пресечению посягательств на незаконное завладение указанной информацией. Непосредственно участвует в проведении названных мероприятий.

7.13. Участвует в расследованиях по фактам незаконного собирания, похищения, разглашения и утраты сведений, составляющих банковскую (коммерческую) тайну и незаконных посягательств в сфере компьютерной информации банка.

7.14. Вырабатывает предложения по совершенствованию системы защиты нфиденциальной информации банка на основании анализа и оценки ее эф-ективности.

7.15. Участвует в координации совместных действий подразделений бан-, его контрагентов и правоохранительных органов в выявлении и пресече-и незаконных посягательств на защищаемую информацию.

7.16. Участвует в организации охраны и физической защиты помещений, нических средств и носителей конфиденциальной информации банка от отивоправных посягательств.

ДОГОВОР
(проект)
Об оформлении допуска сотрудника к банковской,
(коммерческой) тайне
(приложение к трудовому договору)

«УТВЕРЖДАЮ»

_____

(наименование должности,
Ф. И. О. лица, назначившего
расследование)
«____»_____200 __ года

Работодатель (*наниматель*) в лице администрации банка, руководствуясь положениями ст. 57 ТК РФ и инструкции о порядке допуска работников к банковской (коммерческой) тайне (*наименование банка*), и гражданин (*фамилия, имя, отчество*), действующий от своего имени, признаваемые в дальнейшем сторонами, заключили настоящий договор (*контракт*) о нижеследующем:

1. Предмет договора (*контракта*)

Я (*фамилия, имя, отчество*), оформляясь на работу в (*наименование банка*), будучи поставлен (*а*) в известность о том, что по роду своей деятельности буду допущен (*а*) к банковской (коммерческой) тайне, принимаю на себя добровольные обязательства, связанные с оформлением допуска к коммерческой тайне, на условиях, предусмотренных законодательством Российской Федерации.

2. Условия договора

В соответствии с законодательством Российской Федерации о банковской (коммерческой) тайне, другими нормативными и организационно-распорядительными актами, регламентирующими защиту банковской (коммерческой) тайны, с которыми меня ознакомили, принимая обязательства о неразглашении доверенных мне сведений, составляющих банковскую (коммерческую) тайну, даю согласие на частичные временные ограничения моих прав, которые могут касаться права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления (*переоформления*) допуска к защищаемой информации.

Принимаю на себя следующие обязательства:

- своевременно представлять в кадровый аппарат (*наименование банка*) сведения о возникновении оснований для отказа мне в допуске к бан-

ковской (коммерческой) тайне в соответствии с Положением о банковской (коммерческой) тайне банка:

- не уклоняться от проверочных мероприятий и не сообщать заведомо ложные анкетные данные;
- представлять в установленном порядке в кадровый аппарат (*наименование банка)* документы об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих банковскую (коммерческую) тайну;
- в случае попытки посторонних лиц получить от меня информацию конфиденциального характера немедленно сообщить об этом в подразделение защиты интересов банка (*наименование банка*);
- полно и своевременно информировать кадровый аппарат банка (*наименование банка)* об изменениях в биографических данных.

Я предупрежден(*а*) о том, что даже в случае однократного нарушения
: на себя обязательств, связанных с защитой банковской (коммерч
ны, а равно возникновения обстоятельств, являющихся, согласно По
о банковской (коммерческой) тайне банка, основанием для отказа
ке к коммерческой тайне, мой допуск к коммерческой тайне может
кращен и трудовой договор (*контракт*) расторгнут в соответствии с
иями.

Обязуюсь добросовестно выполнять свои обязательства по настоящем
ру (*контракту*), строго сохранять доверенные мне сведения, относящ
ковской (коммерческой) тайне, в том числе:

не разглашать сведения, составляющие банковскую (коммерч
тайну банка, его клиентов и контрагентов;

выполнять требования организационно-распорядительных актов
регламентирующих порядок защиты банковской (коммерческой)
ны;

не использовать информацию, составляющую банковскую (ком
скую) тайну банка в ущерб его интересам;

незамедлительно сообщать сотруднику банка, уполномоченному
щите информации, об утрате документов (*других носителей инф
ции*), содержащих банковскую (коммерческую) тайну, удостовер
пропусков, ключей от режимных помещений, хранилищ, сейфов
ных печатей и о других обстоятельствах, связанных с защитой ба
ской (коммерческой) тайны банка;

при увольнении возвратить представителю банка все полученные
и с исполнением должностных обязанностей носители инфор
имущество, предназначенное для защиты информации, сост
щей банковскую (коммерческую) тайну банка.

редупрежден(*а*), что за разглашение сведений, составляющих банк
ческую) тайну, буду привлечен(*а*) к ответственности в соотв
ующим законодательством.

Мне известно, что в соответствии с ч. 2 ст. 139 ГК РФ, ч. 2 ст. 183 УК РФ, ст. 57 ТК РФ и Положением о банковской (коммерческой) тайне банка прекращение допуска к защищаемой информации не освобождает меня от взятых обязательств по неразглашению составляющих ее сведений.

Банк (*наименование банка)* в случае положительного результата проверочных мероприятий и приема на работу обязуется в соответствии со ст. 57 ТК РФ создавать необходимые условия для работы со сведениями, составляющими банковскую (коммерческую) тайну.

3. Прочие условия

Наряду с законодательством Российской Федерации о защите банковской (коммерческой) тайны стороны обязуются строго руководствоваться требованиями трудового законодательства, в том числе при разрешении возможных споров.

Настоящий договор (*контракт*) составлен в 2-х экземплярах, один из которых хранится в личном деле работника, а другой — в подразделении защиты интересов (собственной безопасности) банка (*наименование банка*).

(*фамилия, подпись лица, принимаемого на работу*)
«___»_____ 200__г.

(*фамилия, подпись руководителя банка, заключающего договор* (*контракт*))
«___»_____ 200__г.

ИНСТРУКЦИЯ
(проект)
О порядке проведения внутреннего расследования по фактам незаконного получения и разглашения сведений, составляющих банковскую (коммерческую) и служебную тайну, нарушения порядка конфиденциального делопроизводства

«УТВЕРЖДАЮ»

_____

(*наименование должности,*
Ф. И. О. лица, назначившего
расследование)
«____»_____200 __

1. Общие положения

. Расследование по фактам незаконного получения и разглашения све-, составляющих банковскую (коммерческую) тайну, нарушений порядка иденциального делопроизводства, установленного в банке[1], является раз-ностью внутриорганизационной деятельности. Оно проводится с целью ения обстоятельств происшедшего, установления вины конкретных азмера причиненного ущерба, а также выявления причин и условий, ствовавших изучаемому событию.

Расследование представляет собой процесс гласного сбора и докумен-ия информации, относящейся к событию и получаемой путем опроса иков банка и других лиц (*с их согласия*), располагающих ею; ознаком-документами, осмотра служебных помещений, предметов, участков ги, а также оценки этой информации, подготовки выводов и предло-

2. Назначение расследования

снованием для проведения расследования являются ставшие извест-оводителю банка сведения о фактах причинения ущерба банку либо ниях внутренних правил банка, которые могут повлечь причинение кие сведения могут содержаться в служебных записках руководите-зделений, сообщениях правоохранительных органов, иных государ-а также негосударственных структур и частных лиц.

етствии с рекомендациями, изложенными в настоящей инструкции, может прово-разбирательство по иным нарушениям порядка, установленного нормативно-распо-документами банка.

Университетская

2.2. Расследование назначается руководителем, наделенным правом изда-ния приказов, после получения сведений о событии путем дачи письменного указания либо издания приказа о назначении группы сотрудников (*комиссии во главе с председателем*) для выполнения этой работы.

2.3. Председателем комиссии разрабатывается план проведения расследо-вания, распределяются направления работы, изучаются законодательные и другие нормативные акты по вопросам, подлежащим выяснению.

2.4. Руководитель, назначивший расследование, дает указание о направле-нии и объеме изучения события.

2.5. Сотрудники, на которых возложено проведение расследования, могут освобождаться от исполнения функциональных постоянных обязанностей на период расследования.

2.6. Сотрудники не могут участвовать в проведении расследования, если они прямо или косвенно заинтересованы в его результатах.

3. Проведение расследования

3.1. В ходе расследования устанавливается:

3.1.1. Действительно ли имело место событие.

3.1.2. Обстоятельства (*где, когда*), при которых оно произошло.

3.1.3. Наличие отрицательных последствий события, характер и раз-мер ущерба.

3.1.4. Причинная связь между проступком (*действиями, бездействи-ем*) конкретного лица (*лиц*) и результатом события.

3.1.5. Причины и условия, способствовавшие событию (*совершению проступка*).

3.1.6. Наличие обстоятельств, смягчающих или отягчающих ответствен-ность виновного лица.

3.2. Расследование проводится в срок до 30 дней.

В случае необходимости срок расследования может быть продлен руково-дителем, назначившим расследование по мотивированному обращению пред-седателя комиссии.

3.3. Сотрудники, которым поручено проведение расследования, подотчет-ны руководителю, назначившему расследование, и председателю комиссии.

3.4. Сотрудники, которым поручено проведение расследования, обязаны:

3.4.1. Соблюдать предусмотренные законом права и интересы лиц — участников расследования.

3.4.2. Делать выводы по результатам работы комиссии только на ос-новании фактических данных, полученных в результате расследования и закрепленных документально.

3.4.3. Своевременно докладывать руководителю, назначившему рас-следование, о выявленных нарушениях закона, причинах и условиях, способствовавших совершению проступка (*лица*

3.4.4. В случае установления в ходе расследования признаков преступления едленно доложить об этом руководителю и по его указанию направить мате- ы в установленном порядке в следственные (правоохранительные) органы.

3.5. Сотрудники, которым поручено расследование, имеют право:

3.5.1. Приглашать для беседы сотрудников, а также других граждан *согласия*). Получать от них письменные объяснения по фактам, имею- отношение к предмету расследования.

тказ от дачи пояснений оформляется отдельной справкой с указанием зов отказа.

3.5.2. С разрешения руководителя, назначившего расследование, зна- омиться с документами организации, имеющими отношение к предмету асследования.

случае необходимости приобщать указанные документы либо их копии риалам расследования.

3.5.3. Получать в установленном порядке консультации у специали- ов банка и других структур государственной и негосударственной форм бственности по вопросам, требующим специальных познаний.

3.5.4. Осматривать предметы, документы, изделия, участки местно- , имеющие отношение к событию.

3.5.5. Применять для фиксации полученной информации средства ио- и видеозаписи по правилам уголовно-процессуального законода- ьства.

3.5.6. Приобщать к заключению о результатах расследования свое бое мнение в случае несогласия с процессом расследования или выво- и по результатам работы.

4. Завершение расследования

По результатам расследования проводившие его сотрудники составля- зированное заключение, которое представляется руководителю, на- му расследование.

ючении должно быть указано:

4.1.1. Должности, фамилии сотрудников, проводивших расследова- и основание для его назначения.

4.1.2. Установочные данные лица, в отношении которого проводи- расследование.

4.1.3. Аргументированные ответы на вопросы, перечисленные в п. 3.1 щей инструкции.

4.1.4. Предложения (в зависимости от результатов расследования):

- о применении к виновному конкретного дисциплинарного взыскания, привлечения его к материальной ответственности, мерах, направленных на устранение причин и условий, способствовавших совершению проступка;
- о прекращении расследования или направлении материалов расследования в правоохранительные органы для решения вопроса о возбуждении уголовного дела.

4.2. Мотивированное заключение, подписанное сотрудниками, проводившими расследование, не требует согласования с непосредственными руководителями этих сотрудников.

4.3. Руководитель, назначивший расследование, изучает собранные материалы и заключение, оценивает их полноту и объективность, утверждает заключение либо возвращает с конкретными указаниями о сборе дополнительных сведений. Расследование считается законченным в день утверждения заключения.

Если в ходе расследования будут установлены признаки состава преступления, руководитель организации направляет материалы в установленном порядке в правоохранительные органы.

4.4. Руководитель, утвердивший заключение, определяет форму, в которой сотрудники, в отношении которых проводилось расследование, знакомятся с его материалами.

4.5. Материалы расследования приобщаются к отдельным делам, ведущимся службой безопасности.

ЗАКЛЮЧЕНИЕ
(проект)
О результатах расследования по факту нарушения порядка защиты сведений конфиденциального характера

«УТВЕРЖДАЮ»

_____
(*наименование должности, Ф. И. О. лица, назначившего расследование*)
«____»_____200 __ года

омиссия (*наименование банка*) в составе _____ на основании приказа (*на-вание, номер и дата приказа*) провела расследование по факту нарушения ика защиты сведений конфиденциального характера, установленного именование банка*) (*наименование распорядительного документа, регламен-щего указанный порядок*).

водом для назначения расследования стали поступившие сведения ушении порядка хранения, незаконном получении, разглашении или использо-защищаемой информации банка*): _____.

оведенным расследованием установлено (*приводятся фактические дан-идетельствующие о том, что сведения, составляющие банковскую (ком-скую) тайну, включены в систему охранительных отношений, зафиксирова-ментально и имеют соответствующие реквизиты и гриф конфиденциаль-

*Называется лицо, ответственное за сохранность документированных й в банке, основания и цель, с которыми это лицо получило доступ к све-дается ссылка на соответствующие учеты и подпись лица, принявшего т на ответственное хранение. Описываются время, место, способ и дру-ояльства разглашения сведений. Приводятся данные, свидетельствую-аличии либо отсутствии вины лица, обязанного сохранять конфиденци-ь доверенных сведений. Излагаются мотив и цель нарушения (правонару-Указываются обстоятельства, подтверждающие (либо опровергающие) законного разглашения конфиденциальной информации. Дается обоснова-стера ущерба, понесенного банком вследствие разглашения конфиденци-ведений. Указываются обстоятельства, способствовавшие совершению ушения и предлагаются способы совершенствования защиты информа-дущее): _____.

ленное позволяет прийти к следующим выводам:

вовая оценка события (имел место факт незаконного получения, раз-или использования сведений, составляющих банковскую (коммерческую)

номическая оценка тяжести наступивших последствий;

в) правовая оценка действия лиц, незаконно завладевших документом и использовавших содержащуюся в нем информацию;

г) правовая оценка действий лица, ответственного за сохранность конфиденциальной информации).

По итогам расследования полагаем целесообразным:

(высказывается мнение комиссии о наличии (или отсутствии) признаков преступления в действиях конкретного (либо неустановленного) лица, похитившего документ либо незаконно использовавшего содержащуюся в нем защищаемую информацию. О целесообразности передачи собранных материалов в органы следствия (суд). При установлении нарушения установленного порядка хранения конфиденциальной информации, способствовавшего выходу документа из законного владения, высказывается мнение о целесообразности наказания виновного в рамках трудового законодательства).

Председатель комиссии:
(*подпись*)
Члены комиссии:
(*подписи*)

КОММЕНТАРИЙ:

1. Поводом для назначения расследования могут служить сообщения граждан, коммерческих организаций, контролирующих и правоохранительных органов о фактах, свидетельствующих об утечке защищаемой информации банка. Так, таможенные органы могут сообщить о попытке незаконного (не декларированного) вывоза за рубеж документа (дискеты) при обстоятельствах, свидетельствующих об их выходе из законного владения (например, нахождение документа (дискеты) без отражения в таможенной декларации и других необходимых правовых оснований в багаже лица, вылетающего за рубеж).

О незаконном использовании защищаемой информации банка может сообщить работник конкурирующей организации. Такие сведения могут быть получены подразделением защиты интересов банка (собственной безопасности банка) в результате проведения сыскных мероприятий.

2. В ходе расследования следует установить наличие либо отсутствие связи между действиями лица, которому доверен документ, и выходом документа из законного владения. Указанное лицо может совершить умышленные противоправные действия (*быть соучастником похищения документа*) либо способствовать выходу документа из владения собственной неосторожностью (*не выполнить обязательных действий по охране документа по легкомыслию или небрежности*). Если документ похищен, несмотря на выполнение всех предписанных мер защиты, то оснований для привлечения работника к ответственности не имеется.

Гамза Владимир Андреевич
Ткачук Игорь Борисович

БЕЗОПАСНОСТЬ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

Учебник

Формат издания $70 \times 100^{1}/_{16}$.
Печать офсетная. Гарнитура NewtonC.
Печ. л. 25,5. Тираж 2000 экз. Заказ № 2796.

Главный редактор *Н. В. Разевиг*
Редактор *Н. Г. Петрович*
Корректор *Е. В. Глушенкова*
Компьютерная верстка *В. С. Чукашев*
Дизайн обложки *Б. В. Зипунов*

ООО «Маркет ДС Корпорейшн»
125190, Москва, Ленинградский просп., д. 80, корп. Г, оф. 202(8)
Тел.: (495) 987-43-74
e-mail: book@marketds.ru
www.marketds.ru

Отпечатано в полном соответствии с качеством
предоставленных материалов в ОАО «Дом печати — ВЯТКА»
610033, г. Киров, ул. Московская, 122