МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО
СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ
РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ ФИНАНСОВЫЙ ИНСТИТУТ

И.А. Муругова, Г.Я. Бабаева

ПЛАТЕЖНАЯ СИСТЕМА И БАНКОВСКАЯ БЕЗОПАСНОСТЬ

Рекомендовано Министерством высшего и среднего специального образования Республики Узбекистан в качестве учебного пособия

Ташкент
«IQTISOD-MOLIYA»
2019

УДК: 336.717.1(075.8)
ББК: 65.262.1

Рецезенты: д-р экон. наук, проф. **Т.М. Каралиев;**
канд. экон. наук, доц. **Ф.Н. Насриддинов**

М91 Платежная система и банковская безопасность: Учебное пособие / И.А. Муругова, Г.Я. Бабаева; – Т.: «Iqtisod-Moliya», 2019. – 164 с.

Необходимость издания учебного пособия, посвященного платежной системе и банковской безопасности, связана с недостатком учебной литературы по данной дисциплине. Пособие не претендует на исчерпывающее рассмотрение тем дисциплины «Платежная система и банковская безопасность», но дает общее направление для изучения тем, включенных в учебную рабочую программу данного курса, что позволит студентам более глубоко самостоятельно изучить, указанные в пособии темы и получить полное представление о функционировании платежной системы и обеспечении банковской безопасности.

УДК: 336.717.1(075.8)
ББК: 65.262.1

ISBN 978-9943-13-797-4

ВВЕДЕНИЕ

Место банков в экономике огромно, от их деятельности зависит ее стабильность. Эффективная деятельность банков во многом зависит от правильной организации учета его операций, в первую очередь, по безналичным расчетам, а также от состояния и развитости платежной системы. Свидетельством важного значения последнего является тот факт, что руководством нашей страны придается особое значение развитию платежной системы. Так в Указе Президента Республики Узбекистан от 9 января 2018 года № УП-5296 одним из стратегических целевых ориентиров деятельности Центрального банка названо обеспечение стабильности и развития платежной системы, а среди приоритетных направлений деятельности Центрального банка в рамках проводимых реформ - дальнейшее развитие платежной системы, включая организацию эффективного взаимодействия информационных систем коммерческих банков при оказании дистанционных банковских услуг, позволяющих оперативно управлять счетами и проводить банковские операции в режиме реального времени.[1]

Целью учебного пособия по дисциплине «Платежная система и банковская безопасность» является ознакомление, выпускаемых магистратурой кадров по специальностям «Банковское дело» и «Банковский учет и аудит», с платежной системой Центрального банка Республики Узбекистан и ее структурой, безналичными расчетами, организацией межбанковских расчетов как основы платежной системы, ее развитием, розничными платежными системами и порядком проведения через них платежей.

Важным также является понятие межбанковских расчетов, их развитие, изучение корреспондентских отношений банков, понятие системы электронных платежей, понятие и значение единого

[1] Указ Президента «О мерах по коренному совершенствованию деятельности Центрального банка Республики Узбекистан». 2018 . 9 января. № УП-5296.

корреспондентского счета, изучение новых банковских технологий, роли пластиковых карточек, программного обеспечения «Банк-клиент», системы наличных денежных переводов. Кроме того, студенты должны усвоить вопросы безопасности банков: цели и задачи баноковской безопасности; виды угроз; объекты банковской безопасности; банковскую тайну; правовые основы банковской безопасности.

Главное в организационной работе по обеспечению банковской безопасности состоит в том, что она требует комплексного подхода, творческого отношения, глубокого анализа, прогнозирования, выявления и своевременного принятия мер по устранению внутренних и внешних угроз.

В связи с этим возникает необходимость перехода с уровня охранительных представлений о безопасности банковской системы на уровень ее интеллектуально-наступательного обеспечения.

Дисциплина «Платежная система и банковская безопасность» имеет тесную взаимосвязь с банковской практикой и экономикой. Организация и совершенствование платежной системы, расчетных операций в банках, использование различных форм безналичных расчетов и банковских технологий, основные направления по укреплению банковской безопасности, проведение корреспондентских отношений банков по системе электронных платежей будут способствовать своевременному проведению расчетов в экономике, а также обеспечат устойчивое функционирование банковской системы страны с учетом изучения и применения зарубежного опыта построения и совершенствования платежной системы.

ГЛАВА I. ПЛАТЕЖНАЯ СИСТЕМА И ЕЁ СТРУКТУРА

1.1. Понятие платежной системы и её элементы

Платежная система - это совокупность методов и реализующих их субъектов, обеспечивающих в рамках системы условия для использования платежного инструмента оговоренного стандарта в качестве платежного средства. Это понятие так же раскрывается как «набор механизмов для выполнения обязательств, принимаемых хозяйствующими субъектами при приобретении ими материальных или финансовых ресурсов». К числу таких механизмов они относят «учреждения, предоставляющие платежные услуги, различные инструменты, используемые для передачи платежных указаний (включая каналы связи) и договорные отношения между заинтересованными сторонами». Платежным инструментом может выступать пластиковая карта, «электронный кошелек» в открытой сети или счет в электронной интерактивной банковской системе. Можно дать определение банковским платежным системам с точки зрения их экономической сущности. С этой позиции, банковские платежные системы представляют собой часть системы безналичных расчетов, основанной на собственных принципах, способах платежа и формах расчетов и активно взаимодействующей со всей системой безналичных расчетов. На рис. 1 представлена классификация платежных систем по различным признакам.

Согласно законодательству Республики Узбекистан, «Платежной системой является совокупность отношений, возникающих между субъектами платежной системы при осуществлении электронных платежей».[2]

В Узбекистане выделяют следующие виды платежной системы (рис.2).

---

[2] Закон РУз. «Об электронных платежах». 2005.16.12. № ЗРУ-13.

Рис.1. **Классификация платежных систем**[3]

Межбанковская платежная система предназначена для осуществления электронных платежей между банками через их корреспондентские счета, открытые в Центральном банке Республики

[3] Деньги, кредит, банки: Учебник / Под ред. Г.Н.Белоглазовой. М.: Высшее образование, 2009. С.250.

Узбекистан. Правила межбанковской платежной системы определяются Центральным банком Республики Узбекистан.

Внутрибанковская платежная система предназначена для осуществления электронных платежей между филиалами и клиентами банка, а также для взаимодействия с межбанковской платежной системой. Правила внутрибанковской платежной системы определяются банком–членом платежной системы.

Рис. 2. **Классификация платежных систем в Узбекистане**[4]

Система розничных платежей предназначена для осуществления электронных платежей с применением банковских карт и других средств электронного платежа (далее – средства электронного платежа). Средство электронного платежа должно иметь отличительные признаки (товарный знак, знаки обслуживания), позволяющие идентифицировать его принадлежность к данной системе розничных платежей. Правила системы розничных платежей определяются организацией, создавшей данную систему розничных платежей.

Субъектами платежной системы являются члены платежной системы и пользователи платежной системы.

Членами платежной системы являются юридические лица, оказывающие пользователям платежной системы услуги по осуществлению электронных платежей.

---

[4] Составлено автором на основе закона РУз «Об электронных платежах». 2005.16.12. № ЗРУ-13.

Пользователями платежной системы являются юридические или физические лица, которым оказываются услуги по осуществлению электронных платежей.

К элементам платежной системы относятся следующие:

- институты, предоставляющие услуги по осуществлению денежных переводов и погашению долговых обязательств;
- финансовые инструменты и коммуникационные системы, обеспечивающие перевод денежных средств между экономическими агентами;
- контрактные соглашения, регулирующие порядок безналичных расчетов.

Элементы платежной системы тесно взаимосвязаны между собой, их взаимодействие осуществляется по определенным правилам, закрепленным в нормативно-правовых актах государства и международных соглашениях. Работа платежной системы страны в целом построена согласно соответствующим правовым актам, на основе которых разработаны правила ее функционирования. Они являются едиными для любой системы и определяют совокупность процедур, которые необходимы для функционирования платежной системы и осуществления переводов денежных средств от одних экономических агентов к другим. К процедурам платежной системы относятся установленные формы проведения безналичных расчетов, стандарты платежных документов, а также различные средства передачи информации (линии связи, программное и техническое обеспечения). В экономической литературе встречается также иная общая концепция подхода к платежной системе с позиции платежной инфраструктуры. Хорошо продуманная платежная инфраструктура способствует надлежащему функционированию рынков и помогает устранить трения в торговле. Поэтому механизмы перевода средств являются непременным условием для большинства экономических отношений (т.е. «нет платежа, нет торговли»). В более ограниченном смысле термин «платежная система» иногда используется как синоним «системы межбанковских денежных переводов».

Однако в целом термин «платежная система» относится к полному набору инструментов (посредники, правила, процедуры, процессы и системы межбанковских переводов денежных средств), которые облегчают обращение денег в стране или валютной зоне. [5]

1.2. Платежная система Республики Узбекистан и её образование

Процесс становления платёжной системы Республики Узбекистан можно разделить на пять этапов.

1. К первому этапу (1988-1991 гг.) относится период, когда Узбекистан входил в состав союзного государства. Во время этого этапа формировались элементы рыночной экономики в хозяйственном механизме. При этом механизмы расчётов не изменялись; они осуществлялись на основе бумажных платёжных документов и системы МФО (межфилиальных оборотов). Государственные специализированные банки, как субъекты хозяйствования имели все атрибуты юридически самостоятельных лиц, но при этом включались в единую государственную банковскую систему. На практике незначительное расширение прав специализированных банков не сопровождалось надлежащим разграничением ресурсов.

Сохранилась также централизованная схема управления банковской системой со стороны неэффективного Госбанка, которая превращала банковские займы на фактически бесповоротные дотации нерентабельным предприятиям. В результате такого «реформирования» ещё в большей степени усилились недостатки в деятельности банковской системы. Госбанк был лишён возможности регулировать денежный оборот и контролировать деятельность спецбанков, а также применять на финансовом рынке экономические методы регулирования банковской системы. Это свело к нулю попытки проведения денежно - кредитной политики,

[5] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. C. 25.

а именно, «монобанк» в лице Госбанка, который был основой одноуровневой банковской системы, и был заинтересован в переходе к двухуровневой банковской системе.

2. Ключевым моментом второго этапа (1991-1994 гг.), во время которого происходила дезинтеграция бывшей советской платёжной системы, является создание Центрального банка Республики Узбекистан, реформирование банковской и платёжных систем путём реструктуризации сети банков.

3. Платежная система в 1995-2003 гг. входит в третий этап её развития.

Из-за отсутствия в начале 90-х гг. банковской телекоммуникационной сети и передачи бумажных денежно-расчетных документов через почту платежи между экономическими субъектами проходили до двух месяцев, а оборачиваемость средств была очень низкая. Анализируя состояние платежной системы, Правительство РУз приняло Постановление «О мерах по совершенствованию банковской системы и стабилизации денежно-кредитных отношений», в соответствии с которым Центральный банк совместно с коммерческими банками разработал концепцию компьютеризации банковской системы республики, и с начала 1995 года централизованно начал внедрение системы электронных платежей в банковскую систему. Это мероприятие было завершено в марте 1996 года.

До сентября 2003 года в банках функционировала децентрализованная система расчетов, то есть филиалы банков самостоятельно открывали корреспондентские счета в Центральном банке и управляли своими ресурсами и рисками. Система электронных платежей обеспечивала файловую обработку информации на валовой основе. Инициированные платежные документы поступали в систему и обрабатывались непрерывно в порядке поступления. Время обработки транзакций составляло 3-5 минут для внутриобластных платежей и 10-15 минут для межобластных платежей.

4. Совершенствование платежной системы в 2003–2010 гг.

Проведение межбанковских платежей стало осуществляться через единые корреспондентские счета головных коммерческих банков, открытые в Центре расчетов Центрального банка.

Кроме того, постепенно происходило создание единой базы данных и централизованной обработки платежных операций в головных офисах коммерческих банков.

Работы по переходу на единый корреспондентский счет были завершены к 8 сентября 2003 г., и все многофилиальные коммерческие банки перешли на единый корреспондентский счет. При этом, были упразднены все территориальные центры расчетов и стал функционировать единый центр расчетов при Главном управлении ЦБ по г. Ташкенту.

С мая 2004 г. все операции, проводимые расчетно-кассовыми центрами территориальных главных управлений Центрального банка, отражаются в едином балансе Центрального банка в режиме реального времени. В 2005–2008 гг. были завершены работы по созданию единой базы данных и централизованной обработки платежных операций в головных офисах коммерческих банков, кроме ГК Народного банка.

5. Создание системы управления информацией в банках.

Современное развитие экономики обусловливает необходимость глубокого изучения причин изменения экономических показателей в разрезе банков, регионов и в целом по республике для выработки оптимальных решений. В связи с этим, в настоящее время становятся востребованными и выдвигаются на первое место не просто информационные, а аналитические технологии, позволяющие повысить эффективность управления. Учитывая это, учетно-бухгалтерское ядро вновь создаваемых автоматизированных банковских систем базируется на принципиально новой технологической базе с учетом защиты, и обеспечивающих полноту информации, необходимой для функционирования системы поддержки принятия решений по управлению банком. В настоящее время уровень развития автоматизированных банковских систем, программно-аппаратных средств и опыт работы персонала поднялись на качественно новую ступень, и уже подошло время, когда банки должны больше внимания уделять вопросам управления, поддержания рентабельности и эффективности функционирова-

ния, чтобы динамично развиваться в конкурентной среде. Поэтому проводятся дальнейшие работы по развитию платежной системы, банковской телекоммуникационной сети и банковских информационных технологий, глобальной системы безопасности, обеспечивающей соответствующий уровень защиты информационных сетей банков.

1.3. Межбанковская платежная система

Межбанковская платежная система предназначена для осуществления электронных платежей в национальной валюте между банками через их корреспондентские счета, открытые в Центральном банке Республики Узбекистан. Правила межбанковской платежной системы определяются Центральным банком Республики Узбекистан.

Межбанковская платежная система ЦБ функционирует в соответствии со следующими нормативно-правовыми документами:

• Законом Республики Узбекистан от 21.12.1995 г. № 154-I «О Центральном банке Республики Узбекистан»;

• Законом Республики Узбекистан от 25.04.1996 г. № 216-I «О банках и банковской деятельности»;

• Законом Республики Узбекистан от 16.12.2005 г. № ЗРУ-13 «Об электронных платежах»;

• Положением ЦБ от 14.02.2006 г. № 1545 «О порядке осуществления электронных платежей через межбанковскую платежную систему Центрального банка»;

• Положением ЦБ от 13.06.2013 г. № 2465 «О порядке проведения безналичных расчетов банками Республики Узбекистан».

Межбанковская платежная система является личной собственностью Центрального банка Республики Узбекистан. Участниками межбанковской платежной системы являются Главный центр информатизации и Центр расчетов. Пользователями межбанков-

ской платежной системы являются банки и финансовые институты, которые имеют корреспондентские счета в Центре расчетов.

Центр расчетов Центрального банка (далее - ЦР ЦБ) – это отдел управления учета, отчетности и расчетов Главного управления Центрального банка Республики Узбекистан города Ташкента, в функции которого входит открытие и обслуживание корреспондентских счетов головных офисов коммерческих банков и бесперебойное обеспечение электронных расчетов между ними.

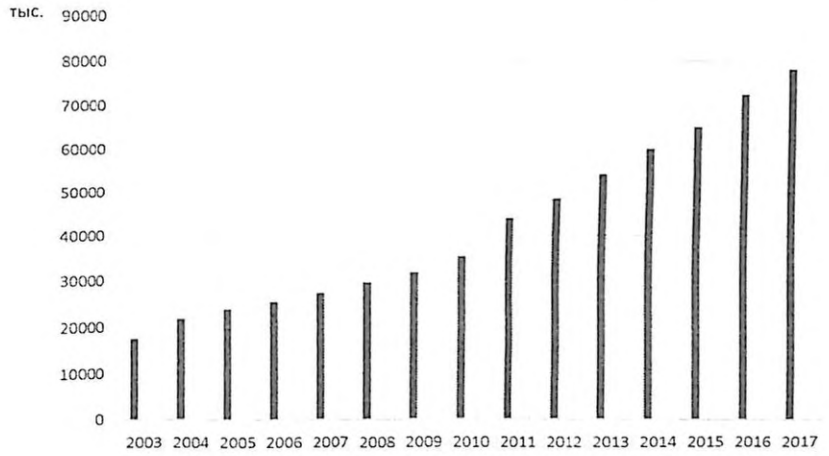

Рис. 3. **Количество транзакций, осуществленных через межбанковскую платежную систему Центрального банка РУз**[6]

Главный центр информатизации Центрального банка (далее – ГЦИ) – центр, обеспечивающий техническое, программное и эксплуатационное сопровождение межбанковской платежной системы в соответствии с действующим законодательством, а также договорами между ГЦИ и банками.

Права и обязанности участников и пользователей межбанковской платежной системы регулируются двусторонними договорами банков-пользователей с ЦР ЦБ – на открытие и обслужива-

[6] http://www.cbu.uz/ru/platyezhnye-sistemy.

ние корсчетов банков, с ГЦИ – на проведение электронных платежей через межбанковскую платежную систему.

Количество транзакций через межбанковскую платежную систему из года в год растет (рис. 3).

Динамика роста количества транзакций впечатляет своими темпами. Если в 2003 году количество транзакций составляло менее 20 млн. в течение года, то начиная с 2014 года их количество утроилось, достигнув 60 млн. операций. При этом продолжается ежегодный стабильный рост количества осуществляемых операций.

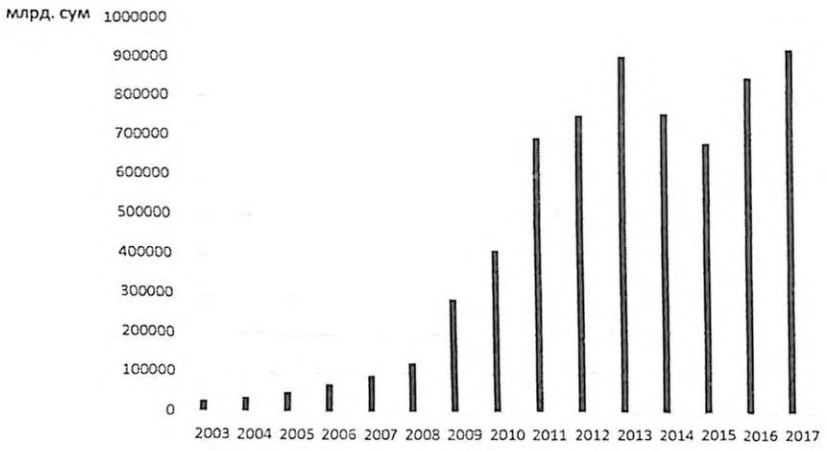

Рис. 4. **Сумма транзакций, осуществленных через межбанковскую платежную систему Центрального банка РУз**[7]

Аналогичная динамика наблюдается и по сумме транзакций, осуществляемых через межбанковскую платежную систему (рис. 4).

Резкое увеличение суммы транзакций отмечалось в 2011 году, когда она превысила 600 трлн. сум. В последующие годы сумма транзакций варьирует в интервале 600-900 трлн.сум.

[7] http://www.cbu.uz/ru/platyezhnye-sistemy.

Электронные платежи от банков осуществляются только в пределах остатка средств на корреспондентском счете, если иное не оговорено в договоре между ЦР ЦБ и банком.

С 9-00 до 16-00 часов – время передачи-приема-контроля электронных платежных документов (далее – ЭПД) по межбанковским расчетам:

1) банки в любой момент данного периода могут передавать ЭПД в ЦР ЦБ;

2) предназначенные для отправки ЭПД проходят контроль, заверяются электронной цифровой подписью, шифруются и по линиям банковской телекоммуникационной сети передаются для дальнейшей обработки в ЦР ЦБ.

До 17-00 часов производится передача ЭПД по переводу средств на соответствующие счета накопительной пенсионной системы республиканского бюджета. При этом, до 16-30 часов завершается обработка ЭПД, направленных между коммерческими банками, а до 17-00 часов – ЭПД, направленных коммерческими банками в Центральный банк и Народный банк, а также из Центрального банка.

С 17-00 часов ГЦИ направляет банкам извещение о закрытии дня и информацию по отбракованным ЭПД (по банку-инициатору и банку-бенефициару).

После этого в ГЦИ осуществляется этап «Закрытие дня». Условиями выполнения этапа «Закрытие дня» в ЦР ЦБ являются:

- истечение времени приема ЭПД от банков;

- все ЭПД, переданные в ЦР ЦБ, должны быть обработаны и отражены на соответствующих корреспондентских счетах банков.

Время проведения этапа «Закрытие дня» в банках определяется самостоятельно в соответствии с требованиями внутрибанковской платежной системы. Исходя из параметров денежно-кредитного управления Центрального банка Республики Узбекистан время перевода межбанковских ЭПД может продлеваться на основании письменного распоряжения заместителя председателя, контролирующего вопросы платежной системы. Об этом участники и

пользователи системы извещаются не позднее чем за час до завершения времени обработки ЭПД.

Ключевые слова и понятия

Платежная система, электронная цифровая подпись, закрытый ключ электронной цифровой подписи, открытый ключ электронной цифровой подписи, подтверждение подлинности электронной цифровой подписи, электронный документ.

Вопросы для самопроверки

1. Объясните сущность платежной системы и её основные элементы.
2. Охарактеризуйте на макроуровне платежную систему.
3. Охарактеризуйте на микроуровне платежную систему.
4. Проклассифицируйте платежные системы.
5. Какие виды платежной системы выделяют в Узбекистане?
6. Раскройте содержание закона РУз "Об электронных платежах".
7. Какие элементы относятся к платежной системе?
8. Как образовалась платежная система в РУз?
9. Чем является межбанковская платежная система в Узбекистане?
10. Как осуществляются электронные платежи банков РУз?

ГЛАВА II. СИСТЕМА БЕЗНАЛИЧНЫХ РАСЧЕТОВ

2.1. Система безналичных платежей и её элементы. Сущность положения «О безналичных расчетах в Республике Узбекистан», его значение и применение на практике

Безналичные расчеты – это денежные расчеты путем записей по счетам в банках, когда деньги списываются со счета плательщика и зачисляются на счет получателя.

В зарубежной экономической литературе безналичные расчеты определяются с позиции безналичного платежного инструмента. Безналичные платежи включают перевод средств между счетами. Таким образом, безналичный платежный инструмент является средством, с помощью которого плательщик дает банку разрешение на перечисление средств или по которому получатель через банк имеет возможность получения средств от плательщика.[8]

Существовавшая в стране с 30-х годов вплоть до 1993 года система безналичных расчетов была приспособлена к затратному механизму хозяйствования, и соответствовала административно – командным методам управления экономикой. Действовавшая система безналичных расчетов была ориентирована на обслуживание, в первую очередь, интересов поставщика, сводившихся к выполнению своих плановых заданий по производству и поставкам продукции. При этом действовали довольно жесткие принципы организации безналичных расчетов, соблюдение которых в некоторой степени компенсировало отсутствие подлинной экономической

[8] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. С. 28.

заинтересованности и ответственности предприятий за выполнение своих договорных обязательств.

Эти принципы, в частности, строго регламентировали:

- место платежа – банк (он выступал организатором и контролером безналичных расчетов);
- время платежа – после отгрузки продукции или оказания услуг (что означало запрещение авансов и коммерческого кредита);
- согласие плательщика (акцепт) – как основание платежа;
- источник платежа – собственные средства покупателя или банковский кредит при наличии прав на его получение;
- форму безналичных расчетов, сфера использования каждой из которой была заранее предопределена.

Все безналичные расчеты осуществлялись на основе платежных документов, имеющих хождение только во внутрибанковском обороте.

Указанные принципы расчетов не учитывали требования платежеспособности и кредитоспособности покупателя, отрицательное влияние нарушения хронологической очередности платежей на ликвидность балансов участников расчетов, возможность использования на практике и более гибких форм и способов платежа.

В настоящее время в Республике Узбекистан безналичные расчеты осуществляются на основе Положения ЦБ РУз «О порядке проведения безналичных расчетов банками Республики Узбекистан» от 13.06.2013г. № 2465. Согласно положению, расчетные операции осуществляются банками с депозитных счетов клиентов. Банк хранит денежные средства клиентов на их счетах, зачисляет поступающие на эти счета суммы, выполняет распоряжения клиентов об их перечислении и выдаче со счетов, проводит другие банковские операции. Платежи производят за счет собственных средств клиента, а в отдельных случаях за счет кредита банка. Зачисление средств на счет получателя осуществляется лишь после списания этих средств со счета плательщика. Споры между банками и его клиентами решаются взаимно в соответствии

с заключенными договорами на обслуживание. При невозможности решения споров путем взаимного согласия, они решаются через хозяйственный суд. Расчеты между банками на территории Республики Узбекистан осуществляются через их корреспондентские счета по системе электронных платежей в национальной валюте. Документооборот в банках организуется в соответствии с Положением «О ведении расчетов между банками Республики Узбекистан по системе электронных платежей» № 1010 от 19.02.2001 года. Списание средств со счетов клиентов осуществляется на основе Инструкции ЦБ РУз «О порядке списания денежных средств с банковских счетов хозяйствующих субъектов» от 22.03.2012 г. № 2342. Сведения о количестве клиентов и счетов в стране показаны в табл. 1.

Таблица 1

Сведения о количестве клиентов и их счетах, зарегистрированных в Национальной информационной базе банковских депозиторов РУз[9]

(на 1 января)

Год	Количество клиентов	Количество счетов
1997	187 415	206 514
2001	373 090	416 713
2005	656 137	2 007 607
2009	1 026 844	3 327 260
2013	1 285 424	4 289 556
2017	1 638 673	5 809 172

Данные таблицы свидетельствуют о многократном увеличении количества клиентов и их счетов, зарегистрированных в Национальной информационной базе банковских депозиторов за последние 20 лет. Такая ситуация отражает общее развитие банковской системы страны и рост выполняемых операций, в том числе и по безналичным расчетам.

[9] http://www.cbu.uz/ru/platyezhnye-sistemy/29/.

В экономике большое количество транзакций происходит каждый день по инициативе широкого круга экономических субъектов. Все транзакции имеют два компонента расчета: поставка товара (оказание услуги) и перевод средств.

Платежный инструмент - это инструмент или набор процедур, позволяющих передавать средства от плательщика до получателя платежа. Существует множество различных платежных инструментов, каждый со своими характеристиками в зависимости от типа отношений и транзакции между плательщиком и получателем. Наиболее распространено различие между наличными и безналичными платежными инструментами.[10]

При осуществлении безналичных расчетов в Республике Узбекистан используются следующие формы денежно-расчетных документов, установленные Центральным банком:

- Платежное поручение (№ 0505411002);
- Платежное требование (№ 0505411001);
- Заявление на аккредитив (№ 0505411009);
- Инкассовое поручение (№ 0505411013).

Эти документы являются основными при соответствующих формах расчетов.

Форма расчетов между плательщиком и получателем средств определяется ими самими в хозяйственных договорах (соглашениях). Денежно-расчетные документы должны соответствовать требованиям и установленных стандартам Центрального банка.

Платежное поручение представляет собой поручение клиента обслуживающему его банку о перечислении определенной суммы со своего счета на счет получателя. Поручениями могут производиться расчеты за товары, работы, услуги и по другим платежам. Дата поручения должна соответствовать дате его предъявления в банк, при их несоответствии платежное поручение не принимается к исполнению (кроме платежей в бюджет и внебюджетные фонды). Поручение принимается банком только при наличии

[10] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. С. 28.

средств на депозитном счете клиента. Особенностью платежных поручений является их широкое применение по нетоварным операциям (платежам в бюджет и т.п.).

Платежные поручения принимаются банком от юридических лиц по платежам в бюджет и внебюджетные фонды до наступления срока уплаты. При отсутствии средств на банковском счете платежные поручения принимаются обслуживающим банком в картотеку № 2.

Платежное требование представляет собой денежно-расчетный документ, содержащий требование поставщика плательщику об уплате определенной суммы через банк. Поставщик (получатель средств) представляет в банк требование, которое может выставляться за отгруженные товары, выполненные работы, оказанные услуги и по другим платежам. Платежное требование содержит все необходимые реквизиты, позволяющие определить какой товар отгружен, каковы его сортность, цена, время отгрузки и т.д. К требованию должны прикладываться товарно-транспортные, либо заменяющие их документы, в которых поставщик обязан указывать обоснование цен на товары и услуги. Требование вместе с вышеуказанными документами, сдается поставщиком на инкассо.

При учете операций по платежным требованиям используются следующие счета:

- 90962 - расчетные документы, ожидающие срока оплаты (картотека №1). По дебету этого счета проводится сумма документов, которые ожидают акцепта и принимаются в картотеку к этому счету. По кредиту проводится сумма расчетных документов, для которых срок оплаты наступил. В аналитическом учете по этому счету ведутся лицевые счета отдельно по каждому плательщику.
- 90963 - расчетные документы, не оплаченные в срок (картотека № 2). По дебету счета проводятся суммы расчетных документов в неоплаченной части. А сами документы принимаются в картотеку № 2 к этому счету. По кредиту счета проводится сумма документов, оплачиваемых при поступлении средств на счет клиента.

Для ведения бухгалтерских проводок по картотекам №1 и №2 открываются также контрсчета:

- 96319 - контрсчет по расчетным документам, ожидающим оплаты;

- 96321 - контрсчет по расчетным документам, не оплаченным в срок.

Эти счета корреспондируют со счетами картотек.

Аккредитив - условное денежное обязательство банка, выдаваемое им по поручению клиента в пользу его контрагента по договору, по которому банк, открывший аккредитив (банк-эмитент), обязуется произвести поставщику платеж или предоставить полномочия другому банку производить такие платежи при условии представления им документов, предусмотренных в аккредитиве и при выполнении всех условий аккредитива.

Плательщик представляет в банк заявление на аккредитив. Срок действия и порядок расчетов по аккредитиву устанавливаются в договоре между плательщиком и поставщиком.

Аккредитивы учитываются банком на отдельных счетах непредвиденных обстоятельств и на балансовом счете 22602 «Депозиты клиентов по аккредитивам». Для каждого поставщика открывается отдельный депозитный счет по аккредитивам в обслуживающем его банке.

В современной практике используются следующие виды аккредитивов: покрытые (депонированные), непокрытые (гарантированные), отзывные и безотзывные.

Инкассовое поручение представляет собой требование клиента банку списать средства со счета плательщика в бесспорном порядке. Инкассовое поручение могут выставлять:

• налоговые органы (о взыскании не внесенных налогов);

• внебюджетные фонды (о взыскании недоимок);

• таможенные органы (о взыскании таможенных платежей);

• судебные органы (по выданным им исполнительным документам);

• другие органы, согласно законодательству.

Списание средств со счетов плательщиков производится банком только по подлинным документам или их дубликатам.

В инкассовых поручениях на взыскание сумм по решению хозяйственного суда обязательно должна быть ссылка на номер и дату решения, причем необходимо выделить отдельно суммы долга и расходов по госпошлине. Степень использования платежных документов существенно различается (рис. 5).

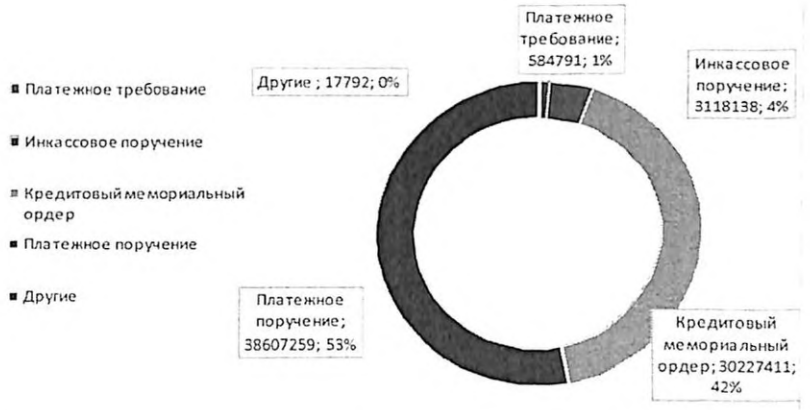

Рис. 5. **Количество транзакций, осуществленных через межбанковскую платежную систему Центрального банка в течение года** (данные на 1 января 2017 года)[11]

Более половины операций осуществляются платежными поручениями, которые являются основной формой безналичных расчетов. Также распространенным платежным документом является мемориальный ордер.

2.2. Пластиковые карточки и их место в национальной платёжной системе

Основной целью создания национальной карточной системы является сокращение наличных денег в обороте, упорядочивание денежного обращения, привлечение денежных средств населения

[11] http://www.cbu.uz/ru/platyezhnye-sistemy.

и вовлечение их в хозяйственный оборот, создание международно-признанных банковских услуг по обслуживанию населения, предприятий и организаций. Система должна отвечать потребностям финансового рынка и обеспечивать ее участникам, начиная от банков-эмитентов, выпускающих в обращение пластиковые карточки, до держателей этих карточек возможность достижения указанных целей.

Исходя из сложившейся банковской системы Узбекистана, а также принципов создания карточной системы, национальную систему безналичных расчетов с применением пластиковых карточек необходимо было организовать из следующих 4-х уровней:

- ✓ Республиканского главного процессингового центра (РГПЦ);
- ✓ Региональных процессинговых центров (РПЦ);
- ✓ Банков-участников (эмитентов);
- ✓ Пунктов обслуживания карт (предприятия сферы услуг).

Система безналичных расчетов с применением пластиковых карточек должна иметь доступ к базам данных 14 региональных процессинговых центров с базой данных главного республиканского процессингового центра, а также банков-эмитентов.

Основные преимущества безналичного денежного оборота с помощью пластиковых карточек для экономики в целом показаны на рис. 6.

Определение пластиковой карты как платежного инструмента даётся в различных источниках литературы по-разному. **Платежные карты** - это устройства доступа, которые могут использовать их держатели для оплаты товаров и услуг - либо в точке продажи (POS), либо удаленно (в режиме «card-not-present» транзакции) - или снимать деньги с банкоматов. Как правило, функция оплаты и функция денежных средств объединяются на одной плате. Карты используются для авторизации дебетов со счета держателя карты или для привлечения кредитной линии, предоставленной держателю карты эмитентом карты.[12]

[12] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. С. 31.

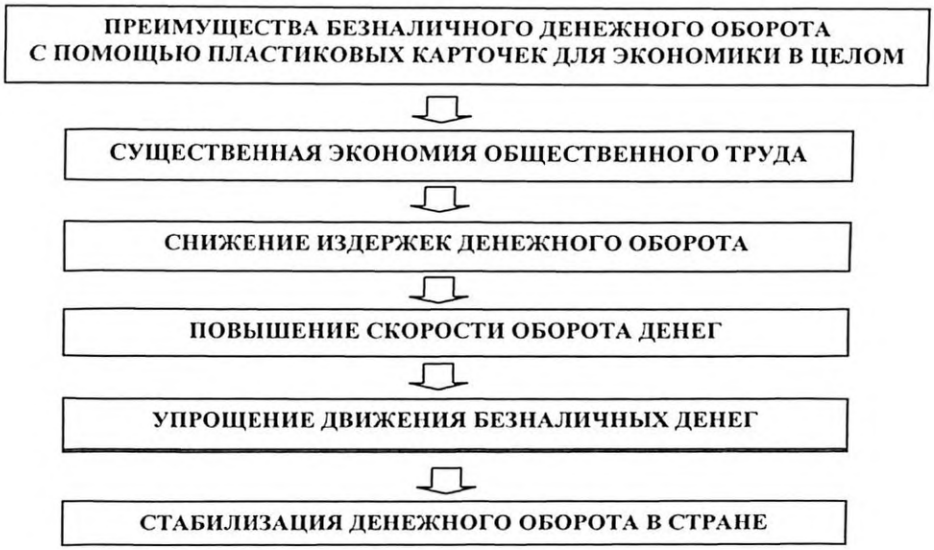

Рис. 6. **Преимущества безналичного денежного оборота с помощью пластиковых карточек**

Виды предлагаемых пластиковых карточек различаются по своему назначению, функциональным и техническим характеристикам. Сами по себе практически все карты имеют один и тот же размер (примерно 54 х 86 мм) и толщину (около 1 мм), но классифицируются по разным критериям на целый ряд видов.

1. По материалу, из которого они изготовлены:

- **бумажные** (картонные);
- **пластиковые** (в настоящее время практически имеют повсеместное распространение);
- **металлические**.

2. На основании механизма расчетов:

- **двусторонние системы** - возникли на базе двусторонних соглашений между участниками расчетов, при которых владельцы карт могут использовать их для покупки товаров в замкнутых се-

тях, контролируемых эмитентом карт (универмаги, бензоколонки и т.д.);

➢ **многосторонние системы** - предоставляют владельцам карт возможность покупать товары в кредит у различных торговцев и организаций сервиса, которые признают эти карты в качестве платежного средства. Многосторонние системы возглавляют национальные ассоциации банковских карт, а также компании, выпускающие карты туризма и развлечений (например, American Express).

3. По способу нанесения на карты необходимой информации (имя держателя карты, номер карты, срок ее действия и пр.):

➢ **карты с графическим изображением; карты эмбоссированные** - информация: имя держателя карты, номер карточки, срок действия карточки и пр. нанесена рельефным шрифтом (выдавлена) специальным аппаратом эмбоссером;

➢ **карты со штрих-кодированием** - запись информации на карту с помощью штрих-кодирования применялась до изобретения магнитной полосы и в платежных системах распространения не получила;

➢ **карты с кодированием на магнитной полосе** (магнитные карты) -изобретение в конце 1960-х гг. автоматических аппаратов выдачи наличных денег совершило революцию и в карточном бизнесе. Чтобы таким аппаратом могли пользоваться держатели карт, на их обратную сторону стали наклеивать полоску из магнитной пленки. На магнитной полосе банковских карт записывается (обычно в закодированном виде) номер карты, срок ее действия и ПИН-код держателя карты. Поэтому магнитная запись является одним из самых распространенных на сегодняшний день способов нанесения информации на карты;

➢ **карты с чипом** (чиповые карты или микропроцессорные карты) - микропроцессор позволяет выполнять определенные операции над хранящимися в карте данными. Эти операции составляют операционную систему карты, которая обеспечивает боль-

шой набор функций управления памятью, сервисных функций и средств безопасности. Смарт-карты по своим надежностным и эксплуатационным характеристикам значительно превосходят обычные магнитные карточки. Проведение любой операции с использованием смарт-карты требует от владельца набора личного пароля, этот пароль записан на самой карточке;

➢ **карты с лазерной записью** (лазерные или оптические карты) - в 1981 году Дж.Дрекслером была изобретена оптическая карточка. Запись и считывание информации с такой карточки производится специальной аппаратурой с использованием лазера. Эти карточки могут накапливать большие объемы информации, и с их помощью можно выполнять множество операций – от оплаты товаров и услуг до использования в медицинских целях для диагностики состояния здоровья в любой момент времени в любой обстановке. Для этого клиенту достаточно приложить палец к сенсору на карточке, и на экране монитора появится расшифровка показателей состояния здоровья клиента, но в банковских технологиях эти карточки пока не получили распространение вследствие высокой стоимости как самих карточек, так и считывающего оборудования. Наиболее широко лазерные карточки представлены в США.

4. По целевому назначению:

➢ **идентификационные** (служащие для идентификации их владельцев), в том числе клубные (прежде всего, визитная карточка элитного клуба, ресторана, фитнес-центра). Внешний вид клубной карты обязательно должен сочетать в себе элегантность и стиль, традиционность и оригинальность, респектабельность и элитарность. Обычно клубные карточки имеют связь с базой клуба (номер, ФИО, фото члена клуба);

➢ **дисконтные** - их используют торговые дома, супермаркеты, предприятия сферы обслуживания. Дисконтные карты позволяют клиентам постоянно пользоваться скидками, бонусами, дополнительными услугами в целой сети предприятий;

➢ **для денежных операций** - для безналичной оплаты товаров и услуг владельцам карты с соответствующего банковского карточного счета, а также для получения им наличных денег с указанного счета в банкоматах.

5. По эмитентам:

➢ **банковские карты**, выпускаемые банками (или консорциумами банков) и финансовыми компаниями;

➢ **частные карты**, выпускаемые коммерческими нефинансовыми компаниями для платежей в торговой и/или сервисной сети данной компании;

➢ карты, выпускаемые организациями, чьей деятельностью непосредственно является **эмиссия карт** и создание инфраструктуры для их обслуживания.

6. По категории клиентуры, на которую ориентируется эмитент (в международных платежных системах это называется видами карт или продуктами):

➢ **обычные** (стандартные);

➢ «**серебряные**» (бизнес-карты) - предназначены для сотрудников компаний, уполномоченных расходовать средства своей компании в определенных пределах;

➢ «**золотые**» - выдаются лицам с высокой кредитоспособностью и предусматривают разные льготы для пользователей;

➢ **электронная карточка** - для получения наличных в банкоматах и в специальных электронных терминалах (Electronic Banking Mashine - EBM, или Automatic Teller Mashine - ATM), например “Cirrus/Maestro”, “Electron Visa”. Она является разновидностью дебетной карточки, предназначена для получения наличности в пределах имеющихся на счете клиента средств и внесения наличных денег на счет клиента. Может быть выдана любому клиенту.

7. По времени использования:

➢ **ограниченные** каким-либо временным промежутком (иногда с правом пролонгации);

- **неограниченные** (бессрочные).

8. По территориальной принадлежности:

- **международные**, действующие в большинстве стран;
- **национальные**, действующие в пределах какого - либо государства;
- **локальные**, используемые на части территории государства;
- **карты**, действующие в одном конкретном **учреждении**.

9. По сфере использования:

- **универсальные** карты - служат для оплаты любых товаров и услуг;
- **частные коммерческие** карты - служат для оплаты какой-либо определенной услуги (например, карты гостиничных сетей, автозаправочных станций, супермаркетов).

10. В зависимости от владельца картсчета:

- **личные - индивидуальные**, выдаваемые только физическим лицам; могут использоваться другими лицами, например, членами семьи, друзьями и др., на основании доверенности владельца данной карточки;
- **корпоративные** - выдаваемые только юридическим лицам; предназначаются исключительно для осуществления безналичных расчетов и не могут быть использованы для выплаты заработной платы и др. выплат социального характера, а также для выплаты наличных денежных средств.

11. По режиму функционирования:

- **дебетовые** - карты, которые позволяют их держателю распоряжаться средствами, находящимися на счете (оплата товаров и услуг), и/или получать при необходимости наличные (все в пределах расходного лимита, установленного банком). Данные карты позволяют клиенту банка получать наличные в банкоматах и оплачивать свои покупки только в пределах суммы, имеющейся на его специальном карточном счете (либо просто на счетах в банке - эмитенте карты);

➢ **кредитные** - карты, которые позволяют их держателям оплачивать товары и услуги и/или получать наличные в размере предоставленной банком кредитной линии (в пределах лимита). Клиент банка, пользующийся такой картой, имеет возможность получать у банка ограниченный кредит в случае оплаты картой товаров или услуг. Выданный клиенту кредит затем погашается путем списания необходимой суммы с его страхового депозита либо клиент компенсирует банку расходы из собственных сбережений наличными или с другого счета.

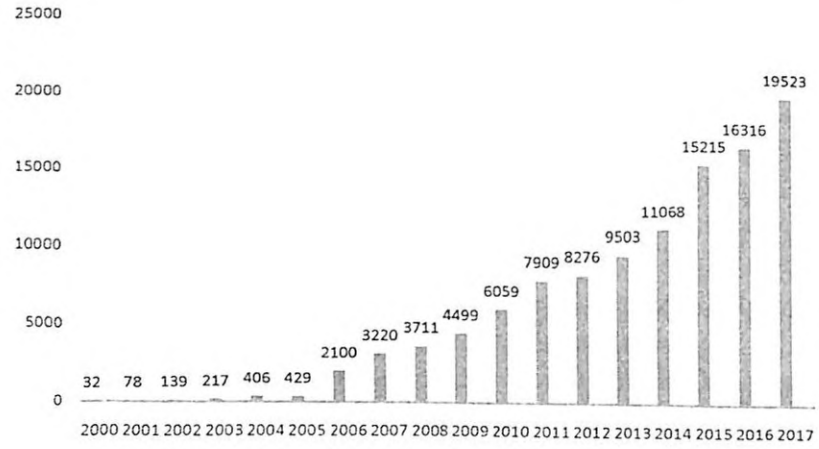

Рис. 7. **Количество выпущенных в обращение банковских карт**[13] (на 1 января, тыс.шт.)

За рубежом по способу пользования или по назначению различаются три вида платежных карт. Наиболее распространенными платежными картами общего назначения являются *дебетовые* карты, *кредитные* карты и *отложенные дебетовые* карты. Как кредитные, так и отложенные дебетовые карты используются, когда откладывается платеж и предоставляется кредит. Существуют и другие карты, такие как *одноразовые* и *многоцелевые* карты

[13] http://www.cbu.uz/ru/platyezhnye-sistemy.

предоплаты. Они выдаются небанковскими учреждениями или банковскими от имени торговцев для использования в указанных торговых точках.[14]

Как видно из рис. 7, особый толчок в выпуске пластиковых карт наблюдается начиная с 2005 года, очевидно, что этому способствовало Постановление Кабинета Министров Республики Узбекистан № 445 «О мерах по дальнейшему развитию системы расчетов на основе пластиковых карт», принятое 24 сентября 2004 года. В настоящее время количество выпущенных пластиковых карточек имеет устойчивую динамику роста.

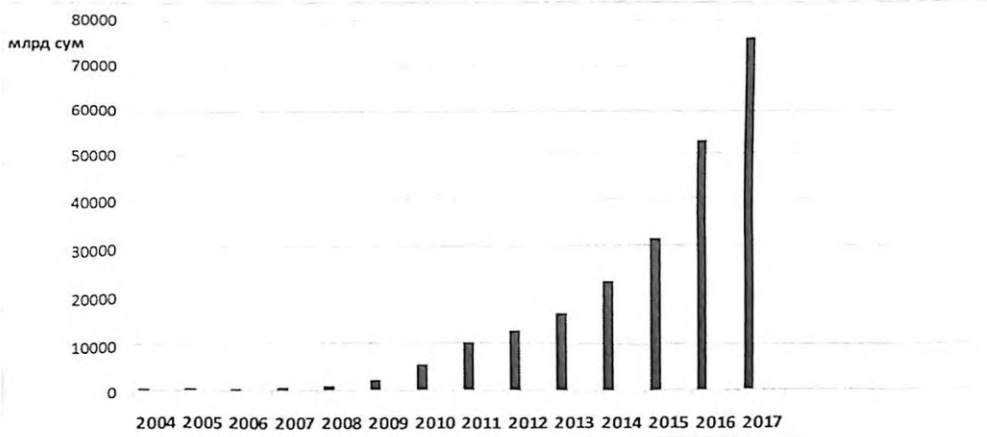

Рис. 8. **Сумма транзакций, осуществленных через банковские карты физических лиц в национальной валюте**[15]

На рис. 8 приведены данные о сумме транзакций, осуществленных через банковские карты физических лиц в национальной валюте. Как видно, динамика данного показателя имеет тенденцию устойчивого роста. В целом, за рассматриваемый период уве-

[14] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. С. 31.

[15] http://www.cbu.uz/ru/platyezhnye-sistemy.

личение данного показателя наблюдается с 2010 года, по сравнению с которым уже произошел десятикратный рост суммы транзакций.

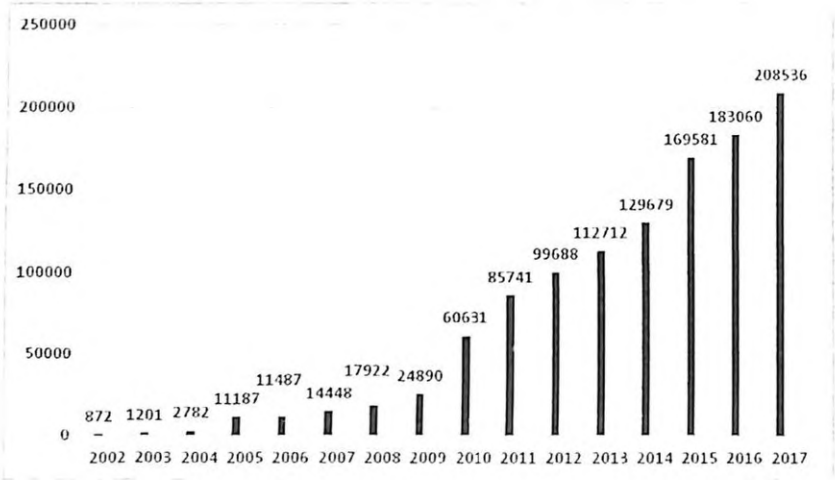

Рис. 9. **Количество установленных расчетных терминалов**[16]
(на 1 января)

На рис. 9 показана динамика изменения количества расчетных терминалов за 15 лет, резкий рост которых также наблюдается с 2010 года. К 2017 году количество установленных расчетных терминалов превысило 200 тысяч единиц.

Количество установленных банкоматов и инфокиосков к 2017 году составило около 5000 единиц, что видно из рис. 10. Интересным является то, что резкий скачок этого показателя произошел в 2016 году, в котором было достигнуто удвоение количества банкоматов и инфокиосков по сравнению с предыдущим годом.

Владельцы пластиковых карт широко используют преимущества этих карт, такие как возможность в безналичном порядке оплатить потребительские товары, различные услуги, кредиты банков, а также оплату топлива в бензоколонках страны.

[16] http://www.cbu.uz/ru/platyezhnye-sistemy.

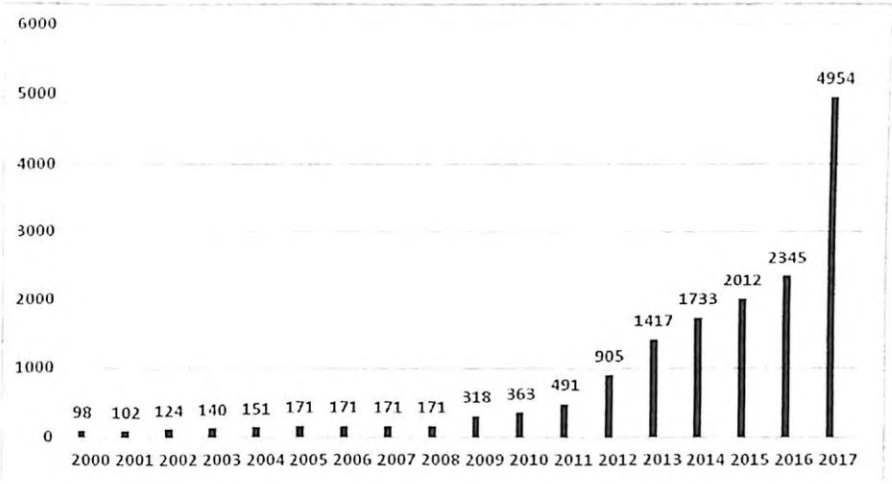

Рис.10. **Количество установленных банкоматов и инфокиосков**[17] (на 1 января)

Ключевые слова и понятия

Бесспорное списание средств, корреспондентский счет, очередность платежей, отказ от акцепта, акцепт, платежное поручение, формы безналичных расчетов, платежное требование, инкассовое поручение, покрытый аккредитив, непокрытый аккредитив, пластиковая карточка.

Вопросы для самопроверки

1. Каковы основные принципы организации безналичных расчетов?

2. Назовите формы безналичных расчетов, применяемых в РУз.

3. Какие виды аккредитивов применяются при безналичных расчетах?

[17] http://www.cbu.uz/ru/platyezhnye-sistemy.

4. Что понимается под инкассо?

5. Какова практика очередности платежей?

6. Что представляет собой акцепт, какова его роль и история применения?

7. В каких случаях производится безакцептное списание средств со счетов плательщика?

8. Какие счета используются при оплате платежного требования?

9. Каким образом осуществляются расчеты платежными поручениями?

10. В чем специфика использования расчетов инкассовыми поручениями?

11. Пластиковые карточки и их виды.

12. Развитие рынка пластиковых карт.

ГЛАВА III. СИСТЕМА ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ И ЕЁ РОЛЬ В ОРГАНИЗАЦИИ МЕЖБАНКОВСКИХ РАСЧЕТОВ

3.1. Сущность и значение системы электронных платежей, её развитие в Узбекистане и принципы её работы

Наиболее важным элементом инфраструктуры финансового рынка республики, обеспечивающим его стабильное функционирование, является платежная система. Динамично развивающаяся, надежная национальная платежная система, эффективность макроэкономических инструментов, регулирующих деятельность ее членов, качество законодательных и нормативных документов являются важнейшим условием не только дальнейшего обеспечения устойчивого экономического роста Узбекистана, но и признания его как равноправного члена мировой экономики.

В Законе Республики Узбекистан «Об электронных платежах» под платежной системой понимается совокупность отношений, возникающих между субъектами платежной системы при осуществлении электронных платежей. В более широком смысле, платежная система – это совокупность платежных инструментов, а также участников системы, которые по взаимной договоренности используют указанные инструменты для расчетов друг с другом (купли-продажи, кредитования, аренды и т.д.).

В стратегии развития национальной платежной системы, направленной на дальнейшее повышение ее эффективности и надежности, особую роль играют электронные платежи. Территориальный разброс клиентов банковско-финансового сектора, рост их количества и объема проводимых транзакций обусловили необходимость использования возможностей информационно-коммуни-

кационных технологий (ИКТ) для технического и программного сопровождения функционирования платежной системы. Тенденция увеличения использования ИКТ в финансовом секторе характерна для большинства развитых и развивающихся стран мира, недаром у крупнейших мировых производителей телекоммуникационного оборудования на банковский и страховой сектор приходится до 15% совокупного объема продаж.

По мнению ряда специалистов, системы электронных платежей входят в десятку технологических достижений, которые оказали наибольшее влияние на развитие человечества в течение последних пятидесяти лет, наравне с технологиями создания и обработки цифровых изображений, генной инженерией, космическими полетами, ядерной энергетикой, созданием роботов и систем искусственного интеллекта.

Сегодня для Узбекистана все более актуальными становятся вопросы, связанные с механизмами внедрения электронных платежей в практику республики и социально-экономическим эффектом от их использования. При рассмотрении этих вопросов нами будут использованы понятия - электронный платеж (Electronic transaction) и электронная система платежей (ЭСП) или система электронных платежей (СЭП).

Мировой опыт показывает, что причинами отказа от наличных средств (а в ряде стран и чеков) в пользу электронных платежей стал активный рост количества банковских пластиковых карточек и развитие электронной коммерции. В настоящее время в мире выпущено порядка одного миллиарда дебетовых карточек. Общемировая динамика этого средства платежа показывает, что повсеместно активно растет доля потребительских закупок, осуществленных с помощью пластиковых карточек.

В Узбекистане за последние годы очевидна тенденция увеличения количества пластиковых карточек, что свидетельствует не только об общем повышении финансовой грамотности и культуры граждан нашей страны, но также и эффективности принятых мер по развитию системы электронных платежей. Совершенствование

общенациональной платежной системы является одним из основных направлений реформ в банковской сфере страны. В рамках договоренности между правительством Узбекистана и Международной финансовой корпорацией проведено комплексное изучение национального рынка пластиковых карточек и разработана программа по расширению их использования. В республике создан Единый общереспубликанский процессинговый центр при Ассоциации банков Узбекистана. Система прохождения платежей строится на базе технологии DUET ((Direct Universal Electronic Transaction) международной компании BGS Smart CARD Systems AG, занимающей ведущие позиции в области разработки технологий и внедрения платежных систем на основе микропроцессорных пластиковых карт. Кроме того, в республике совершенствуется инфраструктура обслуживания сумовых пластиковых карточек, внедряется инфраструктура, обеспечивающая процессинг международных платежных карт. Лидерами в области эмиссии (банк-эмитент обслуживает покупателя) и эквайринга (банк-эквайер обслуживает продавца при покупке с использованием платежной карты) в Узбекистане сегодня являются Национальный банк внешне-экономической деятельности РУз и Государственно-акционерный коммерческий банк «Асака».

Внедрение ИКТ в финансовый сектор Узбекистана, в частности, для осуществления электронных платежей, стимулировали указы Президента и постановления правительства, а также отраслевые нормативно-законодательные акты и решения. Среди них, принятые в 2003-2009 гг. Олий Мажлисом законы Республики Узбекистан «Об информатизации», «Об электронном документообороте», «Об электронной коммерции», «Об электронных платежах», «Об электронной цифровой подписи», «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с усилением ответственности за совершение незаконных действий в области информатизации и передачи данных», «О защите информации в автоматизированной банковской системе», а также постановления Кабинета Министров Республ-

лики Узбекистан «О мерах по дальнейшему развитию системы расчетов на основе пластиковых карточек», «О мерах по дальнейшему совершенствованию проведения платежей при осуществлении электронной коммерции», Постановление Правления Центрального банка Республики Узбекистан «Об утверждении положения о порядке осуществления электронных платежей через межбанковскую платежную систему Центрального банка».

Внедрение электронных платежей, несомненно, должно регулироваться на государственном уровне. Говоря о макроэкономических аспектах электронных платежей этот вопрос, по нашему мнению, следует рассматривать сегодня в макроэкономической практике государства в следующих плоскостях. С одной стороны, совокупность макроэкономических рычагов (налоговые, тарифные в процессе проведения внешнеэкономической деятельности и др.) содействуют росту и эффективности функционирования системы электронных платежей страны. С другой стороны, рост использования электронных платежей сопровождается значительным экономическим и, в первую очередь, макроэкономическим эффектом.

Одним из эффективных макроэкономических рычагов стимулирования развития пластиковых карточек на территории Республики Узбекистан является освобождение от уплаты таможенных платежей коммерческих банков и предприятий по выпуску банковских микропроцессорных пластиковых карточек, платежных терминалов, банкоматов, информационных киосков (инфокиосков) самообслуживания, другого оборудования и расходных материалов, программного обеспечения, используемых при осуществлении платежей по пластиковым карточкам. Кроме того, коммерческие банки и Единый общереспубликанский процессинговый центр были освобождены от уплаты налога на имущество до 2010 года в части оборудования, а также программного обеспечения, используемых для осуществления платежей по пластиковым карточкам. В настоящее время разрабатывается новый порядок налогообложения и учета предприятий розничной торговли, осуществляющих электронную коммерцию.

Принятие на государственном уровне мер, реально стимулирующих развитие рынка безналичных расчетов, привносит в развитие Узбекистана как экономический, так и социальный эффект. Использование электронных платежей способствует значительному макроэкономическому эффекту. По оценкам специалистов, электронные платежи экономят около 1% ВВП, в основном, за счет повышения эффективности финансового посредничества. Снижается стоимость проводимых трансфертов, необходимость дополнительной эмиссии с целью насыщения рынка наличностью, а отсюда - необходимость печатания наличности. Использование электронных платежей приводит к уменьшению спроса на наличность и повышает скорость обращения денег. Внедрение электронных платежей приводит к сокращению внебанковского оборота наличности, что является одной из важнейших задач, поставленных перед банковской системой республики.

Электронные платежи повышают «прозрачность» финансовых потоков, что способствует сокращению объема теневой экономики. Значителен эффект использования электронных платежей для всех экономических агентов. При этом надо отметить, что капитальные затраты и расходы на техническое обслуживание – эксплуатацию и ремонт оборудования, задействованного при электронных платежах, относительно невелики, а эффект от их использования значителен.

Электронные платежи можно классифицировать по различным критериям: по типу плательщика, по местонахождению клиентов, по размеру платежа. В зарубежной экономической литературе различают оптовые платежи и платежи между нефинансовыми учреждениями.

Оптовые платежи - это платежи между финансовыми учреждениями. Обычно такие платежи проводятся на крупные суммы. Кроме того, они, как правило, должны проводиться и завершаться в определенный день - иногда даже в пределах определенного периода времени в этот день.

Платежи между нефинансовыми учреждениями (например, частными домохозяйствами, нефинансовыми корпорациями или государственными учреждениями) обычно классифицируются как **розничные платежи**. Как правило, эти платежи проводятся на более мелкие суммы, и по их осуществлению не устанавливаются строгие временные рамки.

В дополнение к двум вышеуказанным категориям иногда выделяют также **коммерческие платежи** (платежи, производимые корпорациями). В зависимости от размера и типа корпорации, а также типа коммерческой сделки, эти платежи могут иметь довольно большие значения, особенно по международным корпорациям.[18]

Являясь составной частью кредитно-денежной политики страны, система электронных платежей начинает проникать в такие смежные направления проведения макроэкономической политики, как налогово-бюджетная политика и политика международной торговли, повышая эффективность их функционирования. Все это происходит благодаря скорости и транспарентности проведения электронных платежей (при автоматическом режиме получения информации о поступающих налоговых платежах физических и юридических лиц, внедрении уплаты налогов через платежные терминалы, а также внедрении электронной системы таможенных платежей), в отличие от традиционных способов оплаты.

В зарубежной экономической литературе платежи также группируют на основе количества плательщиков и получателей платежей, участвующих в конкретной транзакции. Например, в сделке «один к одному» один плательщик перечисляет средства одному получателю: от клиента к клиенту. В транзакциях «один ко многим» один плательщик перечисляет средства нескольким получателям. Операции «один ко многим» также называются «массовыми платежами». В сделках «многие к одному» несколько плательщиков перечисляют средства одному получателю, обычно

[18] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. С. 27.

по инициативе получателя. Обычно это переводы частных домохозяйств предприятиям или государству - например, коммунальные или налоговые платежи.[19]

Активно развивающийся процесс глобализации в настоящее время сопровождается интеграцией финансовых рынков и информационного пространства, и качественно новым состоянием платежной системы на огромных территориях. Большую актуальность этот вопрос приобретает для Узбекистана и других стран ЕврАзЭС в силу роста взаимной экономической активности. По нашему мнению, с целью повышения эффективности взаимной торговли и продвижения инвестиционных потоков в рамках активно развивающихся экономических отношений стран СНГ и ЕврАзЭС рационально создать единую электронную платежную систему стран содружества. Большие потери связаны, во-первых, с конвертацией валют в процессе межстранового прохождения платежей и, во-вторых, высокими ценами на проводимые трансферты для расчетов в национальных валютах.

Опыт успешной интеграции в этом направлении показали страны – члены Евросоюза, а также Норвегия, Исландия, Лихтенштейн и Швейцария. Решая поставленную Еврокомиссией задачу снижения цен на проводимые в еврозоне трансферты, в начале 2008 г. ими начато введение единой платежной системы SEPA (Single Euro Payments Area). Речь идет о гигантском платежном рынке: ежегодно в странах Евросоюза производится 74 млрд. безналичных платежей – более одной трети мирового объема. За счет системы в еврозоне, на территории с населением в 330 млн. человек, будет обеспечено 85% всех безналичных транзакций. В перспективе планируется также перевод на единый общеевропейский стандарт мобильных платежей.

Развитие электронных платежных систем в Узбекистане напрямую зависит от уровня развития банковской инфраструктуры, качественных банковских услуг, в частности, от «технологической культуры» населения.

---

[19] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. C. 27.

В связи с этим был принят следующий ряд постановлений, направленных на развитие современных банковских услуг и совершенствование банковской инфраструктуры:

1. Постановление Кабинета Министров РУз от 24 сентября 2004 года № 445 «О мерах по дальнейшему развитию системы расчетов на основе пластиковых карточек».

2. Постановление Президента РУз от 17 апреля 2006 года ПП № 325 «О мерах по ускорению развития услуг и сервиса в РУз в 2006-2010 годах», где указано считать одним из основных направлений развития сферы услуг и сервиса новых перспективных видов – банковско-финансовых и информационно-коммуникационных услуг.

3. Постановление Президента РУз от 3 августа 2006 года ПП № 433 «О дополнительных мерах по дальнейшему развитию системы расчетов на основе пластиковых карточек». В постановлении установлено, что Узбекское агентство связи и информатизации по заявкам Ассоциации банков Узбекистана, Единого общереспубликанского процессингового центра и коммерческих банков в установленном порядке обеспечит предоставление соответствующих каналов и физических линий связи, а также телекоммуникационных услуг для организации обслуживания населения при осуществлении расчетов с использованием пластиковых карточек.

4. Постановление Президента РУз от 7 ноября 2007 года ПП № 726 «О дополнительных мерах по дальнейшему развитию банковской системы и вовлечению свободных денежных средств в банковский оборот».

5. Постановление Президента РУз от 6 апреля 2009 года № ПП–1090 «О дополнительных мерах по дальнейшему стимулированию привлечения свободных средств населения и хозяйствующих субъектов на депозиты в коммерческие банки» (создание при Народном банке национальной платежной системы «Uz-to'lov», в том числе с использованием пластиковых карточек, обеспечивающих быстроту, надежность и удобство осуществляемых денежных переводов для физических лиц 01.07.2009).

Нельзя реализовать эти постановления, не обеспечив прозрачность и безопасность транзакций. Для обеспечения безопасности взаимодействия при проведении транзакций в системе электронных платежей стороны используют электронную цифровую подпись (ЭЦП).

Согласно Постановлению Президента РУз от 08.07.2007 № ПП 117 «О дополнительных мерах по дальнейшему развитию ИКТ» УзАСИ (агентство связи и информатизации) определен специально уполномоченным органом в области использования ЭЦП и УзАСИ разрабатывает законодательные - нормативные акты, государственные стандарты, технологические условия и требования по использованию ЭЦП.

Постановлением Кабинета Министров РУз от 26.09.2005 г. № 215 «О совершенствовании нормативно-правовой базы в области использования ЭЦП», утверждены положения «О порядке государственной регистрации Центров регистрации ключей ЭЦП», «О порядке деятельности Центров регистрации ключей ЭЦП». Согласно постановлению УзАСИ является органом регистрации ключей ЭЦП.

Реализация обозначенных задач воплотилась в следующем:

15 марта 2006 года был открыт первый в РУз Центр регистрации ключей ЭЦП, являющийся необходимым компонентом для развития электронной коммерции, Интернет – банкинга, защищенного документооборота и других систем, использующих технологии инфраструктуры с открытыми ключами («Центр «UNICON.UZ»).

УзАСИ 25 мая 2007 года выдало второе свидетельство о государственной регистрации Центра регистрации ключей ЭЦП научно- информационному центру новых технологий Государственного налогового комитета РУз.

7 апреля 2008 года компания «Multisoft Solutions», разработчик информационно–коммуникационных и Интернет технологий, прошла регистрацию, как первый негосударственный Центр реги-

страции ЭЦП, и стала обладателем государственного свидетельства.

В начале 2009 года WebMoney Uzbekistan (ООО «TILLO-GARANT») зарегистрирован Узбекским агентством связи и информатизации в качестве Центра регистрации ключей электронных цифровых подписей, а в мае 2009 года таким центром стало также и ОАО «Navoiyazot».

Эти меры способствовали эффективному механизму осуществления электронных платежей.

3.2. Технологический процесс передачи информации посредством межбанковской платёжной системы

Межбанковские расчёты позволили обособить ресурсы каждого из банковских учреждений, что стало решающим фактором преобразования их в коммерческие банки, а Центральный банк Узбекистана смог задействовать инструменты денежно-кредитного регулирования экономики, принятые в мировой практике. Ибо механизм расчётов между коммерческими банками посредством движения средств по счетам, открытым в Центральном банке, является основой для регулирования последним деятельности банков второго уровня, и, в конечном счёте, всей экономики.

Правила межбанковской платежной системы определяются Центральным банком Республики Узбекистан. Межбанковская платежная система ЦБ функционирует в соответствии со следующими нормативно-правовыми документами:

- Законом Республики Узбекистан от 21.12.1995 г. № 154-I «О Центральном банке Республики Узбекистан»;
- Законом Республики Узбекистан от 25.04.1996 г. № 216-I «О банках и банковской деятельности»;
- Законом Республики Узбекистан от 16.12.2005 г. № ЗРУ-13 «Об электронных платежах»;

• Положением ЦБ от 14.02.2006 г. № 1545 «О порядке осуществления электронных платежей через межбанковскую платежную систему Центрального банка»;

• Положением ЦБ от 13.06.2013 г. № 2465 «О порядке проведения безналичных расчетов банками Республики Узбекистан».

Межбанковская платежная система является личной собственностью Центрального банка Республики Узбекистан. Участниками межбанковской платежной системы являются Главный центр информатизации и Центр расчетов ЦБ. Пользователями межбанковской платежной системы являются банки и финансовые институты, которые имеют корсчета в Центре расчетов ЦБ. **Центр расчетов** Центрального банка (далее - ЦР ЦБ) – это отдел управления учета, отчетности и расчетов Главного управления Центрального банка Республики Узбекистан города Ташкента, в функции которого входит открытие и обслуживание корреспондентских счетов головных офисов коммерческих банков и бесперебойное обеспечение электронных расчетов между ними. **Главный центр информатизации** Центрального банка (далее – ГЦИ) – центр, обеспечивающий техническое, программное и эксплуатационное сопровождение межбанковской платежной системы в соответствии с действующим законодательством, а также договорами между ГЦИ и банками.

Права и обязанности участников и пользователей межбанковской платежной системы регулируются двусторонними договорами банков-пользователей с ЦР ЦБ – на открытие и обслуживание корсчетов банков, с ГЦИ – на проведение электронных платежей через межбанковскую платежную систему.

Электронные платежи от банков осуществляются только в пределах остатка средств на корсчете, если иное не оговорено в договоре между ЦР ЦБ и банком.

С 9-00 до 16-00 часов – время передачи-приема-контроля электронных платежных документов (далее – ЭПД) по межбанковским расчетам:

1) банки в любой момент данного периода могут передавать ЭПД в ЦР ЦБ;

2) предназначенные для отправки ЭПД проходят контроль, заверяются электронной цифровой подписью, шифруются и по линиям банковской телекоммуникационной сети передаются для дальнейшей обработки в ЦР ЦБ.

До 17-00 часов производится передача ЭПД по переводу средств на соответствующие счета накопительной пенсионной системы республиканского бюджета. При этом до 16-30 часов завершается обработка ЭПД, направленных между коммерческими банками, а до 17-00 часов – ЭПД, направленных коммерческими банками в Центральный банк и Народный банк, а также из Центрального банка.

С 17-00 часов ГЦИ направляет банкам извещение о закрытии дня и информацию по отбракованным ЭПД (по банку-инициатору и банку-бенефициару).

После этого в ГЦИ осуществляется этап «Закрытие дня». Условиями выполнения этапа «Закрытие дня» в ЦР ЦБ являются:

- истечение времени приема ЭПД от банков;
- все ЭПД, переданные в ЦР ЦБ, должны быть обработаны и отражены на соответствующих корсчетах банков.

Время проведения этапа «Закрытие дня» в банках определяется самостоятельно в соответствии с требованиями внутрибанковской платежной системы.

Исходя из параметров денежно-кредитного управления Центрального банка Республики Узбекистан время перевода межбанковских ЭПД может продлеваться на основании письменного распоряжения заместителя председателя, контролирующего вопросы платежной системы. Об этом участники и пользователи системы извещаются не позднее чем за час до завершения времени обработки ЭПД.

Существуют три варианта подключения банков к межбанковской платежной системе:

1) подключение *платежного* (расчетного) центра банка;

2) подключение *банка, не имеющего филиала* (при этом электронные платежи производятся через операционное управление банка);

3) подключение *филиала банка.*

Для подключения платежного (расчетного) центра банка к межбанковской платежной системе банк обращается с письмом в Департамент платежной системы и информатизации Центрального банка (далее - ДПСИ ЦБ), в котором указывается наименование центра и его адрес. На основании этого письма ДПСИ ЦБ готовит порядок подключения платежного (расчетного) центра банка и перевода остатков корсчетов его филиалов.

Для подключения банка, не имеющего филиала, или филиала банка к межбанковской платежной системе они должны быть зарегистрированы в установленном законодательством порядке в Центральном банке Республики Узбекистан, иметь уникальный код в Национальной информационной базе банковских депозиторов (далее - НИББД) и располагать соответствующим программным комплексом, имеющим возможность выхода в межбанковскую платежную систему.

Порядок подключения банка, не имеющего филиала:

1. Департамент лицензирования и регулирования деятельности коммерческих банков Центрального банка извещает ДПСИ ЦБ о получении банком лицензии Центрального банка Республики Узбекистан на осуществление банковской деятельности с указанием полного наименования банка и его адреса.

2. На основании письменного сообщения ДПСИ ЦБ отдел НИББД ГЦИ резервирует для коммерческого банка уникальный код и соответствующие ему реквизиты и одновременно сообщает об этом банку и ДПСИ ЦБ.

3. Банк после получения уникального кода обращается в Центр регистрации Центрального банка, зарегистрированного в установленном порядке, для получения ключа электронной цифровой подписи, в ГЦИ - для определения аутентификационных данных для доступа к серверу ЦР ЦБ.

4. Производится экспериментальная проверка готовности банка путем проведения нескольких технологических циклов приема-контроля-передачи нескольких ЭПД с помощью работников ГЦИ. Эксперимент проводится в следующем порядке:

а) данные банка заносятся в соответствующий справочник на экспериментальном комплексе;

б) с работниками банка предварительно проводится инструктаж по совершению обмена информацией;

в) на корсчет банка в экспериментальном комплексе заносится предварительно оговариваемая сумма в качестве уставного фонда для работы банка;

г) банк формирует информацию и ЭПД для подтверждения остатка на корсчете банка и отправляет их в отладочном режиме в ГЦИ, ГЦИ проверяет правильность сформированных данных;

д) ГЦИ формирует для банка информацию по подтверждению корсчета, окончанию работы и обработке ЭПД, а банк должен подтвердить умение работать с ними;

е) эксперимент продолжается до получения положительных результатов проверки готовности банка. После завершения эксперимента ГЦИ совместно с банком составляет акт о состоянии готовности банка к работе в межбанковской платежной системе.

5. ДПСИ ЦБ на основании извещений Департамента лицензирования и регулирования деятельности коммерческих банков Центрального банка о выдаче банку лицензии, Департамента безопасности и защиты информации Центрального банка о готовности банка к работе в межбанковской платежной системе и акта ГЦИ о положительном результате эксперимента, а также копии удостоверения о регистрации в Государственном налоговом комитете, в котором указан идентификационный номер налогоплательщика, направляет всем банкам официальное сообщение об открытии банка, присвоении ему уникального кода в НИББД и подключении к межбанковской платежной системе.

Учитывая, что филиалы банка не открывают счета в ЦР ЦБ, все подготовительные работы (экспериментальная проверка го-

товности филиала, создание ключа электронной цифровой подписи) по подключению филиалов банка к межбанковской платежной системе банки ведут самостоятельно. Для резервирования уникального кода филиалу банк обращается непосредственно в отдел НИББД ГЦИ.

Ключевые слова и понятия

СЭП (система электронных платежей), Центр расчетов Центрального банка, банк–инициатор, банк-бенифициар, межбанковские расчеты, межфилиальные расчеты, корреспондентский счет филиала, единый корреспондентский счет головного банка.

Вопросы для самопроверки

1. Сущность и значение системы электронных платежей, её развитие в Узбекистане и принципы её работы.
2. Бухгалтерская модель ведения межбанковских расчетов.
3. Технологический процесс передачи информации посредством межбанковской платёжной системы.
4. Сущность электронной подписи и ее значение.
5. Содержание Положения ЦБ РУз «О ведении расчетов между банками Республики Узбекистан по системе электронных платежей».
6. Функции Главного центра информатизации (ГЦИ).

ГЛАВА IV. ПЛАТЕЖНАЯ СИСТЕМА, ОСНОВАННАЯ НА ЕДИНОМ КОРРЕСПОНДЕНТСКОМ СЧЕТЕ

4.1. Понятие единого корреспондентского счета. Бухгалтерская модель организации расчетов между банками

В течение 2002-2003 годов банки Республики Узбекистан перешли на расчеты в порядке единого корреспондентского счета (корсчета). Проведение межбанковских расчетов в системе единого корсчета имеет ряд преимуществ, позволяющих:

1) делать рациональное распределение ресурсов на каждый операционный день, в соответствии с требованиями каждого подчиненного филиала;

2) проводить расчеты между филиалами банка только через внутреннюю систему без расхода средств единого корсчета, путем перераспределения ресурсов;

3) вести централизованный контроль за использованием ресурсов;

4) получать допуск на работу в СЭП только на основании сверки состояния единого корсчета, общего для всех подчиненных филиалов;

5) производить самостоятельный анализ работы всех подчиненных филиалов по проведению межбанковских расчетов.

Филиалы коммерческих банков открывают корсчета в Головном банке, а Головной банк открывает единый корсчет в Центре расчетов Центрального банка. Внутренний корсчет филиала коммерческого банка на его балансе учитывается по счету 16103 «К получению из Головного офиса/филиала по межфилиальным и межбанковским расчетам». Внешний корсчет филиала на балансе Головного банка учитывается по счету 22204 «К оплате в Голов-

ной офис/ филиалы по межфилиальным и межбанковским расчетам». Единый корсчет Головного банка на его балансе учитывается по счету 10301 «К получению с корреспондентского счета в ЦБРУ – Ностро».

Учет межфилиальных и межбанковских расчетов в условиях использования единого корсчета ведется в соответсвии с «Положением о ведении расчетов между банками РУз, по системе электронных платежей», утвержденным ЦБ РУз 8.02.2001 г.- № 485 (Министерством Юстиции РУз- 19.02.2001 г. - № 1010).

По межфилиальным платежам (между филиалами одного банка) осуществляются следующие проводки:

При проведении межфилиальных расчетов в филиале-инициаторе программно совершается следующая бухгалтерская проводка:

Дебет – Счет клиента или внутрибанковский счет.

Кредит 16103 – К получению из Головного офиса/филиала по межфилиальным и межбанковским расчетам.

В головном банке программно формируются следующие бухгалтерские проводки по переводу средств между филиалами:

Дебет 22204 филиал «А» – К оплате в Головной офис/ филиалы по межфилиальным и межбанковским расчетам.

Кредит 22204 филиал «Б» – К оплате в Головной офис/филиалы по межфилиальным и межбанковским расчетам.

При получении платежей по межфилиальным расчетам в филиале-бенефициаре программно совершается следующая бухгалтерская проводка:

Дебет 16103 – К получению из Головного офиса/филиала по межфилиальным и межбанковским расчетам.

Кредит – Счет клиента или внутрибанковский счет.

По межбанковским платежам (между филиалами разных банков) осуществляются следующие проводки:

В филиале-инициаторе программно совершается следующая бухгалтерская проводка:

Дебет – Счет клиента или внутрибанковский счет.

Кредит 16103 – К получению из Головного офиса/филиала по межфилиальным и межбанковским расчетам.

В головном банке-инициаторе совершается следующая бухгалтерская проводка:

Дебет 22204 – К получению из Головного офиса/филиала по межфилиальным и межбанковским расчетам.

Кредит 10301 – К получению с корреспондентского счета в ЦБРУ – Ностро.

При поступлении платежа в головном банке-бенефициаре совершается следующая бухгалтерская проводка:

Дебет 10301 – К получению с корреспондентского счета в ЦБРУ – Ностро.

Кредит 22204 – К получению из Головного офиса/филиала по межфилиальным и межбанковским расчетам.

При поступлении электронного платежа по межбанковским расчетам в филиале-бенефициаре совершается заключительная бухгалтерская проводка:

Дебет 16103 – К получению из Головного офиса/филиала по межфилиальным и межбанковским расчетам.

Кредит – Счет клиента или внутрибанковский счет.

Основным критерием при расчете суммы, в пределах которой филиалы банка могут производить расчеты, является сумма средств на корсчете филиала банка. Поэтому при проверке принимаемой от филиала порции платежных документов на «нехватку средств», проверке будет подвергаться каждый отдельный документ независимо от кода филиала, его сумма будет сравниваться с последним состоянием остатка на его корсчете.

В зарубежной экономической литературе межбанковские корреспондентские отношения называют корреспондентскими банковскими механизмами или корреспондентскими банковскими соглашениями, которые бывают двусторонними и трёхсторонними.

В двусторонних корреспондентских банковских соглашениях два финансовых учреждения производят сортировку и обработку платежей самостоятельно, без привлечения посредника. Однако,

как правило, термин «корреспондентские банковские соглашения» относится к договоренности, в которой два финансовых учреждения используют третью сторону – отдельное финансовое учреждение, известное как «банк - корреспондент» или «учреждение, предоставляющее услуги». Одно или оба учреждения направляют платежные документы на предоставление услуг в банк для сортировки и обработки.[20] Указанные корреспондентские отношения предполагают международные расчеты, которые имеют свою специфику и являются отдельным предметом изучения.

4.2. Организация безопасности электронной информации

Конкурентоспособность, надежность и массовое использование электронных платежных систем основывается на безопасности системы и сети. Как мы знаем, сегодня появилось множество видов несанкционированных действий в сети, а именно, рассылка спама; взлом веб-сайтов и серверов; создание, распространение и внедрение вирусов, вредоносных кодов и программ; киберпреступность «фишинг» (phishing) и его новые виды «фарминг» (pharming), «вишинг» (vishing). С бурным развитием Интернета в Узбекистане имеются также случаи по инцидентам и угрозам в области информационной безопасности.

По результатам деятельности службы UZ-CERT периодически выявлялись следующие негативные результаты: часть веб-сайтов государственных органов не соответствовала необходимому уровню информационной безопасности. Некоторые из них использовали старые и уязвимые версии программного обеспечения. Часть корпоративных сетей государственных органов не соответствовала минимальным требованиям информационной безопасности. В части государственных органов не было отдела по обеспечению информационной безопасности или лица, исполняющего

[20] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. С. 39.

эти обязанности. В отдельных организациях персонал, обслуживающий информационные системы, являлся низко квалифицированным, или отсутствовало достаточное количество штатных единиц.

Рынок электронных платежей в Узбекистане имеет тенденцию к развитию, постепенно увеличивается количество пользователей Интернет, которые производят финансовые операции в сети, совершают онлайн-покупки. Именно по этой причине уделяется особое внимание безопасности электронных платежей. А это значит, что нужно пресечь возможные инциденты, такие как фишинг, кража паролей в зоне «.UZ». Согласно международному опыту, в первую очередь безопасность электронных платежей должна быть обеспечена в законах и нормативных актах государства, а для этого нужно ужесточить санкции против киберпреступников, так как мягкость наказания (например, наказание в виде штрафа) и сложность расследования такого рода уголовных дел являются одной из главных причин роста киберпреступности. Так 27 сентября 2007 года Законодательной палатой Олий Мажлиса РУз был принят закон «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с усилением ответственности за совершение незаконных действий в области информатизации и передачи данных». Целью закона является, прежде всего, установление ответственности за противозаконные действия в области информационно-коммуникационных технологий, а именно - определение норм для привлечения к уголовной или административной ответственности при выявлении соответствующих правонарушений. Согласно этому закону, в Уголовный кодекс Республики Узбекистан, Уголовно-процессуальный кодекс Республики Узбекистан, Кодекс Республики Узбекистан об административной ответственности внесено ряд изменений и дополнений.

Кроме того, нужно упомянуть то, что для минимизации рисков, связанных с мошенническими операциями, целесообразно

платежным системам обмениваться соответствующей информацией, составить «black list».

Ответственность по обеспечению безопасности функционирования электронных платежей должны нести и компании, продающие эти услуги (согласно закону «Об электронных платежах»). Компании должны не только проводить «promotion» своих услуг, вкладывать средства в обеспечение их безопасности, но и проводить разъяснение своим клиентам правил предосторожности, которые те должны соблюдать. Чтобы донести всю необходимую информацию до потребителя и поднять уровень правовой, финансовой грамотности и «технологической культуры» населения, необходимо проводить целенаправленную разъяснительную работу среди всех потенциальных пользователей о видах и эффективности использования электронных платежных систем.

Основываясь на вышесказанном можно сказать, что в Узбекистане создается благоприятная среда для развития электронных платежных систем, создается правовая основа, и при этом государство не ограничивается только принятием законов. Так как технологии бурно развиваются, в некоторых случаях они, по сути, из-за инновационности требуют координации законодательства сферы информационно-коммуникационных технологий, банковско-финансовой сферы, различных отраслей права, в том числе уголовного и гражданского права республики, добавления новых пунктов.

Ключевые слова и понятия

Центр расчетов Центрального банка, отдел обработки данных Центрального банка, Главный центр информатизации Центрального банка, корреспондентский счет банка, единый корреспондентский счет банка, электронный платежный документ, межфилиальные расчеты, межбанковские расчеты.

Вопросы для самопроверки

1. Понятие единого корреспондентского счета и его значение.

2. Особенности единого корреспондентского счета в платёжной системе.

3. Дайте характеристику бухгалтерским счетам, которые используются банками при учете операций по межбанковским и межфилиальным расчетам.

4. Организация расчетов между банками и их филиалами на основе единого корреспондентского счета.

5. Организация безопасности электронной информации.

6. Центр расчетов и его основные функции.

ГЛАВА V. ПЛАТЕЖНАЯ СИСТЕМА, ОСНОВАННАЯ НА ПРОГРАММНОМ ОБЕСПЕЧЕНИИ «БАНК-КЛИЕНТ»

5.1. Программное обеспечение «Банк-Клиент», его значение и основные функции

Программный комплекс «Банк-Клиент» (далее – ПК «Банк-Клиент») предназначен для автоматизированного взаимодействия банка и клиента, способствует повышению оперативности управления денежными средствами и позволяет:

- клиенту экономить свое время и средства за счет отказа от ежедневных визитов в банк:
- клиенту выбирать банк, не обращая внимания на территориальную близость:
- оказывать банковские услуги клиенту посредством создания у него на дому или в офисе автоматизированного рабочего места;
- расширить перечень услуг, оказываемых клиенту в плане информационного и операционного обслуживания;
- повысить производительность труда бухгалтеров банка;
- обеспечить высокую оперативность и качественную регистрацию операций.

Функционирование ПК «Банк-Клиент» основано на файловом обмене информацией между банком и клиентом по коммуникационным каналам связи.

Для обмена информацией с клиентами в банке создаются почтовые ящики клиентов, доступ к которым осуществляется клиентами по идентификатору и паролю.

Обработка запросов клиентов, прием-передача информации производится в автоматическом режиме.

Основными задачами ПК «Банк-Клиент» являются:

- подготовка электронных денежно-расчетных документов;

- формирование запросов и сообщений;
- шифрование информации и электронная подпись;
- модемная связь с банком;
- прием-передача информации;
- обработка полученной информации;
- печать выходных форм;
- архивирование информации.

Взаиморасчеты и обмен информацией между пользователями программного обеспечения системы «Банк-Клиент» в Республике Узбекистан осуществляется на основе Положения Центрального банка РУз № 497 от 08.10.1998 г. «О проведении расчетов с использованием ПК "Банк-Клиент», разработаного в соответствии с Гражданским кодексом Республики Узбекистан, законом «О банках и банковской деятельности», положениями «О безналичных расчетах в Республике Узбекистан» и «О ведении расчетов между банками Республики Узбекистан по системе электронных платежей», и другими нормативными документами Центрального банка Республики Узбекистан.

На основании первых экземпляров денежно-расчетных документов, клиент осуществляет ввод данных в компьютер. По окончании ввода документов, необходимо распечатать опись введенных документов. Ответственный работник (главный бухгалтер или другое лицо, на которое возложена эта обязанность) должен сверить опись с первыми экземплярами денежно-расчетных документов, поступившие по системе электронных платежей денежно-расчетные документы, после исполнения помещаются в почтовый ящик клиента.

Вся информация, полученная от клиентов, ежедневно архивируется и хранится в установленном порядке. Количество пользователей ПК «Банк- Клиент» в нашей стране постоянно растёт, что потверждается данными ЦБ РУз в динамике.

На рис. 11 показан график роста пользователей дистанционного банковского обслуживания. Как видно, постепенно идёт увеличение числа пользователей Интернет-банкинга и системы

«Банк-Клиент», которое с 2011 до 2017 года увеличилось почти в 10 раз.

Развитие системы «Банк-Клиент» в Узбекистане происходит вместе с развитием Интернет-банкинга в стране. 9 апреля 2002 г. в адрес Национального банка поступило официальное сообщение от АФИРАТО (Ассоциации финансовых институтов развития Азии и Тихого Океана) о победе и присуждении награды НБУ в номинации «Развитие технологий» за выдвинутый банком продукт — «Система удаленного электронного обслуживания клиентов» (Система R-Bank).

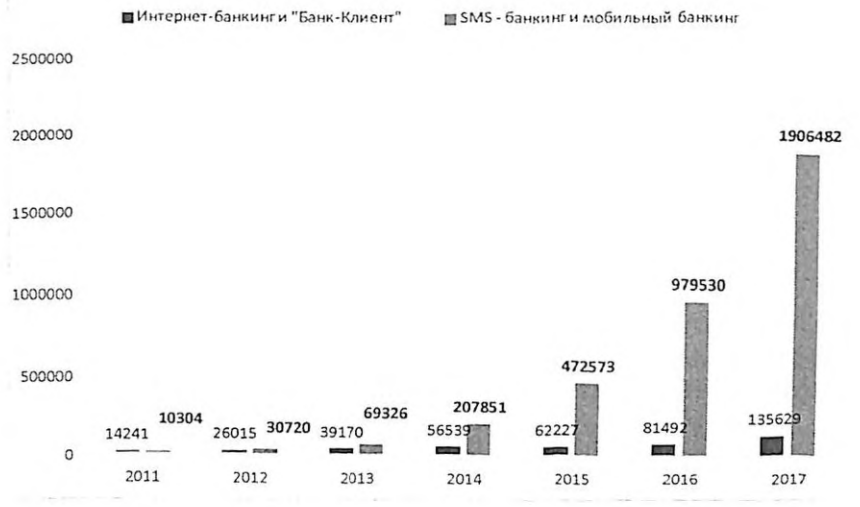

Рис. 11. **Количество пользователей дистанционным банковским обслуживанием по видам систем**[21]

Награждение состоялось на торжественном вечере во время проведения 25-ой ежегодной конференции и генеральной ассамблеи АФИРАТО в 2002 г. в период с 14 по 16 мая 2002 г. Национальный банк ВЭД РУз разработал и внедрил одну из самых

[21] http://www.cbu.uz/ru/platyezhnye-sistemy.

современных банковских услуг — систему удаленного обслуживания клиентов, или, как сейчас принято называть, Internet-banking (Интернет- банкинг) — программный комплекс «Банк-Клиент», соответствующую самым высоким международным стандартам.

5.2. Порядок проведения расчетов через систему «Банк-Клиент»

Ввод электронных денежно-расчетных документов клиента в базу данных банка осуществляется по следующей схеме (рис. 12).

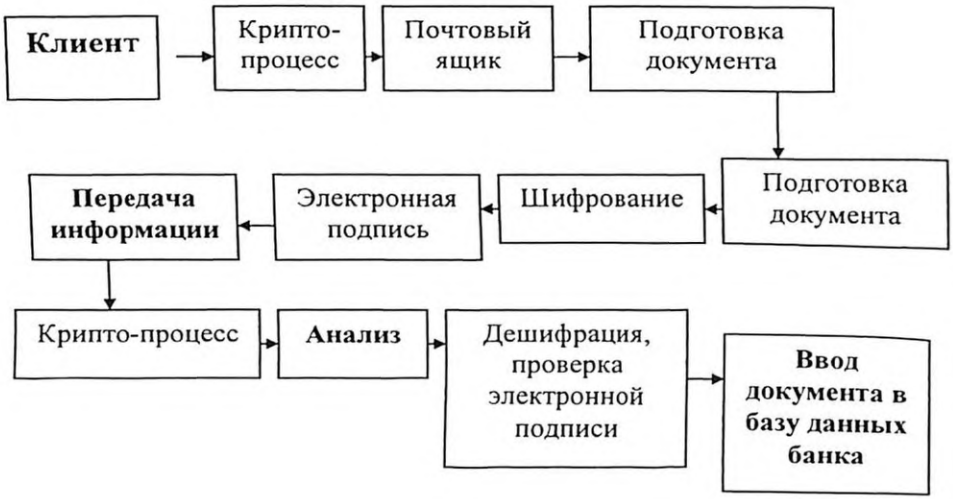

Рис. 12. **Схема ввода денежно-расчетных документов клиента в базу данных банка**[22]

ПК «Банк-Клиент» является собственностью банка.

Пользователями ПК «Банк-Клиент» являются клиенты, которые заключают договор с банком, регламентирующим их отношения в процессе работы.

При подключении ПК «Банк-Клиент» клиенту требуется:

[22] Составлено автором.

- персональный компьютер;
- модем;
- печатающее устройтсво;
- соответствующее программное обеспечение.

Клиент несет ответственность за правильность формирования электронных денежно-расчетных документов, шифрацию и передачу их в банк по каналам связи.

Банк несет ответственность за правильность зачисления и списания средств со счетов клиента и своевременную передачу информации по системе электронных платежей.

Обмен информацией по каналам связи между клиентом и банком осуществляется в оговоренное в договоре время.

Перед открытием нового операционного дня, клиент должен сверить с банком обороты и остатки на своих депозитных лицевых счетах за предыдуший операционный день.

В случае идентичности оборотов и остатков клиенту разрешается открыть операционный день и начать ввод документов. В противном случае устанавливаются причины расхождений, информация клиента приводится в соответствии с информацией банка.

Обмен информационными запросами и сообщениями осуществляется между клиентом и банком независимо от результатов сверки оборотов и остатков на депозитных лицевых счетах.

При осуществлении расчетов по системе «Банк-Клиент» клиент перечисляет средства со своего счета только в форме платежного поручения.

В банке электронные денежно-расчетные документы, полученные от клиента по каналам связи, после оплаты распечатываются в двух экземплярах:

- один экземпляр подшивается в документы дня банка в общем порядке;
- другой экземпляр остается в банке до получения оригиналов денежно-расчетных документов для сверки.

Клиент обязан, в сроки оговоренные в договоре, представить в банк оригиналы денежно-расчетных документов, отправленных в банк по каналам связи, где они сверяются с электронными денежно-расчетными документами, заверяются подписью бухгалтера, штампом банка, закрепленным за данным бухгалтером и вместе с экземплярами электронных денежно-расчетных документов подшиваются в документы дня банка.

В банке ведется отдельный документооборот по учету оригиналов денежно-расчетных документов клиентов, использующих ПК «Банк-Клиент».

Порядок работы клиента заключается в следующем:

Клиент оформляет денежно-расчетные документы согласно требованиям, установленным в положении «О безналичных расчетах в РУз». На основании первых экземпляров денежно-расчетных документов клиент осуществляет ввод данных в компьютер. По окончании ввода документов, необходимо распечатать опись введенных документов. Ответственный работник (главный бухгалтер или другое лицо, на которое возложена эта обязанность) должен сверить опись с первыми экземплярами денежно-расчетных документов, утвердить их тождество и дать разрешение на отправку в банк. После утверждения информации электронной подписью, она проходит криптографическую защиту и формируется электронный файл, который по каналам связи передается в обслуживающий коммерческий банк.

После криптографической защиты файл становится недоступным для клиента. Принятая из коммерческого банка информация программно обрабатывается и формируется опись поступивших документов, электронные денежно-расчетные документы и лицевые счета.

Клиенту недоступны корректировка и удаление полученной информации, он может только просмотреть и распечатать ее. Вся информация по денежно-расчетным документам, отправленная и поступившая из банка, программно архивируется и хранится в порядке, установленном Госархивом. По истечению срока хранения

информация программно удаляется из архива. Доступ к архиву имеет только ответственный работник предприятия (организации).

Порядок работы банка заключается в следующем:

1. Для обмена информацией с клиентами в банке создаются почтовые ящики клиентов.

2. Вся информация, поступившая от клиентов, программно дешифруется, проходит реквизитный контроль и заносится в базу данных банка со статусом «Введен».

3. При необходимости ответственный работник банка на своем рабочем месте распечатывает электронные документы, нуждающиеся в дополнительной проверке, и согласует их с соответствующими отделами банка.

4. После проверки электронных денежно-расчетных докуметов они утверждаются и передаются на обработку в операционный день банка, а затем отправляются получателю по системе электронных платежей.

5. В случае отсутствия средств на счете клиента, весь файл с денежно-расчетными документами снимается с обработки и возвращается в почтовый ящик клиента, если иное не предусмотрено договором или другими нормативными документами.

6. Поступившие по системе электронных платежей денежно-расчетные документы, после исполнения помещаются в почтовый ящик.

Вся информация, полученная от клиентов, ежедневно архивируется и хранится в установленном порядке.

5.3. Развитие системы «Банк- Клиент» и её связь с системой «Интернет- банкинг»

Развитие системы «Банк-Клиент» в Узбекистане происходит вместе с развитием Интернет-банкинга в стране.

В 2008 году Национальный банк, первым из коммерческих банков, успешно внедрил принципиально новую услугу по сумовым пластиковым карточкам DUET Online – предоставление кли-

ентам доступа к их карточным счетам через Интернет с персональных компьютеров, находяшихся дома или в офисе. Теперь клиенты НБУ получили возможность загружать средства со счета на пластиковую карту и инкассировать торговую выручку без посещения банковского учреждения. В соответствии с намеченной программой развития системы DUET Online банком в опытную эксплуатацию внедрена ее новая версия с возможностью производить оплату со счетов в адрес получателей платежей, с которыми банком заключен соответствующий договор. При этом, пока речь не идет о получателях, имеющих свою биллинговую систему, таких как операторы сотовой связи и Интернет-провайдеры. В ближайшем будущем будут приниматься платежи только в оплату коммунальных услуг.

Сейчас в Узбекистане ведется работа по внедрению банковских операций через Интернет и через средства мобильной связи. В этом направлении Центральный банк изучает опыт зарубежных стран.

В частности, по развитию Интернет-банкинга установлено сотрудничество с банком Credit Suisse; делегация из Узбекистана побывала в Швейцарии и собрала нужную информацию. Также изучен опыт Казахстана по внедрению мобильного банкинга.

Особенно глубоко при внедрении новшеств будут учитываться вопросы обеспечения безопасности.

Узбекский InfinBank первым предложил своим клиентам услугу удаленного банковского обслуживания через Интернет. Таким образом, в республике создан первый в своем роде прецедент с запуском сервиса онлайн-банкинга для населения.

Для работы в системе InfinONLINE клиенту потребуется компьютер с любой операционной системой, произвольным веб-браузером и доступом в Интернет. Управлять банковским счетом можно с любого персонального компьютера, ноутбука, а также при помощи карманного компьютера.

На данный момент воспользоваться системой Интернет-банкинга могут клиенты учреждения – физические лица. В режиме

реального времени они могут управлять срочными и сберегательными вкладами (открытие, пополнение, закрытие вклада): осуществлять операции с кредитными счетами (погашение и заявка на кредит); проводить платежи за услуги операторов мобильной связи, интернет-провайдеров, коммунальных служб и пр.

Гарантией безопасности дистанционного взаимодействия между банком и клиентом выступает ЭЦП (электронно-цифровая подпись).

В Узбекистане Интернет-банкинг, как и рынок электронной коммерции в целом, находится на стадии формирования. Однако Интернет-банкинг является, пожалуй, наиболее перспективным на сегодняшний день сектором данного рынка. Так, по прогнозам некоторых банков, реализация проектов Интернет-банкинга позволит расширить клиентскую базу на 30%. Этому способствует ряд факторов.

Во-первых, финансовые возможности банков позволяют им создавать современные, полностью отвечающие требованиям защиты информации и скорости осуществления операций, системы Интернет-банкинга. В среднем стоимость разработки и внедрения подобной системы составляет от 1 до 5 миллионов долларов США. Более того, большинство крупнейших банков уже создали и опробовали такие системы. Полномасштабному их использованию до недавнего времени мешало отсутствие законодательной базы. Поэтому использовались так называемые системы пассивного Интернет-банкинга, которые позволяли получать информацию о состоянии счета, однако эти системы не имели функций управления им.

Во-вторых, на рынке банковских услуг Узбекистана существует реальная потребность в Интернет-банкинге. Система «Банк-Клиент» доказала свою полезность и привлекательность для пользователей. Большинство предприятий и организаций, географически дистанцированных от крупных городов или же имеющих большой объем банковских транзакций, предпочли использование системы «Банк-Клиент» обычному очному обслуживанию. Интернет-банкинг превосходит системы «Банк-Клиент» с точки зре-

ния удобства использования. Кроме того, он позволяет управлять счетом из любой точки мира. Очевидно, что по мере внедрения систем Интернет- банкинга и повышения уровня доверия пользователей к ним, именно такие системы станут основным средством осуществления дистанционных банковских транзакций.

Все вышесказанное позволяет сделать однозначный вывод: для Узбекистана Интернет-банкинг является одним из наиболее перспективных рынков развития.

Основной задачей для узбекского Интернет-банкинга является на сегодняшний день завоевание пользователей. Для этого необходимо активно популяризировать системы Интернет-банкинга. Большинство банков не предоставляют доступ в свои системы в демонстрационном режиме, тогда как это позволило бы уменьшить степень недоверия пользователей к работе через Интернет. Кроме того, необходимо активно продвигать технолгоии Интернет-банкинга в общеэкономической и специализированной прессе. Необходимо создать Интернет-портал, посвященный Интернет-банкингу, на базе Центрального банка Узбекистана, где была бы централизованно представлена информация о данном секторе рынка, статистические данные, динамика его развития и т.д.

Для успешного преодоления недоверия пользователей, необходима твердая законадательная база для Интернет-банкинга. Это позволит выработать четкие и понятные «правила-игры» на Интернет – рынке. Также достаточно сложна и громоздка процедура сертификации специализированного банковского программного обеспечения. Создание четкой нормативной базы для банков, работающих на рынке Интернет-банкинга, несомненно, позволит повысить доверие пользователей к данному виду бизнеса.

Ключевые слова и понятия

ПК «Банк-Клиент», электронная цифровая подпись, закрытый ключ электронной цифровой подписи, открытый ключ электронной цифровой подписи, подтверждение подлинности электронной

цифровой подписи, электронный документ, почтовый ящик клиента, автоматизированное рабочее место, информационно-коммуникационные технологии, Интернет-банкинг.

Вопросы для самопроверки

1. Программное обеспечение «Банк-Клиент» и его значение.
2. Основные функции системы «Банк-Клиент».
3. Порядок проведения расчетов через систему «Банк-Клиент».
4. Распорядок дня клиента по программному обеспечению «Банк-Клиент».
5. Подготовка электронных денежно-расчетных документов.
6. Формирование запросов и сообщений.
7. Шифрование информации и электронная подпись.

ГЛАВА VI. ЭЛЕКТРОННАЯ ПЛАТЕЖНАЯ СИСТЕМА «ИНТЕРНЕТ-БАНКИНГ»

6.1. Роль электронной платёжной системы "Интернет- банкинг" в банковской деятельности

Интернет-банкинг – это высокотехнологичный банковский продукт, который предполагает проведение всех видов банковских операций из своего дома, офиса, с любого компьютера, имеющего доступ в глобальную сеть Интернет. Высочайшая степень безопасности, современные алгоритмы шифрования информации, использование цифровых сертификатов и 128-битного SSL-протокола, гарантирующего безопасную передачу данных по сети, электронные ключи digipass, уникальные пароли пользователя делают невозможным несанкционированный доступ к информации клиента.

Можно проводить следующие виды операций через Интернет:

- международные и местные платежи в любых валютах;
- выписку по расчётному счёту или группе счетов клиента;
- выписку за определённый период;
- просмотр остатков на расчётном счёте или счёте платёжной карточки в режиме реального времени;
- проведение операций по конвертации валюты;
- отправку в банк конфиденциальных писем, распоряжений.

«Интернет-Клиент» - канал предоставления полного спектра банковских услуг исключительно с помощью Интернет-технологий. Данная подсистема позиционируется и как самостоятельный продукт, и ориентирована на крупных клиентов банка, как физических, так и юридических лиц.

Данная система проводит следующие операции: ввод и обработку различных типов платежных документов клиентов банка,

как юридических, так и физических лиц; обмен сообщениями произвольного формата; получение выписок в различных видах и форматах, а также иной информации из банка; организацию Интернет-коммерции как самому банку, так и любому его клиенту; построение расчетных и клиринговых систем в режиме реального времени.

В данной системе совершенно оригинальные средства защиты, которые невозможно вскрыть. Массовость внедрения «Интернет-Клиента» обеспечивается «легкостью» самой системы и простотой начала работы с ней, что обусловливается использованием только стандартных Интернет-технологий, а также ее стоимостью.

При использовании «Интернет-Клиента» управление счетом и проведение различных банковских операций происходит при работе с обычным Web-сайтом банка, доступ клиентов к которому осуществляется через сеть Интернет. Клиент, из любой точки мира обращается к Web-серверу банка. На клиентской стороне не содержится никакой информации – все документы, справочники и иные ресурсы находятся в банке. Клиент может создавать и редактировать платежные (сумовые и валютные) и иные документы, просматривать архив документов, сообщения из банка и выписки за любой период, пользоваться стандартными справочниками (как общими - банков, курсов валют и др., так и персональными – корреспондентов, оснований платежа и т.д.) физически находящимися на стороне банка.

При подготовке любого документа осуществляется его контроль на корректность введенных данных, после чего осуществляется операция электронно-цифровой подписи. Далее документ пересылается на сервер банка и после процедур проверки подписи и правильности заполнения попадает в общую базу данных единой банковской части, где и производится его дальнейшая обработка (распечатка, посылка уведомлений, выгрузка в АБС, исполнение или отказ). При выполнении обработки документа, клиент получает результат об исполнении документа или его отказе с указанием причины такового.

Юридическая значимость подсистемы «Интернет-Клиент» обеспечивается следующими основными принципами:

- существованием между клиентом и банком договора на обслуживание по системе «Интернет-Клиент», определяющего их взаимоотношения, а также механизм решения конфликтных ситуаций со ссылками на основные функции системы, скрепленный физическими подписями и оттисками печатей сторон. Ключевым моментом такого договора является понятие электронно-цифровой подписи банка и клиента;
- электронно-цифровой подписью не только каждого документа со стороны клиента, но и всех сообщений, проходящих по системе в обе стороны, от клиента в банк и из банка клиенту;
- сохранением в журналах работы (обязательно на стороне банка и у клиента) всего прошедшего по системе траффика в исходном, зашифрованном и снабженном электронно-цифровыми подписями сторон виде для разрешения возможных конфликтных ситуаций.

6.2. Развитие Интернет-банкинга в Республике Узбекистан

Сегодня банки предлагают достаточно широкий спектр услуг, объединенных общим термином - дистанционное банковское обслуживание (далее - ДБО). Наиболее востребованным и распространенным является Интернет-банкинг и мобильный банкинг. Ряд банков Узбекистана предоставляют эти востребованные услуги не только юридическим, но и физическим лицам.

Интернет-банкинг подразумевает удаленный доступ к банковскому счету и управление им через Интернет круглосуточно в режиме реального времени со стационарного компьютера или ноутбука. Мобильный банкинг предоставляет практически такие же возможности, но в данном случае средством управления банковским счетом является мобильный телефон.

Сегодня на отечественном рынке все банки предоставляют услугу Интернет-банкинг или мобильный банкинг физическим лицам. Рост числа пользователей Интернета в Узбекистане, заставляет банки серьезно задуматься о предоставлении своих услуг населению через Интернет.

На развитие ДБО в стране было направлено Постановление Президента РУз от 26 ноября 2010 года, согласно которому все коммерческие банки Узбекистана к 2015 году должны были предоставлять физическим и юридическим лицам услуги Интернет- банкинга.

Таблица 2

Количество пользователей дистанционным банковским обслуживанием по отдельным банкам на 1 января 2017 г.[23]

№	Банк	Интернет-банкинг и «Банк-Клиент»	SMS-банкинг и мобильный банкинг	Итого
1	Национальный банк ВЭД	11 048	466 647	477695
2	АКБ «Узпромстройбанк»	16 207	48 139	64 346
3	АКБ «Агробанк»	27 227	798 896	826 123
4	АКБ «Ипотека-банк»	9 148	55 517	64 665
5	АКБ «Микрокредитбанк»	3 969	52 645	56 614
6	АКБ «Народный банк»	5 200	12 117	17 317
7	АКБ «Кишлок курилиш банк»	2 770	43 407	46 177
8	АКБ «Хамкорбанк» с уч. ин. кап.	21 198	80 486	101 684
9	АКБ «Асака»	2 904	128 151	131 055
10	АКБ «Алока банк»	4 258	116 955	121 213
11	Другие банки	31 700	103 522	135 222
	Всего	135 629	1 906 482	2 042 111

Как видно из данных таблицы, степень использования дистанционного банковского обслуживания по банкам различна. Бес-

[23] http://www.cbu.uz/ru/platyezhnye-sistemy.

спорными лидерами в этом отношении являются АКБ «Агробанк» и Национальный банк ВЭД.

В Узбекистане Интернет-банкинг появился в 2007 году как сервис для корпоративных клиентов. Следующим шагом его развития в стране стало внедрение этой услуги и для физических лиц.

Первым банком в Узбекистане, который наиболее полноценно предложил физическим лицам услуги Интернет-банкинга, стал банк «Samarkand». Банк 1 мая 2009 года объявил о запуске новой услуги в Интернете и назвал свой продукт Sam.online – Интернет- банкинг.

Клиенты банка Samarqandbank могли дистанционно оплачивать сотовую и городскую телефонную связь, услуги Интернет-провайдеров, коммунальные услуги, совершать покупки в Интернет-магазинах, переводить средства на счета юридических и физических лиц, отправлять в банки финансовые документы и получать информацию о движении по счету. Затем банк начал предоставлять возможность клиентам дистанционно выбирать и размещать свои деньги на банковских депозитах.

Samarqandbank стал первым в республике и в запуске мобильного банкинга, который был внедрен 1 марта 2010 года. С помощью мобильного телефона, клиенты банка смогли оплачивать сотовую связь и услуги Интернет-провайдеров.

Вторым внедрил Интернет-банкинг Алокабанк, который с 1 ноября 2010 года начал предлагать физическим лицам эту услугу. Затем появилась возможность удаленно оплачивать коммунальные услуги, услуги UzMobile, UzNet и следить за информацией по своим счетам.

В феврале 2011 года молодой банк Hi-Tech Bank также объявил о запуске услуги мобильного банкинга для физических лиц. Данная услуга дала возможность его клиентам с помощью мобильного телефона оплачивать за сотовую связь, услуги Интернет-провайдеров, домашний телефон и получать информацию о текущем состоянии и движении по счету.

Мобильный банкинг является логическим развитием Интернет-банкинга. Однако сегодня, во многих отечественных банках функционирует неполный его вариант, так называемый SMS-банкинг с информационным уровнем доступа, позволяющий отправлять и получать SMS - сообщения с информацией о текущих остатках и движении средств по депозитным счетам в том числе по карточным счетам держателей банковских пластиковых карт UZKART.

Стоит отметить, что дополнительному развитию услуг Интернет-банкинга в Узбекистане поспособствует появление системы мобильных электронных платежей - «SMS-To'lov». Данная система безналичных платежей представляет собой процессинговую систему платежей, сгенерированную в банковскую автоматизированную систему управления платежами между клиентом и компанией, в которую направляется платеж.

В отличие от услуги мобильного банкига, которая позволяет оплачивать услуги по мобильному телефону через сеть Интернета, система SMS-To'lov осуществляет платежи посредством отправки SMS сообщений. Кроме того, система также предоставляет клиенту возможность оплачивать приобретение товаров и услуг через личный кабинет на сайте компании.

17 марта 2011 года тестовые платежи через SMS-To'lov стартовали в операционном управлении Микрокредитбанка. В свою очередь, к приему платежей при помощи новой системы приступил и оператор сотовой связи Билайн.

Рядовых пользователей особенно волнует вопрос - насколько безопасно *дистанционное банковское обслуживание - ДБО*. Несмотря на то, что на отечественном рынке ДБО еще не было случаев мошенничества, но мировой опыт говорит о реальных случаях правонарушений в этой сфере. Тем не менее, при соблюдении правил, которые банки обязательно сообщают на своих сайтах, опасность пользованием Интернет-банкингом минимальна.

Список таких мер прост: установить на компьютере антивирусное программное обеспечение с регулярным обновлением баз

данных; соблюдать осторожность при установке на компьютер иного программного обеспечения (особенно – полученного из непроверенных источников), хранение паролей, ПИН-кодов, электронных цифровых подписей в недоступных для посторонних людей местах.

Особую бдительность нужно соблюдать при «серфинге» в Интернете и посещении малоизвестных подозрительных сайтов, в том числе – по ссылкам, пришедшим в электронных письмах от незнакомых отправителей. Кроме того, физическим лицам крайне не рекомендуется пользоваться системой Интернет-банкинга со служебного компьютера или из Интернет-кафе.

Специалисты мировых банков отмечают, что большинство обманутых мошенниками клиентов сами и сообщают злоумышленникам необходимую им информацию.

Создание системы Интернет-банкинга является достаточно сложной задачей с технической точки зрения. Опыт стран СНГ показывает, что банки предпочитают использовать специализированное программное обеспечение, разработанное третьими фирмами, нежели создавать свое. К сожалению, в Узбекистане на сегодняшней день нет крупных компаний, которые бы занимались разработкой банковского программного обеспечения. Поэтому желательно провести ряд мер по активизации и стимуляции рынка программного обеспечения.

На основании анализа мирового и национального рынков Интернет-банкинга, можно сделать вывод о том, что рынок Интернет-банкинга, как рынок электронной коммерции в целом, является одним из самых перспективных путей развития и интеграции в мировую экономическую систему.

Ключевые слова и понятия

Internet- banking, Интернет-Клиент, mailbank, Paytelecom, электронный платежный документ, банк-инициатор, банк-бенефициар, инициирование электронного платежа, платежная организация, пользователь платежной системы, член платежной системы, мобильный банкинг, дистанционное банковское обслуживание.

Вопросы для самопроверки

1. Развитие дистанционного банковского обслуживания и его особенности.
2. Роль малой платёжной электронной банковской системы “Internet-Banking” в банковской деятельности.
3. Юридическая значимость подсистемы «Интернет-Клиент».
4. Развитие Интернет-банкинга в Республике Узбекистан.
5. Содержание закона «Об электронном документообороте».

ГЛАВА VII. НОВЫЕ БАНКОВСКИЕ ТЕХНОЛОГИИ

7.1. Развитие Интернет- технологий при предоставлении банковских услуг

Одним из высокотехнологичных банковских продуктов в настоящее время является «Интернет-банкинг» - канал предоставления полного спектра банковских услуг исключительно с помощью Интернет-технологий.

В международной практике система «Интернет-банкинг» позиционируется и как «Интернет-клиент» и ориентирована на крупных клиентов банка, как физических, так и юридических лиц. Данная система проводит операции, необходимые для обслуживания клиентов: ввод и обработка данных с различных документов клиентов банка, организация Интернет-коммерции как самому банку, так и любому его клиенту; построение расчетных и клиринговых систем в режиме реального времени.

Остановимся на особенностях малой электронной системы платежей «MailBank». Модуль MailBank предназначен для удаленного обслуживания клиентов с помощью электронной почты и состоит из двух компонентов: «Клиент» и «Банк». Компонент «Клиент» устанавливается на компьютере клиента банка и предназначен для ввода, хранения, передачи данных в банк, приема и сохранения информации из банка. Имеет встроенные средства работы с электронной почтой и систему криптографии. Компонент «Банк» основывается на модуле «Сервер банка» и модулях интеграции с «Главной бухгалтерской книгой» банка.

При использовании банком модуля «MailBank» повышается скорость прохождения платежей. Высокая оперативность работы обусловлена тем, что платежное поручение в электронном виде готовится не работником банка, а работником предприятия. Кроме

того, не нужно подготавливать первичные платежные документы на бумажных носителях.

Вместо них раз в неделю готовится реестр электронных документов, благодаря чему отпадает необходимость в ежедневных посещениях банка для проведения безналичных платежей. Это экономит время и финансовые средства. Развитая система экспорта-импорта информации позволяет модулю «MailBank» легко интегрироваться с основными бухгалтерскими системами (1С и т.д.), что позволяет исключить повторный ввод документов перед отправкой их в банк, что экономит время клиентам. Модуль «MailBank» позволяет контактировать с банком без ограничений во времени, поскольку можно круглосуточно отправлять документы в банк и просматривать полученные оттуда сведения и данные.

Модуль «MailBank» значительно повышает производительность предприятия и бухгалтерского учета в результате снижения непроизводственных расходов персонала на коммуникации за счет: использования общей базы данных в модуле «MailBank»; повышения производительности труда персонала за счет сокращения объема рутинной работы при составлении и печати периодических реестров и выписок при выполнении различных расчетов, повышения эффективности ввода информации в модуле «MailBank» и исключения двойного ввода данных в банковскую систему; снижения вероятности ошибок и расхождений данных учета за счет распределения мест ввода информации, использования единой базы данных и надежных алгоритмов контроля корректности вводимых данных, создания предпосылок для повышения эффективности планирования и управления деятельностью предприятия, улучшения условий труда руководителей, исполнителей и др.

Система «PayTelecom» позволяет принимать платежи за телекоммуникационные услуги, и другие платежи в реальном времени. При этом система комбинирует в себе офф-лайн систему по

продаже PIN-кодов, разработанную компанией Lipman, а также он-лайн систему пополнения счета клиента в реальном времени.

В целях реализации системы в режиме реального времени, разработчиками было предложено доработать программное приложение компанией Lipman, а также разработано приложение «Pay Logical», для обеспечения связи системы с биллингом операторов связи в он-лайн режиме. Связь с биллингом операторов осуществляется через выделенный канал, защищенный физическими файрволами (от анг. firewall).

Принцип работы системы включает несколько этапов.

1. Клиент платит агенту

Клиент, зайдя в любую точку «PayTelecom», производит оплату несколькими простыми действиями. Он указывает название оператора или провайдера, номинал услуги, установленный провайдером или номер телефона (в зависимости, за какую услугу вносится платеж) и производит оплату.

2. Агент платит «PayTelecom»

Информация о принятом платеже от клиента будет передана в систему «PayTelecom», где происходит маршрутизация данных по соответствующим провайдерам. В завершении транзакции система «PayTelecom» распечатывает *информационный чек*, предназначенный для клиента. Проведенная транзакция фиксируется в системе «PayTelecom», биллинге оператора/провайдера и в отчетных формах *агента*. Агент перечисляет денежные средства на счет «PayTelecom» на основе принятых платежей от клиентов.

3. «PayTelecom» платит провайдеру

Принимаемые платежи также фиксируются в биллинге оператора или провайдера. На основе принятых платежей, «PayTelecom» перечисляет средства на счета соответствующего оператора или провайдера.

4. Провайдер активирует услугу для клиента

В случае приобретения номинала Интернет или международной телефонии, услуга предоставляется клиенту, после активации PIN кода в соответствии с его номиналом. При оплате за мобиль-

ный телефон, оператор отправляет SMS сообщение абоненту о пополнении счета.

Подводя итог необходимо отметить, что развитие современных информационных технологий побуждает коммерческие банки использовать альтернативные методы сбыта своих продуктов и обслуживания клиентов.

Таким образом, развитие технологий облегчает жизнь не только клиентам банков, но и самим банкам, что способствует росту эффективности работы и оптимизации многих процессов. Без современного банковского оборудования решение многих задач уже невозможно.

7.2. Сущность системы платежей посредством телефона - "PhoneBank" и её применение на практике

Мобильный телефон как терминал доступа к банковским услугам не требует от банка значительных инвестиций. Общее количество мобильных телефонов, которые находятся на руках у населения, в три раза превышает количество банковских карт, если считать и зарплатные, и «экспресс-кредитные». В этом смысле мобильный телефон является чрезвычайно привлекательным инструментом для банкиров, желающих и далее развивать ритейл. Особенно, если будут решены непростые технические и рганизационно-юридические вопросы использования мобильного телефона как платежного терминала, платежного средства. Вместе с тем формируется новая категория «продвинутых» пользователей мобильной связи, которые могут быть очень интересны банкам. Речь идет о wap-технологиях. О масштабах новой аудитории говорит тот факт, что в 2001 г. технологию wap поддерживали только две модели телефонов, а в 2003–2004 гг. начался бурный рост рынка и спрос аудитории. В итоге на сегодняшний день wap поддерживают практически все современные модели мобильных телефонов. Возможности wap-банкинга гораздо шире, чем sms-

банкинга. По сути, пользователь wap имеет доступ к сайту банка в режиме 7x24. Опять же, банк сокращает затраты на call-центр, привлекает прогрессивную молодежную аудиторию. А в перспективе, обещают провайдеры, возможно и разделение дохода с банками от wap-трафика. Учитывая все преимущества взаимодействия с клиентом через глобальную компьютерную сеть Интернет, некоторые банки предлагают усеченный вариант систем Интернет-банкинга (например, только просмотр выписок по счету). Эта бесплатная услуга предоставляется клиентам через web-сайт банка, размещенный в сети Интернет. Если же клиент не имеет доступа в Интернет, банк может за сумму, существенно меньшую по сравнению с тарифами обычных провайдеров, предоставить клиенту возможность посещать сайт банка, а также подключиться к электронной почте. Гораздо больший интерес представляет мобильный доступ в Интернет. Особенно активно развиваются сегодня различные Java-апплеты и другие приложения под Windows Mobile и др. Они представляют собой набор функций, представленных прямо на экране мобильного телефона (их не надо долго искать и выводить на экран). В режиме защищенного соединения они дают возможность предоставлять банковским клиентам необходимые сервисы. Например, находясь в машине, клиент может обратиться к своему счету, произвести и подтвердить оплату, посмотреть котировки акций, то есть получить некий информационный сервис от банка. Строго говоря, любая информация, которая содержится в АБС, с технической точки зрения может быть предоставлена клиенту с помощью Java и мобильного телефона. Если обычный телефон открывает доступ к информации в жестком статичном формате, то мобильный телефон позволяет «одеть» доступ к разрешенной информации в красивую программную оболочку и предоставить клиенту некоторую самостоятельность в получении информации. Скачать и установить необходимое программное обеспечение на телефон клиент сможет с сайта банка в режиме Интернет-банкинга. Разумеется, особенности мобильного телефона как информационного терминала тоже задают ограничения

по доступу к информации. Например, на «трубку» невозможно получить полноценную выписку по активному брокерскому счету, эту информацию лучше смотреть на экране компьютера. Но на телефон можно поставлять выжимки из информации, которые подвигнут клиента задуматься и зайти на сайт банка, чтобы посмотреть данные внимательнее.

По мнению ряда аналитиков, сам по себе доступ с мобильного телефона никому не интересен. Это хорошая опция, которую следует использовать в комплексе остальных возможностей. А стимулировать использование той или иной опции можно тарифами. Плата за получение одной и той же услуги путем использования Интернета, мобильного или телефонного банкинга должна быть разной. Если банк заинтересован в развитии дистанционного обслуживания, то самая большая плата должна быть при личном обслуживании в отделении банка. Разумеется, грамотное, эффективное использование всех возможностей дистанционного доступа возможно только в том случае, когда система отстроена и все технические решения внедрены. На стадии развития сети и формирования единой системы автоматизации банка и клиентского доступа можно говорить только о концепции. Пока еще грамотность населения достаточно низкая, и услуга дистанционного доступа воспринимается только узкой категорией клиентов. При этом одни виды доступа пользуются большей популярностью на конкретных территориях, другие - меньшей, а какие-то вообще не воспринимаются. Но выстраивание дистанционных отношений с точки зрения экономики больше необходимо банку, клиенту же дистанционный доступ дает дополнительные сервисные возможности. Для пользователя Интернет-банкинга обильный банкинг является пугающей новинкой, но, подключившись, человек понимает, что ничего принципиально нового и сложного банк не предлагает, а возможности растут. Так что недрение новых услуг и способов доступа - это вопрос времени и повышения грамотности клиентуры. Банковские ассоциации могут предпринимать шаги, направленные на повышение грамотности клиентов в этом во-

просе. Отдельным банкам такие расходы не по силам, хотя обучение, информирование клиентов по поводу новых сервисов банка происходит постоянно. Но главное для отдельного банка - к моменту, когда «клиент созреет», необходимо иметь внедренное решение, действующий сервис. Ведь если человек попробовал один интерфейс, жизнь его рано или поздно поставит в такие условия, когда ему понадобится освоить новый способ связи с банком. Аналитики прогнозируют стабильный рост числа случаев оплаты цифровых и физических товаров при помощи мобильных телефонов.

7.3. Банковские технологии в мировой практике и возможности их применения в Узбекистане

Развитие банковских технологий, прежде всего в США и евпопейских странах, стимулирует их расширение и в других регионах. При использовании новых банковских технологий в мировой практике при создании международных платежных систем большое внимание уделяется безопасности транзакций.

В платежных, клиринговых и расчетных системах участники сталкиваются с риском того, что расчет в системе не будет проведен. Эти риски могут привести к системному риску, если проблемы в рамках одного финансового учреждения распространятся на другие. Поэтому при разработке новых банковских продуктов с использованием высокотехнологичных Интернет - технологий большое внимание уделяется разработке ключевых концепций, касающихся рисков, относящихся к обработке платежей и операций, связанных с финансовыми инструментами, а также способов смягчения таких рисков.[24]

В 90-х годах XX века началось ускоренное развитие финансового сектора рынка. Необходимы были интегрированные системы, в которых результаты всех банковских транзакций могли бы неза-

[24] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. C. 115.

медлительно отражаться и учитываться в операциях всех входящих в них подразделений. В этих условиях автообработка банковской информации может обеспечить руководству банков согласованное управление рисками, ликвидностью, активами и обязательствами. В результате на рынке появится новый вид программно-технической и интеллектуальной продукции - «банковская платформа» (продукты совместной деятельности банков и компьютерных фирм). Она строится по модульному принципу и обеспечивает использование единой унифицированной базы для решения всех банковских задач.

Лидерами в области производства компьютерной техники являются: IBM (США), DEC(США), «Siemens» (Германия), «Olivetti» (Италия), "Bull" (Франция).

Так, IBM предлагает второе поколение машин AS/400 с современной операционной системой OS/400, которая обеспечивает защищенность данных, повышает производительность системы и пользователя как в пакетном, так и в диалоговом режимах при работе в сетях разнообразных конфигураций.

Пакет программ IBIS/AS, используемый в настоящее время, отвечает интересам всего персонала банковской системы, создает единую интегрирующую базу данных, предоставляет гибкие средства обработки операций, возможность подключения новых модулей без нарушения целостности существующей системы, обеспечивает пользователей всех уровней обширными стандартными отчислениями и справочниками. Данная система охватывает весь банк со специальной функциональной поддержкой каждого отдела в соответствующих модулях, которые сформированы в 2 группы:

1. Банковские модули, в т.ч. центральное место - «Главная бухгалтерия», банковские функциональные модули;

2. Вспомогательные модули («Архивация», «Аудиторские проверки», «Интерфейс SWIFT» и др.).

С участием фирмы DEC (США) головным разработчиком международной компании «Werter Perters» была создана между-

народная банковская система 90-х гг. Компания «Werter Perters» являлась в течение 20 лет лидером среди поставщиков систем для мирового финансового общества, активно работающей во многих странах мира.

Программа IBS-90 полностью интегрированная, работающая в реальном масштабе времени банковской системы, обеспечивает в режиме обработки транзакций одновременные операции с различными валютами во множестве географически удаленных регионах, автоматизирует оптовые банковские услуги, казначейские операции, инвестиционную деятельность и прочее.

Совместно с разработками «Cilidak of America» и специализированной компанией ITB фирма DEC разработала банковскую платформу будущего – FSA. Разработанные на базе FSA системы в настоящее время установлены в 10 крупных мировых финансовых центрах, включая Лондон, Нью-Йорк, Гонконг.

Для универсального банка фирма DEC создала еще одну банковскую платформу - «Profile». Она допускает генерацию и настройку трех типов систем под конкретные требования заказчиков (собственно интегрированной банковской системы, автоматизирующей все виды розничных услуг; системы управления финансами; системы автоматизации деятельности банка на вторичных ресурсах).

"Olivetti Systems Networks (OSN)" предлагает свою «банковскую платформу» (Platform for banking - PB) для автоматического банка ("Automatic banking"). Это комплексное решение, отвечающее тенденциям построения открытых систем, обеспечит создание гибкой и способной к расширению системы банковских учреждений, реализацию полного набора банковских функций в среде распределяющих услуг и приложений.

Фирма "Olivetti" накопила большой опыт в создании специализированных банковских устройств и автоматов, в т.ч. для систем самообслуживания клиентов банка-принтеров, устройств идентификации, автоматов по выдаче наличных денег, устройств работы со сберкнижками и т.д.

Компания “Bull” создала межбанковскую систему телерасчетов STT для ускорения межбанковских операций, обеспечения непрерывности обмена межбанковскими сообщениями, уменьшения их стоимости.

Для поддержки задач отделений и международных отделов любых по размерам банков фирма «Bull» рекомендует систему ICBS. Она состоит из модулей, функционирует под управлением ОС UNIX и реализовывает клиринговые операции и оформление необходимых отчетов по ним, выполняет функции контроля и управления доходами, курса валют, ставками, ценами, решает задачи взаимодействия с Центральным банком, обеспечивает выполнение международных операций и многое другое.

Таким образом, современное банковское дело в развитых странах мира становится тесно связано с информационно-коммуникационными технологиями, которые позволяют существенно повысить качество предоставляемых услуг, сделать их электронными и впоследствии – интерактивными (то есть подстраивающимися под запросы конкретного пользователя – клиента банка). Благодаря ИКТ удается полностью автоматизировать банковскую деятельность, повысить ее оперативность, надежность и улучшить контроль. Но на этом далеко не исчерпываются выгоды от использования современных информационно-коммуникационных технологий в банковской деятельности. В настоящее время создаются десятки, если не сотни новых банковских услуг, не имеющих в прошлом аналогов и обеспечивающие высокую прибыль для банков, их использующих.

Ключевые слова и понятия

«SMS-Banking», «Phone-bank» , «MailBank», «PayTelecom», «Upay», «Payme», электронная платежная система, автоматизированная банковская система.

Вопросы для самопроверки

1. Электронная платежная система “SMSbanking” и её использование на практике.

2. Сущность системы платежей посредством телефона - “PhoneBank” и её применение на практике.

3. Особенности малой электронной системы платежей “MailBank”

4. Банковские технологии в мировой практике.

5. Сущность автоматизированных банковских систем (АБС).

6. АБС, используемые отечественными коммерческими банками.

7. АБС, используемые зарубежными коммерческими банками.

ГЛАВА VIII. МЕЖДУНАРОДНАЯ ПЛАТЕЖНАЯ СИСТЕМА СВИФТ

8.1. Понятие международной платёжной системы СВИФТ и её организация

СВИФТ-S.W.I.F.T. (Society for World-Wide Interbank Financial Telecommunications) - сообщество всемирных межбанковских финансовых телекоммуникаций является ведущей международной организацией в сфере финансовых телекоммуникаций. Основными направлениями деятельности СВИФТ являются предоставление оперативного, надежного, эффективного, конфиденциального и защищенного от несанкционированного доступа телекоммуникационного обслуживания для банков и проведение работ по стандартизации форм и методов обмена финансовой информацией. В мае 1973 г. 239 банков из 15 стран согласно с бельгийским законодательством учредили СВИФТ, с целью разработки формализованных методов обмена финансовой информацией и создания международной сети передачи данных с использованием стандартизированных сообщений. Последующие четыре года были посвящены решению организационных и технических вопросов, и 9 мая 1977 г. состоялось официальное открытие сети. К концу года число банков-членов увеличилось до 586 (против 513). Они обеспечивали ежедневный трафик до 500 000 сообщений.

В настоящее время СВИФТ объединяет около 50 млн. пользователей (банков кредитных и финансовых предприятий). Все они самостоятельно, независимо от их географического положения, имеют возможность круглосуточного взаимодействия друг с другом 365 дней в году. В числе пользователей СВИФТ наряду с кредитными организациями - центральные/национальные банки, инвестиционные компании, биржи и центральные депозитарии.

Интересны данные о деятельности СВИФТ за декабрь 2017 года по Ежегодному отчету SWIFT.[25]

Пользователи сети СВИФТ:

- Общее количество стран - 204;
- Число членов – 2382;
- Число ассоциированных членов - 3329;
- Число участников – 5625;
- Общее количество пользователей – 11336.

Распределение трафика сообщений:

- Платежи - 49,3%;
- Операции с ценными бумагами - 45,6%;
- Торговля - 0,5%;
- Казначество - 4,3%;
- Системные сообщения - 0,3%.

Использование международных платежных систем является наиболее распространенным способом урегулирования платежных транзакций с участием счетов финансовых учреждений, находящихся в разных странах. Платежная система представляет собой официальную договоренность, основанную на законодательстве или договорные отношения - с множественным членством, общими правилами и стандартизированными процедурами - для передачи, клиринга, взаимозачета и/или расчетов по денежным обязательствам, возникающим между его членами.[26]

На базе СВИФТ построено более 50 национальных платежных систем, помимо этого СВИФТ является основой расчетной системы Ассоциации европейских банков и европейской системы TARGET. Предложенные и реализованные СВИФТ концепция, форматы и правила передачи финансовой информации приобрели сейчас статус общепринятого международного стандарта.

Применение единых стандартов СВИФТ в национальных платежных системах позволяет свести к минимуму расчетные и фи-

---

[25] https:// www.swift.com/about-us/swift-fin-traffic-figures/.

[26] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. С. 40.

нансовые риски, повысить эффективность и безопасность расчетов, удешевить стоимость сообщений. Кроме того, национальные платежные системы, построенные на основе СВИФТ, являются транспарентными и интегрируются в крупнейшие международные платежные системы.

СВИФТ не осуществляет клиринговых функций, являясь лишь банковской коммуникационной сетью, ориентированной на будущее. Передаваемые поручения учитываются в виде перевода по соответствующим счетам «ностро» и «лоро», так же как и при использовании традиционных платежных документов.

СВИФТ - организация бесприбыльная, вся получаемая прибыль идет на покрытие расходов и модернизацию системы. Неизрасходованная сумма платы периодически возвращается обратно пользователям.

При воплощении идеи о создании сообщества всемирных межбанковских финансовых телекоммуникаций ученые экономисты и практики исходили из соображения безопасности и контроля доступа к системе. Условия участия и членства в платежной системе, известные как «критерии доступа», служат для определения потенциальных членов системы.[27] Система СВИФТ соответствует современным требованиям, предъявляемым к уровню безопасности платежных систем.

8.2. Этапы вступления в члены международной платёжной системы СВИФТ

СВИФТ - это акционерное общество, владельцами которого являются банки-члены. Зарегистрировано общество в Бельгии (штаб-квартира и постоянно действующие органы находятся в г. Ла-Ульп (La Hulpe) недалеко от Брюсселя) и действует по бельгийским законам. Высший орган - общее собрание банков-членов либо их представителей (Генеральная ассамблея). Все решения

[27] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. С. 40.

принимаются большинством голосов участников ассамблеи согласно с принципом: одна акция - один голос. Главенствующее положение в совете директоров занимают представители банков стран Западной Европы и США.

Номинал акции составляет 125 ЕВРО. Реестр акционеров ведет сама компания СВИФТ. Акции СВИФТ нигде не торгуются, в связи с этим рыночные котировки отсутствуют. Число акций СВИФТ перераспределяется между акционерами пропорционально трафику передаваемых сообщений один раз в три года (соответственно, уставу СВИФТ). Наибольшее количество акций имеют США, Германия, Швейцария, Франция, Великобритания. Цена акции определяется каждый год по результатам общего собрания членов компании. Банк, которому выделяется дополнительное количество паев (акций), не имеет права отказаться от их оплаты.

Тарифы за трафик зависят от уровня потока сообщений, чем выше размер потока, тем меньше плата за трафик.

Членом СВИФТ может стать любой банк, имеющий согласно с национальным законодательством право на выполнение международных банковских операций. Наряду с банками-членами имеются и две иные категории пользователей сети СВИФТ - ассоциированные члены и участники. В качестве первых выступают филиалы и отделения банков-членов. Ассоциированные члены не являются акционерами и лишены права участия в управлении делами общества. Так называемые участники СВИФТ – все вероятные финансовые институты (не банки): брокерские и дилерские конторы, клиринговые и страховые компании, инвестиционные компании, получившие доступ к сети в 1987 г.

Вступление в СВИФТ состоит из 2-х основных этапов (стадий):

На *первом этапе* банк оформляет и передает в СВИФТ комплект документов, включающий: заявление о вступлении, обязательства банка проводить устав СВИФТ и возмещать затраты (операционные расходы) обществу, адрес банка и лица, ответст-

венные за связь с обществом, обзор трафика сообщений банка. Совет директоров СВИФТ рассматривает документы и принимает решение о приеме банка в общество. Банк-кандидат получает право на оплату единовременного взноса и приобретение одной акции общества. Вступление в СВИФТ стоит дорого: единовременный взнос составляет 400 000 бельгийских франков для банков-членов и 200 000 бельгийских франков для ассоциированных членов. Также, банки-члены должны приобрести одну акцию стоимостью в 55 000 бельгийских франков.

Второй этап непосредственно связан с физическим подключением банка к сети. Именно на этом этапе решаются все технические вопросы, приобретается коммуникационное оборудование (стоимость его может составлять сотни тысяч американских долларов), проводится обучение персонала. Даты подключения к сети фиксированные: это первые понедельники марта, июня, сентября и декабря. Как показывает практика, затраты банков на участие в системе СВИФТ (главным образом на установку современного электронного оборудования) окупаются обычно в течение 5 лет.

Вся *процедура вступления в СВИФТ* занимает не менее четырех месяцев и состоит из следующих этапов:

- ❖ Заполнение и отправка в СВИФТ вступительного заявления (СВИФТ Undertaking);
- ❖ Заполнение вступительных документов в электронной форме (контракт на программное обеспечение, формы заказа оборудования безопасности и так далее);
- ❖ Включение со стороны СВИФТ тестового режима (Test&Training);
- ❖ Включение со стороны СВИФТ режима BKE (обмен ключами с банками-корреспондентами);
- ❖ Отправка подтверждения готовности банка в СВИФТ (Readiness Confirmation).

В каждой стране, в которой развертывается система СВИФТ, общество создает, соответственно уставу СВИФТ, национальную

группу членов S.W.I.F.T. и группу пользователей S.W.I.F.T., объединяющую всех пользователей сети.

8.3. Общий порядок расчётов посредством международной платёжной системы СВИФТ, её преимущества и недостатки

Работа в сети СВИФТ дает пользователям ряд преимуществ.

1. Надежность передачи сообщений, что обеспечивается построением сети, специальным порядком передачи и приема сообщений за счет «горячего» резервирования каждого из элементов сети. Сеть гарантирует полную безопасность многоуровневой комбинацией физических, технических и организационных методов защиты, обеспечивает полную сохранность и секретность передаваемых сведений.

2. Сокращение операционных расходов по сравнению с телексной связью. Более того, с возрастанием трафика (размера) передаваемых сообщений снижается его стоимость.

3. Быстрый способ передачи сообщений в любую точку мира. Есть возможность непосредственного соединения с получателем, что сокращает время передачи сообщения. Время доставки сообщений обычно составляет около 20 минут, но его можно сократить до 1-5 минут за дополнительную плату. Аналогичная передача по телеграфу занимает около 90 минут. Поскольку все платежные документы поступают в систему в стандартизированном виде, то это разрешает автоматизировать обработку данных, исключить возможность различного понимания смысла сообщений отправителем и получателем, и повысить в естественном результате эффективность работы банка.

4. Фиксация осуществленных транзакций позволяет достигать полного контроля (аудита) всех проходящих распоряжений и каждый день до автоматизированного формирования отчета по ним.

5. Кроме этого, преодолеваются языковые барьеры и уменьшаются различия в практике проведения банковских операций.

6. СВИФТ гарантирует своим членам финансовую защиту, то есть если по вине общества в течение суток сообщение не достигло адресата, то СВИФТ берет на себя все прямые и косвенные расходы, которые понес клиент из-за этого опоздания.

Главным недостатком СВИФТ с точки зрения пользователей является дороговизна вступления. Расходы банка по вступлению в СВИФТ составляют 160-200 тысяч долларов. Это создает, естественно, проблемы для мелких и средних банков, однако уменьшить затраты разрешает коллективное подключение через Сервис-бюро либо другую финансовую организацию.

Систему СВИФТ должны были определять три важных фактора: стандартизация коммерческих процессов, система подключения банков к СВИФТ, создание международной сетевой модели и сетевой службы.

Основы этой системы до сих пор являются ключевыми в деятельности СВИФТ: общий язык и организация обработки информации через стандартные процессы, надежность и защита информации, быстрая передача сообщений, сокращение потерь и ошибок, более эффективное управление фондами, прямой контакт с клиентами и корреспондентами, расположенными далеко от банка, сокращение операционных расходов, доступность по всему миру в течение 24 часов.

Сегодня ее клиентами являются различные финансовые и кредитные учреждения, такие как всевозможные банки, брокерские фирмы, инвестиционные компании, биржи, международные депозитарии по операциям с ценными бумагами, расчетные клиринговые организации, пенсионные фонды и пр. Так как все большее число участников присоединялось к этой сети и расширялся международный бизнес, то новые технологические возможности и новые виды услуг увеличили способность и многосторонность системы.

В настоящее время СВИФТ объединяет 10 140 действующих финансово-кредитных организаций, находящихся в 212 странах мира. Несмотря на значительное расстояние между ними, они могут обмениваться сообщениями и взаимодействовать на протяжении круглого года в течение суток бесперебойно. Через данную сеть ее пользователями ежедневно передается до 20 миллионов (иногда и более) финансовых сообщений с суммарной оценочной стоимостью, составляющей около $6 трлн., около половины которых приходится на платежи. Более 2/3 всех СВИФТ-сообщений отправляется из Европы, Среднего Востока и Африки.

Универсальная стандартная форма идентификации банков, предложенная СВИФТ система идентификации банков посредствам BIC-кодов, предоставляется также и банкам, не вступившим в сообщество и не работающим в сети СВИФТ. Сообщения от банка к банку передаются путем авторизации немедленно со всеми необходимыми проверками и контролями, которые выполняются автоматически. Если отправитель и получатель сообщения работают в сети коммуникации одновременно, то доставка сообщения занимает не более 20 секунд. Передача может осуществляться по государственным линиям связи общего пользования или по специальным каналам.

Поскольку система СВИФТ является отлаженной и долголетней практикой международных расчетов, вступление банков Узбекистана в Сообщество всемирных межбанковских финансовых телекоммуникаций помогает наладить и дальше совершенствовать функционирование межбанковских расчетов и в Узбекистане.

Ключевые слова и понятия

SWIFT, основные направления деятельности СВИФТ, BIC, электронный платежный документ, банк-инициатор, банк-бенефициар, пользователь платежной системы, член платежной системы.

Вопросы для самопроверки

1. Понятие международной платёжной системы СВИФТ и её организация.

2. Этапы вступления в члены международной платёжной системы СВИФТ.

3. Преимущества и недостатки международной платёжной системы СВИФТ.

4. Взаимоотношения коммерческих банков Узбекистана с международной платёжной системой СВИФТ.

5. Функции банка – инициатора и банка – бенифициара.

6. Охарактеризуйте мировые электронные системы межбанковских операций (банковских сообщений и межбанковских расчетов).

ГЛАВА IX. СИСТЕМЫ НАЛИЧНЫХ ДЕНЕЖНЫХ ПЕРЕВОДОВ

9.1. Системы наличных денежных переводов и их основные виды

Денежный перевод - это платежный продукт, основанный на инструменте передачи кредита, и удаленно используется для перевода денег. Он часто используется там, где плательщик и/или получатель имеет текущий счет в финансовом учреждении. Он может использоваться как для внутренних, так и для иностранных валютных платежей.[28]

Дадим самую распространенную в экономической литературе характеристику системе денежных переводов. Разработавшая правила передачи и приема денежных средств, обеспечивающая передачу информаций и программных обеспечений с помощью электронных коммуникаций, а также обладающая лицензией Центробанка на осуществление переводов и имеющая свой логотип, вот эта организационная структура и называется системой денежных переводов. Система имеет службу сопровождения - программу, работающую с клиентами, а также свой клиринговый центр. Существуют несколько систем денежных переводов, по которым физические лица осуществляют данное действие. Самыми распространенными являются почтовые переводы и банковские системы денежных переводов, но без открытия счета.

В любой системе переводов, а их в мире достаточно много, деньги могут пересылаться только в пределах одной системы, то есть отправить денежные средства можно только в ту страну и в тот город, где есть агенты или представители системы. В Узбеки-

[28] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. С. 32.

стане деньги пересылаются только между банками, которые заключили соглашение с той или иной системой и выступают ее агентами. В других странах, в зависимости от законодательства, функции агента могут выполнять не только банки, но и другие организации, вплоть до магазинов.

При переводе денег за рубеж или внутри страны большинство переводов осуществляется только между физическими лицами, хотя некоторые системы переводов позволяют переводить деньги от физических лиц к юридическим и наоборот.

Средства в системах денежных переводов «транспортируются» в электронном (безналичном) виде по современным каналам передачи данных, что и обеспечивает высокую скорость перевода, но принимаются и выдаются в наличном виде. Стандартный срок, необходимый для того чтобы деньги попали в пункт назначения - от нескольких минут до одних суток.

Каждому, кто пользуется системой переводов, важно, чтобы деньги попали по адресу и не исчезли по пути. Для этого в каждой системе переводов предусмотрена своя надежная система безопасности, гарантирующая, что деньги будут выплачены только указанному отправителем лицу.

На сегодняшний день в Узбекистане действуют более десятка систем международных денежных переводов, из которых наиболее известны: Western Union, MoneyGram, Анелик, Contact, X-press Money, Быстрая почта, Migom, Unistream, Coinstar, Blizko, Азия Экспресс, Золотая Корона и другие.

Кроме того, услуги денежных переводов с одного города Узбекистана в другой предоставляет ОАО «Узбекистон почтаси».

Дадим краткое описание некоторым из них:

Western Union *(Вестерн Юнион)* – это распространенная и самая крупная международная система переводов. Вестерн Юнион функционирует более ста пятидесяти лет (начиная с 1851 г.) на рынке денежных переводов и главным его организатором считается Американская Компания Western Union. Вестерн Юнион, это

глобальная сеть, которая насчитывает более четырехсот пунктов обслуживания почти в двухстах странах мира.

Переводы осуществляются без зачисления на счет денежных средств и открытия банковского счета, а сумма при переводе выплачивается наличными средствами, в зависимости от страны, в которую прибыл перевод. Размер комиссионного вознаграждения от суммы перевода удерживается только с отправителя. От направления перевода различаются следующие виды тарифов: в ближнее зарубежье, в дальнее зарубежье и по территории Узбекистана.

В мировой практике неоднократно осуществляющиеся денежные переводы проводятся по программе лояльности золотых карт Вестерн Юнион (Western Union Gold Card). Система переводов денежных средств запустила ее с начала второй половины 2008 года и с тех пор такая система лояльности основана на внедрении специальных карт и действует уже в шестидесяти пяти странах мира. Она идентифицирует по базе данных постоянных клиентов и позволяет сократить время обработки переводов. Золотая карта Вестерн Юнион - это программа лояльности, которая направлена на начисление бонусов и поощрение постоянных клиентов.

«MoneyGram» (Маниграмм) – это система международных денежных переводов, реализованная американской компанией (MoneyGram International Limited). Она отделилась от Вестерн Юнион и расположилась в Миннеаполисе. Ее связывает сеть, состоящая из почти 200 тысяч агентов в различных регионах мира, включая страны СНГ, где насчитывается более семи тысяч пунктов обслуживания.

В Европе партнерами «Маниграмм» стали такие крупные финансовые структуры, как Почта Норвегии, Великобритании и т.д. Переводы осуществляются в долларах, евро и местной валюте, без открытия банковского счета, и комиссия за перевод, зависит от суммы и страны, и составляет от трех и до пяти процентов.

Юнистрим – система, работающая по всему миру, обеспечивает систему срочных международных денежных переводов. Оператором Юнистрим является ОАО КБ «ЮНИСТРИМ», как департамент Юниаструм Банка он начал свое функционирование в начале 2000 года, а уже в самостоятельный банк, был преобразован в две тысячи пятом году. Система охватывает больше ста тысяч пунктов обслуживания в девяноста странах мира и контролирует свыше трех процентов рынка СНГ. Данная система денежных переводов имеет разветвленную сеть пунктов по Казахстану, Украине, Молдове, Таджикистану и России, а также и собственные сети в Великобритании и на Кипре.

Юнистрим впервые стал обладать существенным достоинством в России и предоставлять услугу под названием «денежные переводы с помощью сотового телефона», с помощью которой абоненты Билайна, могут получить наличные денежные средства в собственных пунктах обслуживания со счета своего сотового телефона. Получение средств осуществляется только в рублях, т.к. это пока еще дорогая услуга, комиссия составляет пять процентов. Наименьшая сумма одной операции не должна превышать одной тысячи рублей, а наивысшая - тридцати тысяч рублей. В системе Юнистрим, установлены лимиты на количество операций.

BLIZKO - платежная стстема, позволяющая быстро, надежно и удобно осуществить перевод денежных средств по доступным тарифам.

Оператором платежной системы BLIZKO является ПАО АКБ «Связь-Банк». На сегодняшний день платежная система обладает сетью пунктов обслуживания клиентов, насчитывающей более 36 000 отделений в России, странах ближнего и дальнего зарубежья. В России услугами BLIZKO можно воспользоваться не только в банковских офисах, но и в отделениях почтовой связи. Денежные переводы BLIZKO можно осуществлять в 3 валютах: российских рублях (RUR), долларах США (USD) и евро (EUR). Существуют ограничения на отправку денежных средств: на территории России денежные переводы между гражданами России осуществляются

только в рублях РФ. Граждане России могут перевести за пределы России иностранную валюту и рубли в пользу гражданина России в размере не более эквивалента 5000 USD за один день, а в пользу иностранного гражданина без ограничений по сумме.

Рассмотрим приведенные в табл. 3 тарифы на отправку денежных переводов в страны СНГ по некоторым, наиболее популярным видам систем денежных переводов.

Таблица 3

Тарифы на отправку денежных переводов в страны СНГ (срочные) в долл. США на 31.12.2017 г.[29]

Сумма перевода	Western Union	Сумма перевода	MoneyGram	Сумма перевода	BLIZKO
0,01-200,00	3$	1-100	2	до 100,0	2
		100,01-200	4	100,01-200,0	4
		200,01-300	6	200,01-300,0	6
		300,01-400	8	300,01-400,0	8
		400,01-500	10	400,01-500,0	10
200,01-2000,0	1,7% от суммы перевода	500,01-600	12	500,01-600,0	12
		600,01-700	14	600,01-700,0	14
		700,01-800	16	700,01-800,0	16
		800,01-900	18	800,01-900,0	18
				900,01-1000,0	20
2000,01-3000,0	1,3% от суммы перевода	900,01-1000	20	1000,01-1250,0	25
				1250,01-1500,0	30

[29] по данным сайта www.bank.uz

		1000,01-2000	35	1500,01-1750,0	35
				1750,01-2000,0	40
		2000,01-3000	50	2000,01-2500,0	50
				2500,01-3000,0	60
3000,01-5000,0	1,0% от суммы перевода	3000,01-4000	70	3000,01-3500,0	70
				3500,01-4000,0	80
		4000,01-5000	100	4000,01-4500,0	90
				4500,01-5000,0	100

Как видно, несмотря на единство цели, условия и требования рассмотренных систем денежных переводов отличаются. Из-за этого у клиента возникает вопрос выбора наиболее оптимального варианта перевода. Прежде чем сделать свой выбор денежного перевода, необходимо совместить следующие требования, такие как: географию предоставления услуг и скорость, валюту перевода, а также качество, цену оказываемой услуги.

9.2. Другие виды денежных переводов и их особенности

Анелик *(Anelik)* — российская система денежных переводов физических лиц без открытия банковского счета. Основана в 1996 году. Является одним из лидеров на рынке российских международных денежных переводов. Центральный офис находится в г. Москве. Консолидирующим центром системы «Анелик» (Anelik ®) является коммерческий банк «Анелик РУ» (ООО). Банк занимается всеми видами банковской деятельности на территории Российской Федерации, но основным направлением в его деятель-

ности считается перевод денег физических лиц своим родным и близким, осуществляемый без открытия счетов. Банк выступает в качестве клирингового центра. Система Anelik ® объединяет 63 000 пунктов в более чем 90 странах мира. Участниками системы являются более 100 банков в этих странах. Переводы по системе Анелик осуществляют такие банки как: Московский индустриальный банк, Инвестсбербанк, Русский Банк Развития, ОАО «Банк Уралсиб», ЗАО «ВТБ 24», ЗАО КБ «Глобэкс», ЗАО АКБ «Промсвязьбанк», ОАО КБ «Мастер-Банк», ЗАО «Русь-банк», ОАО КБ «Петрокоммерц» и др.

Контакт *(Contact)* – это система международных денежных переводов между физическими лицами, по всему миру (СНГ, Россия, Балтия и страны дальнего зарубежья), без открытия счета в банке. Клиринговым центром и организатором системы, является образованная в 90-ых годах система АКБ «РУССЛАВБАНК», обладающая генеральной лицензией, выданной Российским Банком. В двухтысячном году в России заработала система платежей и денежных переводов Контакт, а уже в 2005 году система начала активно осуществлять денежные переводы в страны СНГ.

Контакт, располагает более тридцати тысячами пунктов в восьмидесяти четырех странах мира и тремя тысячами пунктов обслуживания в России. Осуществление денежных переводов возможно как в долларах, евро, так и в российских рублях. Денежная система переводов, позволяет осуществлять, как отправление переводов наличными, с карточного и банковского счета, так и получение переводов в безналичной форме, зачисляя деньги на банковский счет, или выплатой чеком. При этом комиссия за перевод варьируется в пределах ноль целых, семь десятых и до пяти процентов от суммы перевода. Система Контакт в конце 2009 года внедрила по всему миру смс - информирования клиентов. В России денежная система переводов Контакт работает с Банком «Возрождение», с Банком ГЛОБЭКС, Омск - банком и др.

Аллюр – это система денежных переводов, которая первоначально была ориентированна на внутренний российский рынок, и

только потом стала функционировать в странах СНГ. Процессинговым центром системы переводов физических лиц, также организатором, без открытия банковского счета является закрытое акционерное общество КОКК (Компания объединенных кредитных карточек). Система составляет более пяти тысяч офисов, а также шестьсот кредитных организаций, расположенных на территории России в более чем трёхстах населенных пунктах. В рублях сумма перевода ограничена до шестисот тысяч рублей, а в зарубежной валюте - до пятнадцати тысяч долларов и евро, а также для резидентов Российской Федерации с учетом ограничений - не более пяти тысяч долларов в один операционный день. Только в системе Аллюр, действуют денежные переводы по единым фиксированным тарифам, и его размер зависит от валюты и суммы перевода.

Лидер - международная российская система денежных переводов, обслуживающаяся у НКО ЗАО «ЛИДЕР». Учредителем и расчетным центром является общество с ограниченной ответственностью КБ «ИНКРЕДБАНК», со ста процентами акций. С две тысячи третьего года система Лидер начала свою деятельность и на сегодняшний день охватывает двадцать пять стран мира, более семи тысяч пунктов приема и отправки денежных средств.

В зависимости от страны и валюты перевода, тарифы на денежные переводы Лидер изменяются от одного процента и до четырех процентов от суммы. В зависимости от выбора банка в отдельных странах стоит уточнять тарифный план, так как их может существовать несколько. Уточнив у оператора возможность зачисления денежных средств на банковский счет, клиенты системы Лидер, в соответствии с законодательством страны, могут воспользоваться данной возможностью. Система Лидер для перевода денежных средств, взаимодействует с такими банками, как ОАО ВИП-БАНК, ЗАО КБ Мираф-банк, Азия УниверсамБанк, Банк Индустриальный Кредит и др.

Золотая Корона - международная российская уникальная, динамично развивающаяся и пользующаяся большой популярностью у клиентов - современная денежная система переводов, ос-

нованная для физических лиц. Она начала свое функционирование в 2003 году и была разработана ЦФТ (Центром финансовых технологий), а уже в две тысячи седьмом году система внедрила новую технологию в промышленную эксплуатацию по оформлению отправки переводов через кассовые устройства. Карта денежных переводов оформляется один раз и хранит (как об отправителе, так и о получателе переводов), информацию о хозяине.

Золотая Корона охватывает сеть пунктов республик бывшего союза, также система объединяет сто восемьдесят банков, и количество пунктов из двадцати шести тысяч, которые по сей день продолжают свой рост. Система сотрудничает с ООО «Московским областным банком», ОАО «УРАЛСИБ» и др. Полтора процента составляет стоимость по России от суммы перевода, в страны СНГ- от полутора до трех процентов, а в Китай - независимо от переводимой суммы - двадцать пять долларов. По России, максимальная сумма составляет пятьсот тысяч рублей, за рубежом, для резидентов Российской Федерации - до пяти тысяч долларов, для нерезидентов - до двадцати тысяч долларов. Центр финансовых технологий активно внедряет проекты интеграции с другими денежными системами переводов, к примеру с системами «Анелик», «Аверс», «Маниграмм» и т.д.

Ключевые слова и понятия

Денежный перевод, учредитель системы денежных переводов, условия денежных переводов, скорость перевода, сфера применения, основные виды переводов для ближнего и дальнего зарубежья.

Вопросы для самопроверки

1. Системы наличных денежных переводов и их виды.
2. Денежный перевод Western Union, его преимущества и условия.

3. Порядок перевода наличных денег посредством системы MoneyGram.

4. Порядок перевода наличных денег посредством системы Anelik.

5. Особенности системы перевода наличных денег Контакт.

6. Другие виды денежных переводов и их особенности.

7. Назовите учредителей (организаторов) и страны, в которых были созданы международные системы денежных переводов.

ГЛАВА X. ЦЕЛЬ И ЗАДАЧИ БАНКОВСКОЙ БЕЗОПАСНОСТИ

10.1. Понятие и содержание безопасности

Анализ истории свидетельствует, что потребность обеспечения безопасности относится к числу основных мотивов деятельности людей и сообществ. Стремление к безопасности обусловило объединение наших предков в сообщества, формирование силовых структур, предопределило образование многих специфических органов.

До недавнего времени безопасность являлась монопольной сферой высшего политического руководства, в значительной степени закрытой для широкой общественности. Это обусловило низкий уровень разработки самого понятия "безопасность", которое в течение длительного времени касалось в основном военных аспектов. Но времена меняются, меняется и само понятие безопасности.

Рассмотрим основные определения банковской безопасности:

1. Большая часть авторов под безопасностью понимают состояние потенциальной жертвы.

2. Безопасность весьма часто рассматривается как способность объекта сохранить свою сущность и основную характеристику в условиях целенаправленного, разрушающего воздействия извне или в самом объекте.

3. Безопасность - категория системная, она - свойство системы, построенная на принципах устойчивости, саморегуляции, целостности. Безопасность призвана защитить каждое из этих свойств системы.

4. Безопасность рассматривается как решающее условие жизнедеятельности человека, общества, что позволяет им сохранять и умножать их материальные ценности.

5. Безопасность в абсолютном своем выражении - отсуствие опасностей и угроз материальной и духовной сферы.

6. Безопасность – это гарантированная законадательными и практическими мерами защищенность жизненно важных интересов.[30]

Состояние защищенности личности, общества, государства, состояние защищенности жизненных интересов, состояние защищенности национальных интересов, устойчивое состояние системы по отношению к неблагоприятным воздействиям и т.д. составляет предмет безопасности.

Задача безопасности заключается, прежде всего, в формировании условий, обеспечивающих стабильное, прогрессирующее развитие общественных отношений, сохранение, укрепление и обогащение бытия, т.е. защищенности качественного состояния общественных отношений, обеспечивающих прогрессирующее развитие личности, общества, государства.

Концептуальная модель безопасности банка включает в себя концепцию безопасности, понятие безопасности, обеспечение безопасности, систему безопасности.

- Концепция безопасности банка представляет собой научно обоснованную систему взглядов на определение основных направлений, условий и порядка практического решения задач защиты банка от противоправных действий и недобросовестной конкуренции.
- Под безопасностью банка понимается состояние защищенности интересов владельцев, руководства и клиентов банка, материальных ценностей и информационных ресурсов от внутренних и внешних угроз.
- Обеспечение безопасности является неотъемлемой составной частью деятельности банка. Состояние защищенности

[30] Ярочкин В.И. Безопасность банковских систем. М.: Ось-89, 2004. С.7.

представляет собой умение и способность надежно противостоять любым попыткам криминальных структур или недобросовестных конкурентов нанести ущерб законным и интересам банка.

➢ Система безопасности включает в себя: органы, силы и средства; цели и задачи; структуру, формы и методы; направления безопасности.

10.2. Цель и задачи системы безопасности

Главной целью системы безопасности является обеспечение устойчивого функционирования банка и предотвращение угроз его безопасности, защита законных интересов от противоправных посягательств, охрана жизни и здоровья персонала, недопущение хищения финансовых и материально-технических средств, уничтожения имущества и ценностей, разглашения, утечки и несанкционированного доступа к служебной информации, нарушения работы технических средств обеспечения производственной деятельности, включая и средства информатизации.

Задачи системы безопасности:

❖ прогнозирование и своевременное выявление и устранение угроз безопасности;

❖ отнесение информации к категории ограниченного доступа, а других ресурсов – к различным уровням опасности и подлежащих сохранению;

❖ создание механизма и условий оперативного реагирования на угрозы безопасности и проявление негативных тенденций в функционировании банка;

❖ эффективное пресечение угроз персоналу и посягательств на ресурсы на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;

❖ создание условий для максимального возможного возмещения и локализации наносимого ущерба неправомерными

действиями, ослабление негативного влияния последствий нарушения безопасности банка.

Принципы организации и функционирования системы безопасности:

- ✓ комплексность;
- ✓ своевременность;
- ✓ непрерывность;
- ✓ активность;
- ✓ законность;
- ✓ обоснованность;
- ✓ экономичность;
- ✓ специализация;
- ✓ взаимодействия и координация;
- ✓ Совершенствование;
- ✓ централизация управления.

Общая модель комплексной безопасности банка включает в себя три основные «ветви»: функции, объекты и направления безопасности.

Ключевые слова и понятия

Безопасность, безопасность информационная, безопасность национальная, безопасность банковская, «бомба» компьютерной программы, аудит банковской безопасности, объект безопасности, принципы системы безопасности.

Вопросы для самопроверки

1. Понятие, содержание и сущность безопасности.
2. Концепция безопасности.
3. Цель и задачи системы безопасности.
4. Принципы организации и функционирования системы безопасности.
5. Функции, объекты и направления безопасности.
6. Основные определения банковской безопасности.
7. Инженерно- технические основы безопасности.

ГЛАВА XI. ВИДЫ УГРОЗ, ВЛИЯЮЩИХ НА БАНКОВСКУЮ БЕЗОПАСНОСТЬ

11.1. Виды угроз и их классификация

Опасности и угрозы – это потенциально возможные или реальные действия злоумышленников, способные нанести моральный или материальный ущерб. Угрозы бывают внешние и внутренние, которые, в свою очередь, могут наносить ущерб персоналу, материальным ресурсам, финансам и информации.

«Опасность» можно охарактеризовать как наличие и действие сил (факторов), которые являются деструктивными и дестабилизирующими по отношению к какой-либо конкретной системе (банку).

Деструктивными и дестабилизирующими следует считать те силы (факторы), которые способны нанести ущерб данной системе, временно вывести её из строя или полностью уничтожить.

Предотвращение опасностей в банковской деятельности предполагает своевременное их прогнозирование и принятие необходимых мер, прежде всего:

- постоянное добывание, сбор, анализ информации;
- оценка обстановки;
- выработка и принятие решения;
- осуществление упреждающих действий;
- удержание инициативы в своих руках;
- создание резервов и т.д.

Главная цель безопасности банковской деятельности - обеспечение устойчивого функционирования банка и предотвращение внутренних и внешних угроз. Целями безопасности банка являются также защита его законных

интересов от противоправных посягательств, безопасность и охрана здоровья персонала, недопущение хищения финансовых и материальных средств, порчи и уничтожение имущества, ценностей; недопущение разглашения коммерческой тайны, утечки и несанкционированного доступа к служебной информации, нарушения работы технических средств, обеспечивающих банковскую деятельность.

Классификация источников угроз банковской деятельности :

- ❖ природные (редкое явление);
- ❖ технические (связанные с техникой);
- ❖ социальные (общество-человек).

Следует обратить внимание, что именно социальные угрозы наиболее опасные.

В процессе выявления, анализа и прогнозирования потенциальных угроз интересам банка в рамках безопасности учитываются объективно существующие внешние и внутренние условия, влияющие на банковскую систему в целом.

Таковыми являются:

- ➢ нестабильная политическая, социально-экономическая обстановка, обострение криминогенной ситуации, криминальная конкуренция и т.д.;
- ➢ невыполнение законодательных актов, правовой нигилизм, отсутствие некоторых законов по жизненно важным вопросам;
- ➢ снижение моральной, психологической, производственной ответственности работников банка и т.д.

Виды угроз безопасности банковской деятельности можно разделить на две группы.

Внутренние угрозы – это источники, порождаемые внутренними противоречиями или иными факторами, которые могут исходить непосредственно от коллектива, групп людей и отдельных личностей, наделенных определенными полномочиями при выполнении своих обязанностей в данном учреждении.

Внешние угрозы – это источники, которые существуют или могут появляться за рамками организации, в частности, банка и воздействовать на его интересы извне. Основу внешних угроз, как правило, составляют социальные источники опасности (люди), а также и природные. Классификация потенциальных угроз безопасности банков возможна также по другому признаку:

Первая группа - *физические угрозы.*

Вторая группа – *технические угрозы.*

Третья группа – *интеллектуальные угрозы.*

Внутренние угрозы для банка проявляются также в злоупотреблениях при выполнении расчетных, кассовых, валютных и кредитных операций. Кредитные операции имеют наибольшую опасность, так как они составляют основную часть банковских активов. Поэтому в период банковских кризисов возрастают риски при проведении именно кредитных операций. Не случайно поэтому американские ученые экономисты Кармен М. Рейнхарт и Кеннет С. Рогофф первопричинами происхождения банковских кризисов считали кредитные кризисы и образование так называемых пузырей (пены), связанных с ценой активов.[31] В этой связи изучение и прогнозирование банковских, в том числе кредитных рисков имеет важное значение в снижении потенциальных угроз для коммерческого банка.

11.2. Угрозы преступного характера

Угрозы преступного характера или просто преступление – это общественно опасное деяние, посягающее на личность, общество и государство, а также на иные охраняемые законом объекты.

Виды преступлений экономической неправильности:

- Хищение финансовых и материальных средств;
- Мошенничество в сфере финансовой деятельности;
- Незаконные сделки с валютными ценностями;

[31] Reinhart, Carmen M, and Kenneth S. Rogoff. 2009. The aftermath of financial crises. American Economic Review 99, No. 2. C. 466.

- Изготовление поддельных денег;
- Должностные преступления;
- Взяточничество;
- Скрытие доходов;
- Обман потребителей;
- Продажа товаров, не отвечающих требованиям безопасности;
- Контрабанда.

Процесс совершения криминального акта можно разделить на 3 этапа:

➢ *Первый* – подготовительный, заключается в сборе возможно более полной информации о наиболее уязвимых местах проникновения на объект, местах хранения ценностей, режиме работы банк, схеме функционирования и организации охраны, принципах действия охранной сигнализации и методах ее деблокирования.

➢ *Второй* – непосредственно криминальная акция, ее подготовка и совершение.

➢ *Третий* – уход с места преступления, сокрытие следов и уничтожение улик.

Преступления могут совершаться с использованием физических, технических и интеллектуальных угроз, о которых говорилось выше.

Физические угрозы – это как воздействие физических лиц, совершающих противоправные действия методом физического насилия, а также и природные, техногенные катастрофы.

К физическим угрозам относятся:

❖ похищения и угрозы похищения сотрудников банка, членов их семей и близких родственников;

❖ убийства, сопровождаемые насилием;

❖ разбойные нападения с целью завладения денежными средствами, ценностями и документами;

❖ уничтожение собственности банка и собственности банковских работников;

❖ террористические акции, т.е. совершение преступления в форме взрыва, поджога, применения или угрозы применения взрывных устройств, химических, биологических, токсических веществ, а также захват заложников, транспортных средств и т.д.;

❖ чрезвычайные обстоятельства – это события, вызванные аварией и приведшие на определенной территории к угрозе жизни и здоровью людей, ущербу государственным, коммерческим и иным видам собственности, личному имуществу граждан и природной среде.

Технические угрозы - это совокупность мероприятий и технических средств, направленных на получение нужной информации, а также на нарушение, нейтрализацию аппаратных средств и программного обеспечения интересующего объекта (банка), *к ним относятся:*

- перехват информации;
- радиоразведка связи и управления;
- искажение информации;
- ввод ложной информации;
- информационное нападение;
- уничтожение информации и т.д.

Цель - перехватить, исказить, уничтожить информацию.

Интеллектуальные угрозы - это угрозы, направленные на продукт интеллектуального труда, умственные способности индивида.

Различают ещё так называемые «беловоротничковые угрозы (преступления)». «Белые воротнички» - представители административно-бюрократического аппарата всех сфер управления.

«Беловоротничковые угрозы» - это когда предприниматели, государственные служащие, банкиры и другие представители административного аппарата, обладают возможностью по характеру предоставляемых им полномочий совершать такие экономические преступления, как: нарушение антитрестовского законодательства; мошенничества с ценными бумагами, на

фондовой бирже, с получением кредитов и ссуд; присвоением банковских средств, уклонение от уплаты налогов, взяточничество.

«Золотые воротнички» - новая категория персонала, обладающая высокой компьютерной грамотностью: программисты управляемых производственных комплексов, операторы роботизированных систем, специалисты по сверхновым материалам и т.д. Угрозы психического воздействия можно рассмотреть на двух примерах. Первый - *психическое нападение* - это отрицательные различные психофизиологические состояния, рассматриваемые пострадавшими, как «наведение извне», как исходящий от другого человека, с которым «пострадавший» в момент нападения находился в непосредственном контакте.

Второй - *психическое насилие* - насилие, выражающееся в демонстрации оружия и готовности его применения; на вербальном уровне (словесном) в угрозе нанести побои, связать, лишить свободы передвижения, убить или совершить насилие в отношении близких и родственников жертвы.

Преступления с использованием пластиковых платежных средств:

- операции с поддельными картами;
- операции с украденными/поддельными картами;
- многократная оплата услуг и товаров;
- мошенничество с почтовыми/телефонными заказами;
- многократное снятие со счета;
- мошенничество с использованием подложных слипов;
- использование для выдачи наличных денег через банкомат;
- подключение электронного записывающего устройства к POS – терминалу/банкомату, Скимминг (Skimming) и другие виды мошенничества.

Основные способы подделки пластиковой карты:

✓ изменение информации на магнитном носителе;

✓ изменение информации эмбоссированной на лицевой стороне;

- ✓ их сочетание;
- ✓ подделка подписи законного владельца и т.д.

Многообразие важных угроз преступного характера повышает роль своевременного предотвращения и анализа потенциальных угроз банковской безопастности.

Ключевые слова и понятия

Скимминг, антивирус, аппаратные средства защиты, атака, злоумышленник, промышленный шпионаж, психологический портрет мошенника, внутренние угрозы, внешние угрозы, классификация угроз по объектам.

Вопросы для самопроверки

1. Виды опасностей и угроз, их классификация.
2. Угрозы преступного характера.
3. Компьютерные преступления.
4. Предотвращение незаконных банковских операций.
5. Модель действия злоумышленников.
6. Мошенничество и его виды.
7. Промышленный шпионаж и недобросовестная конкуренция.

ГЛАВА XII. ОБЪЕКТЫ БАНКОВСКОЙ БЕЗОПАСНОСТИ

12.1. Персонал как объект безопасности банка

Обеспечение безопасности персонала коммерческого банка заключается в проведении следующих мероприятий:

✓ организация охраны (личной и средств передвижения, при необходимости - квартир, дач, гаражей);

✓ обеспечение персонала средствами личной безопасности, в необходимых случаях и средствами обороны (оружие, устройства противодействия, средства вызова помощи);

✓ подготовка сотрудников к действиям в экстремальных ситуациях (выработка навыков оценки опасности, адекватного поведения и готовности к отражению угроз);

✓ обучение сотрудников и членов их семей выявлению признаков, указывающих на возможную подготовку против них нежелательных действий;

✓ выработка практических форм взаимодействия с правоохранительными органами по обеспечению безопасности персонала при внешних и внутренних угрозах.

Личную безопасность могут обеспечить личные охранники, обладающие наряду с высокими моральными качествами умением владеть собой в критических ситуациях, способностью быстро и решительно действовать в любой обстановке. Они должны быть хорошо развиты физически, психологически совместимы с охраняемым лицом и членами его семьи и профессионально подготовлены к этой работе.

Действия персонала при нападении на банк также регламентируются. Во время нападения сотрудники должны оставаться совершенно спокойными и не предпринимать никаких

действий, провоцирующих преступников на опасные для жизни действия. Требования бандитов должны быть выполнены безоговорочно. Сотрудники банка должны сконцетрировать свое внимание на запоминании внешности грабителей, их действий и хода развивающихся событий с целью последующей идентификации преступников после нападения на банк . Кнопку тревоги о нападении нажать, только если нет опасности. После нападения сотрудники должны сохранить любые следы преступных действий и подготовить описание преступников по прилагаемым формам.

По характеру, виду и содержанию психологические воздействия классифицируются на:

- информационно-психологические;
- психотронные;
- техно-психологические;
- соматопсихологические;
- психотропные.

Опасность персоналу может быть не только внешняя, но и внутренняя. Внутренним злоумышленником может быть любой сотрудник банка, вступивший в сговор с преступной группой.

Внутренний злоумышленник может быть враждебно настроенный служащий, психически неуравновешенные люди или служащие, подвергающиеся шантажу или угрозам со стороны преступников. Внутренний злоумышленник может быть служащий банка или сотрудник охраны, имеющий доступ на объект, располагающий определенной информацией о режиме работы банка и, возможно, системе охраны. Мотивом преступления является, как правило, личное обогащение, но могут быть и другие: месть начальству или сотруднику, психическое расстройство и т.д. Методы активного воздействия – подкуп, шантаж, жесткая угроза, физическое и психологическое воздействие, специфический форсированный допрос, игра на эмоциях, убеждение, фармакологическое воздействие и т.д.

При этом к группам риска могут быть отнесены:

- ❖ секретари, личные помощники;
- ❖ водители руководителей;
- ❖ системные администраторы и технические специалисты;
- ❖ сотрудники охраны и службы безопасности;
- ❖ технический персонал (курьеры, уборщики).

Внутренняя защита банка – это комплекс мероприятий, действий, исключающих нанесение внутреннего ущерба банковской деятельности.

12.2. Финансовые и материальные средства как объект банковской безопасности

Безопасность финансовых и материальных ресурсов подразумевает предупреждение несанкционированного проникновения злоумышленников в помещения, хранилища и на территорию банка. Охране подлежат все финансовые и материальные ценности банка незаваисимо от их местонахождения. Однако возможно выделение объектов наибольшей важности: денежные хранилища, кассовые залы, инкассаторские пункты и автомобили, банкоматы и другие. Угрозы, источники угроз и объекты криминального характера, а также меры, направления и объекты защиты составляют концептуальную модель безопасности материальных ценностей. Модель безопасности материальных ценностей показана на рис. 13.

Инженерно–технические основы безопасности финансовых и материальных средств также имеют большое значение. Они включают использование различных технических средств и систем. На практике все мероприятия по использованию технических средств подразделяются на три группы:

• *Организационные мероприятия* – это мероприятия ограничительного характера, сводящиеся к регламентаци доступа и использования технических средств обработки информации.

• *Технические мероприятия* – это приобретение, установка и использование защищенных от электромагнитных и акустических воздействий технических средств обработки информации.

Организационно–технические мероприятия обеспечивают блокирование возможных каналов утечки информации через технические средства с помощью специальных устройств, устанавливаемых на элементы конструкций зданий, помещений и технических средств обработки информации.

Рис. 13. **Концептуальная модель безопасности материальных ценностей**[32]

[32] Ярочкин В.И. Безопасность банковских систем. М.: Ось-89, 2004.С.94.

12.3. Информация как объект банковской безопасности

Информация бывает как документированная (документ), так и в виде информационных ресурсов – отддельные документы, отдельные массивы документов, документы и массивы документов в информационных системах.

В свою очередь информация бывает *открытой и ограниченного использования*. Последняя подразделяется на *государственную тайну* и на *конфиденциальную информацию*. Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством.

Технические угрозы безопасности информации - это совокупность мероприятий и технических средств, направленных на получение нужной информации, а также на нарушение, нейтрализацию аппаратных средств и программного обеспечения интересующего объекта (банка). К ним относятся:

- перехват информации;
- радиоразведка связи и управления;
- искажение информации;
- ввод ложной информации;
- информационное нападение;
- уничтожение информации и т.д.

Основная цель таких действий – перехватить, исказить, уничтожить информацию. Преступные покушения на компьютерные и телекоммуникационные системы с целью их вывода из строя реализуются по сетям питания, по проводным линиям, по эфиру.

Основные способы несанкционированного доступа:

1. Использование инсайдеров. Инсайдер – лицо, имеющее в силу своего служебного или семейного положения доступ к конфиденциальной информации о делах банка (компании).

2. Инициативное сотрудничество – отношения между сотрудничающими сторонами, строящиеся на определенных действиях лиц, готовых на любые противоправные действия.

3. Подслушивание: перехват или запись данных, передаваемых по техническим средствам связи; несанкционированный перехват данных при их передаче.

4. Наблюдение, копирование, хищение, перехват, ознакомление, подключение, подделка.

5. Выпытывание: стремление под видом невинных вопросов получить определенные сведения; техника получения информации посредством пыточного воздействия.

6. Склонение к сотрудничеству – как правило, насильственное действие со стороны вербующей стороны, осуществляемое путем подкупа, запугивания, шантажа.

Одной из причин преступных покушений на компьютерные и телекоммуникационные системы является их уязвимость за счет широкого распространения глобальных открытых компьютерных сетей типа Интернет, построенных на основе телекоммуникационных магистралей общего пользования, а также из-за возможности применения средств вычислительной техники с программным обеспечением, позволяющим легко модифицировать, уничтожать или копировать обрабатываемую информацию.

Требования к защите информации в информационно–телекоммуникационной системе банка:

- защита информации при передаче ее по каналам связи, хранении и обработке (конфиденциальность информации);
- обеспечение целостности и подлинности передаваемой, хранимой и обрабатываемой информации;
- аутентификация сторон, устанавливающих связь (подтверждение подлинности отправителя или получателя информации);
- контроль доступа к ресурсам сети, оборудованию и данным абонентов;

➢ криптоживучесть при компрометации части ключевой системы;

➢ возможность доказательства неправомочности действий пользователей и обслуживающего персонала в сети;

➢ обеспечение взаимодействия между различными локальными информационными системами при одновременном исключении возможности «сквозного» проникновения к наиболее важным подсистемам, в которых циркулирует подлежащая защите информация.

При использовании новых банковских технологий в мировой практике при создании международных платежных систем большое внимание уделяется безопасности транзакций. В платежных, клиринговых и расчетных системах участники сталкиваются с риском того, что расчет в системе не будет осуществлен. Эти риски могут привести к системному риску, если проблемы в рамках одного финансового учреждения распространяются на других. Поэтому при разработке новых банковских продуктов с использованием высокотехнологичных Интернет-технологий большое внимание уделяется разработке ключевых концепций, касающихся рисков, относящихся к обработке платежей и операций, связанных с финансовыми инструментами, а также способов смягчения таких рисков.[33]

Очевидно, что общая концептуальная модель объекта безопасности должна содержать, с одной стороны, опасности и угрозы, а с другой- мероприятия по обеспечению безопасности.

Ключевые слова и понятия

Аутентификация информации, дезинформация, «белые воротнички», «беловоротничковые угрозы», «золотые воротнички», психическое нападение, психическое насилие, информационно-психологическое воздействие.

---

[33] The payment system. Payments, securities and derivatives, and the role of the eurosystem / Editor Том Kokkola. Frankfurt am Main Germany: European Central Bank, 2010. С. 115.

Вопросы для самопроверки

1. Мероприятия по обеспечению безопасности персонала банка.
2. Финансовые и материальные средства как объект банковской безопасности.
3. Информация как объект банковской безопасности.
4. Возможные сценарии преступных действий.
5. Концептуальная модель безопасности личности.
6. Действия персонала в экстремальных ситуациях.
7. Классификация психологических воздействий.

ГЛАВА XIII. ПРАВОВЫЕ ОСНОВЫ БАНКОВСКОЙ БЕЗОПАСНОСТИ

13.1. Законодательные основы банковской безопасности

Банки подвергаются риску, как всякое предприятие, но в силу особенностей своей деятельности и особой важности некоторых свойств эксплуатации (широкое применение информатики) они особенно чувствительны к проблемам безопасности. Поэтому необходима концепция информационной безопасности Центрального банка. Данная концепция разработана на основе «Концепции национальной безопасности Республики Узбекистан», принятой 29 августа 1997 года постановлением Олий Мажлиса Республики Узбекистан № 467-1, которая послужила методологической базой для:

- разработки стратегии обеспечения информационной безопасности Центрального банка, включающей в себя цели, задачи и комплекс основных мер по ее практической реализации;
- формирования и проведения политики Центрального банка Республики Узбекистан в области обеспечения информационной безопасности;
- подготовки предложений по совершенствованию организационного, технического и нормативно-методического обеспечения информационной безопасности Центрального банка Республики Узбекистан.

Концепция представляет собой изложение целей и задач обеспечения информационной безопасности, и основывается на следующих принипах:

1. Правовая обеспеченность политики в области информационной безопасности;

2. Программно-техническая обеспеченность;

3. Кадровая обеспеченность;

4. Стандартизация и унификация моделей, средств и методов защиты.

Целью концепции является определение возможных угроз и обеспечение защиты информации как при ее первичной подготовке, так и при передаче по каналам связи с последующей обработкой вычислительными средствами, обеспечение надежного протоколирования при обмене по каналам связи и создание защищенной сети Центрального банка Республики Узбекистан.

К основным задачам информационной безопасности относятся:

- выявление, оценка и прогнозирование источников угроз;
- развитие системы обеспечения безопасности, совершенствование ее организации, форм, методов и средств предотвращения угроз;
- нейтрализация угроз и ликвидация последствий ее нарушения.

Большое значение имеет обеспечение безопасности автоматизированной банковской системы (АБС), которая в большей степени подвержена риску.

Риск – стоимостная оценка вероятного события, ведущего к потерям. Риск позволяет оценить вероятность того, что некоторая величина финансового ущерба будет находиться в определённых количественных пределах. С расширением географии деятельности банков, их АБС, развитием сети отделений и филиалов, осуществлением совместных работ с другими экономическими структурами возрастает риск или вероятность финансовых потерь. Это связано с угрозой появления убытков для банка в целом со стороны от одного из его филиалов или одного из участников вследствие неэффективности его деятельности, либо непрофессионализма персонала или его мошенничества.

Анализ риска – это процесс получения количественной оценки ущерба, который может произойти в случае реализации угрозы безопасности. Анализ рисков включает определение того, что нужно защищать, от чего защищать и как защищать. Для этого надо определить всё, чем оцениваются риски и ранжировать их по уровню важности. Этот процесс включает принятие экономических решений о необходимых методах и средствах защиты, так как средства, выделяемые на защиту, не должны превышать стоимости защищаемого объекта.

Основные этапы анализа риска включают в себя:

- описание компонентов АБС;
- анализ угроз;
- определение уязвимых мест АБС.

Применительно к банковским структурам Республики Узбекистан основными актами в части, касающейся безопасности информации, являются законы РУз «О Центральном банке «, «О банках и банковской деятельности», «Об электронных платежах», «О банковской тайне», «О защите государственных секретов» и др.

Государственными секретами Республики Узбекистан являются особой важности, совершенно секретные и секретные военные, политические, экономические, научно-технические и иные сведения, охраняемые государством и ограничиваемые специальными перечнями.

Государственные секреты являются собственностью Республики Узбекистан. Правовую основу защиты государственных секретов составляют Конституция Республики Узбекистан, закон «О защите государственных секретов», другие, издаваемые в соответствии с ним законодательные акты Республики Узбекистан.

Центральный банк вправе оказывать содействие банкам в организации расчетно-клирингового обслуживания межбанковских платежей, в том числе с оплатой посредством платежных инструментов, определять по своему усмотрению порядок

проведения таких операций и давать соответствующие предписания.

13.2. Порядок обеспечения безопасности банковской системы

С точки зрения права осуществление защиты банка представляет собой процесс реализации законодательства, регламентирующего полномочия, обязанности, ответственность органов государственной власти, представительных и исполнительных органов банка, связанные с процессами его создания и безопасного функционирования.

Законодательство о банковской безопасности состоит из совокупности правовых актов различной юридической силы, регулирующих отношения в сфере охраны и защиты банковского дела. По степени юридической силы среди них выделяются законы, указы и постановления Президента и правительства РУз, а также ведомственные нормативные акты. Одним из таких актов является Положение «О совете банковской безопасности».

Совет безопасности – это коллегиальный орган, создаваемый при директоре банка с целью организации, координации и контроля работ по обеспечению безопасности.

Совет выполняет консультативные функции, а его рекомендации и предложения носят рекомендательный характер. Все члены совета назначаются директором банка из числа ведущих специалистов, имеющих опыт работы и заинтересованных в обеспечении безопасности.

Основными задачами совета являются:

- оценка и выработка основных направлений деятельности банка по обеспечению финансовой безопасности и защите конфиденциальной информации;
- разработка перспективных программ совершенствования системы безопасности;

- разработка предложений о содержании и характере взаимодействия с правоохранительными органами, органами местного самоуправления, с соседними службами безопасности, а также с партнерами в целях соблюдения конфиденциальности, установления и поддержания других мер безопасности;

- рассмотрение проектов о составе, состоянии и деятельности системы безопасности по отчетным периодам;

- систематический учет и анализ нарушений требований безопасности;

- планирование средств на приобретение новой техники безопасности и проведения контрольных и профилактических мероприятий по безопасности.

Совет безопасности назначается в составе председателя совета, его заместителя, секретаря и членов совета, исходя из реальных потребностей обеспечения безопасности, и оформляется приказом директора банка один раз в год.

Члены совета обязаны:

❖ активно участвовать в работе совета по обеспечению финансовой безопасности и защите информации;

❖ своевременно выявлять вероятные угрозы банка в сферах его деятельности;

❖ обеспечивать строгое соблюдение порядка и правил безопасности и защиты информации, и личным примером убеждать сотрудников в необходимости их неуклонного исполнения;

❖ постоянно проводить работу с подчиненными по вопросам безопасности, развивать у них чувство бдительности.

Члены совета имеют право:

✓ участвовать в разработке и реализации мероприятий по усилению безопасности;

✓ требовать от сотрудников соблюдения режима безопасности;

✓ вносить предложения, направленные на обеспечение безопасности и защиты информации.

Заседания совета проводятся в соответствии с планом работы, а в случае необходимости – по решению председателя совета. В настоящее время недостаточное юридическое обеспечение может привести к проблемам в банковской деятельности. Такое положение вещей требует в составе системы безопасности иметь специально подготовленного юридического консультанта в сфере правовых норм по обеспечению безопасности банка.

Ключевые слова и понятия

Агентурная разведка, администратор безопасности, антивирус, аппаратные средства защиты, гриф конфиденциальности, скремблер, хакер, шантаж, шпионаж, автоматизированная банковская система, концепция информационной безопасности ЦБ РУз.

Вопросы для самопроверки

1. Законодательные основы банковской безопасности.
2. Порядок обеспечения безопасности банковской системы.
3. Правовые основы банковской безопасности в аспекте зарубежного опыта.
4. Анализ рисков в автоматизированной банковской системе.
5. Правовая обеспеченность в области информационной безопасности.
6. Кадровая обеспеченность информационной безопасности.
7. Стандартизация и унификация моделей, средств и методов защиты информационной безопасности.

ГЛАВА XIV. ЗАЩИТА БАНКОВСКОЙ ТАЙНЫ

14.1. Понятие и содержание банковской тайны

Банковская тайна – это запрет на предоставление третьим лицам конфиденциальной информации о счетах, вкладах и операциях клиентов кредитных организаций, а также запрет на разглашение информации о самих клиентах и их близких. Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте.

Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также представлены в бюро кредитных историй на основаниях и в порядке, которые предусмотрены законом. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены законом.

Закон Республики Узбекистан «О банковской тайне» от 30 августа 2003 года N 530-II регулирует отношения в области получения, хранения, защиты, опубликования и предоставления сведений, составляющих банковскую тайну.

Банковской тайной являются защищаемые банком сведения:

- об операциях, счетах и вкладах своих клиентов;
- о своем клиенте, полученные банком в связи с оказанием ему банковских услуг;
- о наличии, характере и стоимости имущества клиента, находящегося на хранении в сейфах и помещениях банка;
- о межбанковских операциях и сделках, совершенных по поручению клиента или в его пользу;

➢ о клиенте другого банка, ставшие известными в результате обращения сведений, составляющих банковскую тайну, между банками;

➢ об участниках накопительной пенсионной системы, размере и движении сумм пенсионных взносов, пенсионных накоплениях на индивидуальных накопительных пенсионных счетах граждан.

Разглашением банковской тайны считается опубликование через средства массовой информации, распространение или сообщение в устной либо письменной форме или иным способом сведений, составляющих банковскую тайну, доведение их до третьих лиц, прямое или косвенное предоставление третьим лицам возможности для добывания таких сведений, в том числе вследствие нарушения порядка их хранения лицами, которым эти сведения были доверены или стали известны в связи с выполнением ими служебных обязанностей либо были предоставлены в установленном законом порядке.

Не считается разглашением банковской тайны сообщение или предоставление банком сведений, составляющих банковскую тайну, третьим лицам в случаях, предусмотренных законом, а также лицам, оказывающим банку юридические, бухгалтерские, аудиторские, информационные и консультационные услуги, при условии, что это необходимо для оказания данной услуги и что эти лица обязаны воздерживаться от противоправных действий, установленных законом.

Запрещается разглашение либо использование в личных целях или в интересах третьих лиц сведений, составляющих банковскую тайну, лицам, которым эти сведения были доверены или стали известны в связи с выполнением ими служебных обязанностей либо были предоставлены в установленном законом порядке.

Центральный банк Республики Узбекистан не вправе разглашать или предоставлять сведения, составляющие банковскую тайну, ставшие ему известными в связи с осуществлением возложенных на него законом задач, за исключением случаев, предусмотренных законодательством.

14.2. Защита сведений, составляющих банковскую тайну

Банк гарантирует защиту сведений, составляющих банковскую тайну. Руководителям и другим работникам банка запрещается разглашение сведений, составляющих банковскую тайну, доверенных им или ставших известными в связи с выполнением ими служебных обязанностей, а также их использование в личных целях или в интересах третьих лиц, прямое или косвенное предоставление возможности такого использования третьим лицам, в том числе вследствие нарушения порядка их хранения.

Руководитель или другой работник банка после прекращения трудового договора с банком не вправе разглашать сведения, составляющие банковскую тайну, которые стали ему известны в период работы в банке.

Банк обязан принимать организационные и технические меры, необходимые для надлежащего хранения сведений, составляющих банковскую тайну.

Банк может сообщить суду сведения, составляющие банковскую тайну клиента, в случаях и в пределах, необходимых для защиты своих прав и законных интересов, если спор возник между банком и клиентом.

Сведения, составляющие банковскую тайну, предоставляются самому клиенту, уполномоченным им представителям, а также другим лицам в порядке, установленном законом «О банковской тайне».

Информация об операциях с денежными средствами или иным имуществом, составляющая банковскую тайну, связанная с противодействием легализации доходов, полученных от преступной деятельности, и финансированию терроризма, предоставляется в специально уполномоченный государственный орган в случаях и порядке, предусмотренных законодательством.

Счетная палата Республики Узбекистан вправе получать сведения, составляющие банковскую тайну, если эти сведения необходимы для осуществления возложенных на нее задач. Центральный банк Республики Узбекистан предоставляет сведения, составляющие банковскую тайну, о своих клиентах в порядке, установленном законом.

Сведения, составляющие банковскую тайну, предоставляются органам прокуратуры, следствия и дознания при наличии возбужденного уголовного дела в отношении клиента данного банка в целях обеспечения взыскания нанесенного ущерба или наложения ареста на его имущество по мотивированному постановлению следователя или дознавателя с санкции прокурора.

Сведения, составляющие банковскую тайну, предоставляются суду на основании его письменного запроса по делам, которые находятся в производстве суда в отношении клиента данного банка.

Сведения, составляющие банковскую тайну, предоставляются судебному исполнителю на основании его письменного запроса при наличии вступившего в законную силу решения суда об обращении взыскания или наложении ареста на имущество клиента данного банка.

Сведения, составляющие банковскую тайну, предоставляются органам государственной налоговой службы в случаях, касающихся вопросов налогообложения клиента банка, в соответствии с законодательством.

Предоставление сведений, составляющих банковскую тайну, суду, органам прокуратуры, следствия и дознания, а также судебному исполнителю осуществляется посредством направления их в закрытом и запечатанном конверте запрашивающему органу при наличии для этого оснований, предусмотренных в законе.

Сведения о клиенте, составляющие банковскую тайну, банк предоставляет его наследникам или правопреемникам, если последние или уполномоченные ими представители предоставили все необходимые документы, подтверждающие их право наследования или правопреемства в соответствии с законодательством.

В случае получения документов, не подтверждающих право на наследование или правопреемство, банк обязан в течение трех рабочих дней письменно уведомить обратившееся лицо о невозможности предоставления запрашиваемых сведений, а также вправе потребовать представления дополнительных документов или направить письменный запрос соответствующему нотариусу или органу, осуществляющему государственную регистрацию юридического лица, о подтверждении права на наследование или правопреемства обратившегося лица. При предоставлении всех необходимых документов, подтверждающих право на наследование или правопреемство, банк обязан в течение пяти рабочих дней передать обратившемуся лицу исчерпывающие сведения о соответствующем клиенте и представить все документы.

Банки в целях обеспечения безопасности своей деятельности, гарантирования вкладов, возвратности кредитов и иных инвестиций могут обмениваться между собой и предоставлять друг другу сведения о своих клиентах в порядке и пределах, установленных законом.

Сведения, составляющие банковскую тайну, предоставляются Фонду гарантирования вкладов граждан в банках, а также банкам-агентам для осуществления мероприятий по возврату денег вкладчикам.

Банк, получивший сведения о клиенте другого банка, не вправе разглашать и предоставлять их третьим лицам.

Банк в соответствии с законом предоставляет сведения, составляющие банковскую тайну, только о своем клиенте, при этом, если в хранящихся в банке документах клиента указаны сведения о других лицах, такие сведения считаются сведениями о клиенте. Банк обязан отказать в предоставлении сведений, составляющих банковскую тайну, если требование о предоставлении не соответствует положениям закона.

Отказ в предоставлении сведений, составляющих банковскую тайну, может быть обжалован в суде.

Органы государственной власти и управления, в том числе правоохранительные органы, а также их должностные лица не вправе запрашивать и получать сведения, составляющие банковскую тайну, кроме случаев, указанных в законе.

Незаконное разглашение или использование сведений, составляющих банковскую тайну, лицом, которому они были доверены или стали известны в связи с выполнением им служебных обязанностей, причинившее ущерб клиенту банка, влечет за собой ответственность в соответствии с законом.

Ключевые слова и понятия

Банковская тайна, аудиторская тайна, коммерческая тайна, гриф конфеденциальности, достоверность информации, канал утечки информации.

Вопросы для самопроверки

1. Понятие и содержание банковской тайны.
2. Защита сведений, составляющих банковскую тайну.
3. Источники конфеденциальной информации.
4. Угрозы конфеденциальной информации.
5. Особенности защиты конфеденциальной информации при работе с зарубежными партнерами.
6. Служба безопасности банка как барьер на пути утечки информации, представляющей собой банковскую тайну.
7. Программно-техническая обеспеченность информационной безопасности.

ГЛАВА XV. ОРГАНИЗАЦИЯ ЗАЩИТЫ БАНКОВСКОЙ БЕЗОПАСНОСТИ

15.1. Служба банковской безопасности, функциональные задачи соотрудников банковской безопасности

Система безопасности банковской деятельности – это совокупность специальных органов, служб, средств, методов, взаимосвязанных мероприятий правового характера, осуществляемых в целях защиты банка от внутренних и внешних угроз (реальных или потенциальных противоправных действий физических или юридических лиц).

Организация деятельности системы безопасности определяется Положением о системе безопасности банка. *Цели системы безопасности банка:*

✓ защита прав банка, его структурных подразделений и сотрудников;

✓ сохранение и эффективное использование финансовых, материальных и информационных ресурсов;

✓ своевременное выявление и устранение угроз, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования и развития банка;

✓ отнесение информации к категории ограниченного доступа к различным уровням уязвимости;

✓ создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций функционирования;

✓ эффективное пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности;

✓ создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями для ослабления негативных влияний последствий нарушения безопасности на достижение стратегических целей.

Задачи системы безопасности:

➢ обеспечение безопасности функционирования банка, его кредитно-финансовой деятельности и защиты конфиденциальной информации;

➢ организация работы по правовой, организационной и инженерно-технической защите материальных, финансовых и информационных ресурсов;

➢ организация специального делопроизводства, исключающего несанкционированного получения конфиденциальных сведений;

➢ выявление и локализация возможных каналов разглашения, утечки и несанкционированного доступа к конфиденциальной информации в процессе повседневной деятельности и в экстремальных ситуациях;

➢ обеспечение режима безопасности при проведении всех видов деятельности, включая встречи, переговоры, совещания, связанные с деловым сотрудничеством на национальном и международном уровнях;

➢ обеспечение охраны зданий, помещений, оборудования и технических средств обеспечения деятельности банка;

➢ обеспечение безопасности персонала;

➢ информационно-аналитическая деятельность в интересах оценки ситуации и выявления неправомерных действий злоумышленников и конкурентов.

Система безопасности банка включает в себя 4 подсистемы:

❖ правовую;

❖ организационную;

❖ техническую;

❖ психологическую.

Правовая подсистема – это правовая обеспеченность – состояние, при котором все аспекты функционирования системы управления безопасностью регламентированы законодательными актами и соответствующими нормативными документами. К этим аспектам относятся:

- правовая культура;
- права и обязанности должностных лиц;
- правовое регулирование отношений людей в рабочих коллективах, между различными командными инстанциями, между начальниками и подчиненными и т.д.

Правовой нигилизм – социально-психологическое явление, которое выражается в полном или частичном отрицании полезности и необходимости соблюдения правовых норм отдельными членами общества.

Организационная подсистема предполагает:

- построение и устойчивое функционирование системы управления безопасностью на различных уровнях;
- развитие и создание оптимальной организационно-штатной структуры;
- организационные и другие документы, регламентирующие функционирование системы безопасности банка;
- организацию управления безопасностью повседневной деятельности и т.д.

Техническая подсистема – это:

- техническая политика в оснащении банка современными средствами безопасности;
- подбор квалифицированных технических специалистов;
- высокие требования к техническим средствам системы безопасности;
- всестороннее обеспечение системы безопасности техническими средствами;
- диагностика, осмотр, обслуживание технических средств и т.д.

Психологическая подсистема включает:

♦ психологический анализ управления безопасностью;

♦ учет психологических факторов в работе банковских служащих в повседневной деятельности и, особенно, в экстремальных ситуациях.

Важна также психологическая подготовка банковских служащих, отвечающая требованиям данного вида деятельности и способствующая эффективному выполнению своих служебных обязанностей и т.д.

Служба безопасности банка — подразделение, специально созданное для защиты его законных прав и интересов от криминальной конкуренции со стороны социальных организаций и физических лиц. Служба требует больших затрат. Вместе с тем отказ предприятий от необходимых мер защиты, экономия на защитных мероприятиях, по сути, способствуют развитию преступности.

Основные задачи службы безопасности:

- обеспечение безопасности кредитно-финансовой деятельности и защита информации и сведений, составляющих банковскую тайну;
- организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной) защите банковской тайны;
- организация специального делопроизводства, исключающего несанкционированное получение сведений, представляющих банковскую тайну;
- выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной деятельности и в экстремальных ситуациях;
- обеспечение режима безопасности при проведении всех видов деятельности, а также охрана зданий, помещений и т.п.;
- обеспечение личной безопасности руководства и ведущих сотрудников банка и т.д.

Служба безопасности в своей деятельности руководствуется:

❖ инструкцией по организации режима и охраны;

❖ инструкцией по защите банковской тайны;

❖ перечнем сведений, составляющих банковскую тайну;

❖ инструкцией по работе с конфиденциальной информацией для руководителей, специалистов и технического персонала;

❖ инструкцией по организации хранения дел, содержащих конфиденциальную информацию, в архиве;

❖ инструкцией по инженерно-технической защите информации;

❖ инструкцией о порядке работы с иностранными представителями и представительствами и т.д.

Примерная структура службы безопасности банка (основные задачи).

Сектор охраны:

- охрана помещений и зданий;
- охрана оборудования и имущества;
- охрана сотрудников и мероприятий;
- охрана перевозок и т.д.

Сектор режима:

- обеспечение секретности документов;
- обеспечение режима допуска;
- контроль посетителей и транспорта;
- расследование случаев нарушения режима и т.д.

Сектор технической защиты:

- выявление технических каналов утечки информации;
- контроль за попытками несанкционированного доступа к информации с помощью техники;
- оборудование банка средствами сигнализации и связи;
- оборудование противопожарными средствами и т.д.

Сектор оперативной работы банка:

- выявление и изучение банков и преступных сообществ, которые

являются потенциальными конкурентами или врагами;

- учет и анализ попыток проникновения в секреты банка, осуществления каких-либо враждебных акций;

- выявление возможных «слабых» мест в деятельности банка;

- разработка и осуществление мер противодействия «давлению» извне и так далее.

15.2. Информационно-аналитические способы обеспечения банковской безопасности

Ключевая роль в деятельности службы безопасности банка должна отводиться аналитическому звену, осуществляющему сбор и обработку информации о конкурирующих фирмах и компаниях на товарном рынке, о маркетинговых условиях, о криминально-конкурентных действиях. Таким аналитическим звеном может быть группа информационно-аналитической деятельности.

Информационно – аналитическая группа обеспечивает:

❖ сбор иформации из открытых источников, создание собственных информационных массивов и баз данных;

❖ разработку рекомендаций по совершенствованию системы безопасности;

❖ организацию информационного взаимодействия с единой информационной службой банка;

❖ поддержание деловых контактов с сотрудниками министерств и ведомств, представителями деловых, научных и журналистских кругов;

❖ выполнение сотрудниками требований к конфиденциальности информации.

Составление информационных документов по определенному вопросу включает подбор и систематизацию фактов, касающихся данного вопроса, оценку, отбор и истолкование фактов, а затем их четкое и продуманное изложение в устной или письменной форме, завершающее процесс составления информационного документа.

Формами информационного документа выступают:

- информационное донесение;
- информационная справка;
- информационная сводка.

Информационный доступ может касаться небольшого частного вопроса, может носить характер текущего донесения или представлять собой капитальное исследование.

Важным свойством информационного документа является его полезность для тех, кому он предназначен. Говоря о полезности, мы имеем в виду, что информация прямо или косвенно связана с обеспечением безопасности объекта. Полезность информационных документов определяется рядом параметров. Главные из них – полнота и точность информации. Однако полнота и точность не должны превалировать над своевременностью. Своевременность для информационных документов имеет наибольшее значение.

Немалое значение для информационного документа имеет его назначение и его потребители. Иногда информационный документ может быть кратким, убедительным. Если же документ готовится в качестве справочного материала, степень его полноты и специализации может не лимитироваться.

В современных условиях, когда время необходимо экономить, особое значение для информационного документа приобретает тщательность формулировок к выводов. От качества выводов и их лаконичности зависит успех документа.

В большинстве случаев разведывательная информация со временем устаревает и быстро утрачивает свою ценность. Так, информация тактического плана теряет половину своей ценности через 6 дней после ее представления. Ценность информации меняется со временем также исходя из того, что может измениться обстановка или в связи с потерей внимания к ней со стороны пользователей (утеря потребности), к примеру, оперативно-тактическая информация теряет 10 процентов ценности в день.

В каждом конкретном случае мы имеем дело с массой фактов, некоторые из них имеют к решаемой проблеме непосредственное

отношение, другие – отдаленное, третьи – никакого. Некоторые из них правильные, другие – нет, а третьи - лишь частично. Информационная работа – это процесс, в ходе которого руда фактов просеивается, очищается и превращается в конечный продукт в виде информации.

В процессе работы с фактами необходимо:

- подобрать факты;
- оценить их;
- дать им определенное истолкование;
- построить на их основе гипотезу или выдвинуть идею, замысел, примерную взаимосвязь тех или иных действий.

В современных условиях, характеризующихся широкомасштабным распространением новых ресурсо-, энерго- и трудосберегающих технологий, не только резко обострилась конкурентная борьба, но и по-новому расставились приоритеты, обусловив тем самым необходимость переоценки методов ведения стратегии и техники рынка.

Известно, что недобросовестная конкуренция осуществляется в форме промышленного шпионажа, коррупции, фальсификации продукции конкурентов и т.п. Отношения между производителями и другими участниками экономических отношений в условиях рыночной экономики могут характеризоваться доброжелательностью, терпимостью, взаимодействием либо настороженностью, соперничеством, активным противоборством. Полярными в этой ситуации выступают отношения тесного сотрудничества и противоборства. Между этими крайними формами отношений можно выделить по степени нарастания напряженности такие формы отношений, как взаимодействие, соперничество, конкуренция.

Ключевые слова и понятия

Угрозы банковской безопасности, деструктивные (дестабилизирующие) силы (факторы), главная цель банковской

безопасности, источники угроз банковской деятельности, внутренние угрозы, внешние угрозы, аттестация, контроль доступа, служба безопасности, технические средства охраны.

Вопросы для самопроверки

1. Служба банковской безопасности и ее структура.
2. Функциональные задачи сотрудников банковской безопасностии.
3. Информационно-аналитические способы обеспечения банковской безопасности.
4. Особенности аудита банковской безопасности.
5. Безопасность защищённых помещений.
6. Проведение аудита автоматизированных систем.

ГЛОССАРИЙ

Администратор – инфраструктурное подразделение, создаваемое для эффективного функционирования МЭР (межбанковского электронного рынка).

Анелик (Anelik) — российская система денежных переводов физических лиц без открытия банковского счета. Основана в 1996 году. Является одним из лидеров на рынке российских международных денежных переводов.

Антивирус – программа, обнаруживающая и удаляющая вирусы. Если вирус удалить невозможно, заражённая программа уничтожается.

Аппаратные средства защиты – механические, электромеханические, электронные, оптические, лазерные, радио-, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированного доступа, копирования, кражи или модификации.

Атака – попытка преодоления защиты информационных систем. Степень «успеха» атаки зависит от уязвимости и эффективности системы защиты.

Аттестация – оценка на соответствие определенным требованиям. С точки зрения защиты аттестации подлежат объекты, помещения, технические средства.

Аутентификация информации – установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от её источника.

Банк-бенефициар – это банк, которому адресуется ЭПД, направленный банком-инициатором через межбанковскую платежную систему.

Банк-инициатор – это банк, начавший электронную платежную операцию путем формирования и отправки ЭПД в адрес другого банка.

Банковская тайна – это запрет на предоставление третьим лицам конфиденциальной информации о счетах, вкладах и операциях клиентов кредитных организаций, а также запрет на разглашение информации о самих клиентах и их близких.

БД – база данных.

Безопасность – состояние защищенности жизненно важных интересов личности, предприятия, общества и государства от внутренних и внешних угроз.

Безопасность информационная – это проведение правовых, организационных и инженерно-технических мероприятий при формировании и использовании информационных технологий, инфраструктуры и информационных ресурсов, защите информации высокой значимости и прав субъектов, участвующих в информационной деятельности.

Безопасность национальная – гарантированная конституционными, законодательными и практическими мерами защищённость и обеспеченность национальных интересов.

Безопасность экономическая – обеспечение экономического развития страны с целью удовлетворения экономических потребностей граждан при оптимальных затратах труда и природоохранном использовании сырьевых ресурсов и окружающей среды.

Беловоротничковые угрозы - это когда предприниматели, гос. служащие, банкиры и другие представители административного аппарата, обладают возможностью по характеру предоставляемых им полномочий совершать такие экономические преступления, как: нарушение антитрестовского законодательства; мошенничества с ценными бумагами, на фондовой бирже, с получением кредитов и ссуд; присвоением банковских средств, уклонение от уплаты налогов, взяточничество и др.

Белые воротнички – представители административно-бюрократического аппарата всех сфер управления.

Бомба – тайное встраивание в программу команд, которые должны срабатывать один или несколько раз при определенных условиях. Существуют варианты с «логической» или «временной» бомбой.

Внешние угрозы – это источники, которые существуют или могут появляться за рамками организации, в частности, банка, и воздействовать на его интересы извне. Основу внешних угроз, как правило, составляют социальные источники опасности (люди), а также и природные.

Внутренние угрозы – это источники, порождаемые внутренними противоречиями или иными факторами, которые могут исходить непосредственно от коллектива, групп людей и отдельных личностей, наделенных определенными полномочиями при выполнении своих обязанностей в данном учреждении.

Главная цель безопасности банковской деятельности – обеспечение устойчивого функционирования банка и предотвращение внутренних и внешних угроз

Главный центр информатизации Центрального банка (ГЦИ) – центр, обеспечивающий техническое, программное и эксплуатационное сопровождение межбанковской платежной системы в соответствии с действующим законодательством, а также договорами между ГЦИ и банками.

Дата возникновения просрочки по расчетам – рабочий день, следующий за датой платежа, датой возврата кредита (депозита), датой уплаты процентов.

Дата платежа – рабочий день, в течение которого денежные ресурсы должны быть зачислены на счета заемщика в соответствии с условиями сделки.

Дезинформация – способ маскировки, заключающийся в преднамеренном распространении ложных сведеней об объектах, их составе и деятельности, а так же имитации их деятельности.

Действия, не считающиеся разглашением банковской тайны – сообщение или предоставление банком сведений, составляющих банковскую тайну, третьим лицам в случаях, предусмот-

ренных законодательством, а также лицам, оказывающим банку юридические, бухгалтерские, аудиторские, информационные и консультационные услуги, при условии, что это необходимо для оказания данной услуги и что эти лица обязаны воздерживаться от действий, установленных законодательством.

Деструктивные (дестабилизирующие) силы (факторы) - силы (факторы), которые способны нанести ущерб данной системе, временно вывести её из строя или полностью уничтожить.

Дилер – работник, уполномоченный участником и действующий от его имени на ведение переговоров и заключение сделок на МЭР.

Заемщик – участник, привлекающий денежные ресурсы в форме межбанковских кредитов и/или депозитов.

Закрытый ключ электронной цифровой подписи – последовательность символов, полученная с использованием средств электронной цифровой подписи, известная только подписывающему лицу и предназначенная для создания электронной цифровой подписи в электронном документе.

Закрытый ключ электронной цифровой подписи – последовательность символов, полученная с использованием средств электронной цифровой подписи, известная только подписывающему лицу и предназначенная для создания электронной цифровой подписи в электронном документе.

Закрытый ключ электронной цифровой подписи – последовательность символов, полученная с использованием средств электронной цифровой подписи, известная только подписывающему лицу и предназначенная для создания электронной цифровой подписи в электронном *документе.*

Злоумышленник – лицо (или организация), заинтересованное в получении возможности несанкционированного доступа к конфиденциальной информации, предпринимающее попытку такого доступа или совершившее его.

Золотые воротнички – новая категория персонала, обладающая высокой компьютерной грамотностью: программисты управ-

ляемых производственных комплексов, операторы роботизированных систем, специалисты по сверхновым материалам и т.д.

Инициирование электронного платежа – формирование и подтверждение ЭПД электронной цифровой подписью.

Интернет-Клиент – канал предоставления полного спектра банковских услуг исключительно с помощью Интернет-технологий.

Источники угроз банковской деятельности – природные (редкое явление); технические (связанные с техникой); социальные (общество-человек).

КОНТАКТ (CONTACT) – это система международных денежных переводов между физическими лицами, по всему миру (СНГ, Россия, Балтия и страны дальнего зарубежья), без открытия счета в банке.

Контрагент – один из участников, заключающий сделку на МЭР.

Контроль доступа – предупреждение несанкционированного доступа к защищённым данным.

Корреспондентский счет банка (корсчет) – это счет, который открывается банку в ЦР ЦБ и предназначен для проведения межбанковских электронных платежей.

Кредитор – участник, предлагающий денежные ресурсы в форме межбанковских кредитов и/или депозитов.

ЛВС – локальная вычислительная сеть.

Лицензия – предоставление права использовать защищенные патентами изобретения, технологии.

Межбанковский электронный рынок денежных ресурсов – электронный рынок, создающий условия банкам для размещения и привлечения межбанковских депозитов и/или кредитов, путем организации и проведения электронных торгов.

Маскировка – комплекс мероприятий по введению противника в заблуждение относительно наличия и расположения объектов, их деятельности и намерений.

НСД – несанкционированный доступ к информации:

- о клиенте другого банка, ставшей известной в результате обращения сведений, составляющих банковскую тайну, между банками;

- о межбанковских операциях и сделках, совершенных по поручению клиента или в его пользу;

- о наличии, характере и стоимости имущества клиента, находящегося на хранении в сейфах и помещениях банка;

- о своем клиенте, полученной банком в связи с оказанием ему банковских услуг;

- об операциях, счетах и вкладах своих клиентов;

- об участниках накопительной пенсионной системы, размере и движении сумм пенсионных взносов, пенсионных накоплениях на индивидуальных накопительных пенсионных счетах граждан.

Опасность банковской безопасности - наличие и действие сил (факторов), которые являются деструктивными и дестабилизирующими по отношению к какой-либо конкретной системе (банку).

ОС – операционная система.

Основные направления деятельности СВИФТ - предоставление оперативного, надежного, эффективного, конфиденциального и защищенного от несанкционированного доступа телекоммуникационного обслуживания для банков и проведение работ по стандартизации форм и методов обмена финансовой информацией.

Отдел обработки данных Центрального банка – отдел департамента бухгалтерского учета, отчетности и кассового исполнения государственного бюджета, в функции которого входит обеспечение межбанковских и межфилиальных расчетов Центрального банка при едином его балансе.

Открытый ключ электронной цифровой подписи – последовательность символов, полученная с использованием средств электронной цифровой подписи, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для под-

тверждения подлинности электронной цифровой подписи в электронном документе.

Платежная организация – юридическое лицо, обладающее правом собственности на товарные знаки и (или) знаки обслуживания, идентифицирующие платежную систему, и устанавливающие ее правила.

Платежная система - совокупность отношений, возникающих между субъектами платежной системы при осуществлении электронных платежей.

Подтверждение – сообщение, приравненное к простому письменному, подтверждающее заключение сделки с указанием ее существенных условий, а также, при необходимости, любых иных условий, обычно включаемых в подобные документы в соответствии с банковской практикой, переданное посредством системы S.W.I.F.T., факсимильной, телексной или в иной форме.

Подтверждение подлинности электронной цифровой подписи – положительный результат проверки принадлежности электронной цифровой подписи владельцу закрытого ключа электронной цифровой подписи и отсутствия искажений информации в электронном документе.

Пользователь платежной системы – юридическое или физическое лицо, пользующееся услугами платежной системы при осуществлении электронных платежей.

Просроченная задолженность – не возвращенная кредитору в установленный срок сумма основного долга и/или начисленных процентов.

Психическое нападение – это отрицательные различные психофизиологические состояния, рассматриваемые пострадавшим как «наведение извне», как исходящий от другого человека, с которым «пострадавший» в момент нападения находился в непосредственном контакте.

Психическое насилие – насилие, выражающееся в демонстрации оружия и готовности его применения; на вербальном уровне (словесном) в угрозе нанести побои, связать, лишить сво-

боды передвижения, убить или совершить насилие в отношении близких и родственников жертвы.

Разглашение банковской тайны – опубликование через средства массовой информации, распространение или сообщение в устной, либо письменной форме или иным способом сведений, составляющих банковскую тайну, доведение их до третьих лиц, прямое или косвенное предоставление третьим лицам возможности для добывания таких сведений, в том числе вследствие нарушения порядка их хранения лицами, которым эти сведения были доверены или стали известны в связи с выполнением ими служебных обязанностей, либо были предоставлены в установленном законодательством порядке.

СВИФТ (S.W.I.F.T.) (Society for World-Wide Interbank Financial Telecommunications) – сообщество всемирных межбанковских финансовых телекоммуникаций является ведущей международной организацией в сфере финансовых телекоммуникаций.

Сделка – сделка по привлечению и размещению денежных ресурсов в форме межбанковских кредитов и/или депозитов в национальной валюте и/или иностранной валюте на МЭР на согласованных участниками условиях и в соответствии с действующим законодательством.

Скимминг – тщательное и полное копирование всего содержимого магнитных треков (дорожек).

СУБД – система управления базами данных.

Участник МЭР - Центральный банк Республики Узбекистан и коммерческий банк – резидент Республики Узбекистан, заключающий на МЭР сделки в соответствии с действующим законодательством.

ЦБРУ – Центральный банк Республики Узбекистан.

Центр расчетов Центрального банка (ЦР ЦБ) – это отдел учета, отчетности и расчетов главного управления Центрального банка Республики Узбекистан города Ташкента, в функции которого входит открытие и обслуживание корреспондентских счетов

головных офисов коммерческих банков и бесперебойное обеспечение электронных расчетов между ними.

Член платежной системы – юридическое лицо, оказывающее пользователям данной платежной системы услуги по осуществлению электронных платежей на основе договора с платежной организацией.

Электронная цифровая подпись (ЭЦП) – подпись в электронном документе, полученная в результате специальных преобразований информации данного электронного документа с использованием закрытого ключа электронной цифровой подписи и позволяющая при помощи открытого ключа электронной цифровой подписи установить отсутствие искажения информации в электронном документе и идентифицировать владельца закрытого ключа электронной цифровой подписи.

Электронный документ – информация, зафиксированная в электронной форме, подтвержденная электронной цифровой подписью и имеющая другие реквизиты электронного документа, позволяющие его идентифицировать.

Электронный платежный документ (ЭПД) – это электронный документ, который создается на основании первичных денежно-расчетных документов в формате, установленном Центральным банком Республики Узбекистан, и заверенный электронной цифровой подписью. Он имеет юридическую силу оригинала, при условии, что проверка электронной цифровой подписи и правильности оформления дала положительный результат.

Электронный платежный документ (далее – ЭПД) – это электронный документ, который создается на основании первичных денежно-расчетных документов в формате, установленном Центральным банком Республики Узбекистан, и заверенный электронной цифровой подписью. Он имеет юридическую силу оригинала, при условии, что проверка электронной цифровой подписи и правильности оформления дала положительный результат. При визуальном представлении ЭПД оформляется аналогично оригиналу с пометкой «ЭЛЕКТРОННО».

Internet Banking – это высокотехнологичный банковский продукт, который предполагает проведение всех видов банковских операций из своего дома, офиса, с любого компьютера, имеющего доступ в глобальную сеть Интернет.

MailBank- модуль - предназначен для удаленного обслуживания клиентов с помощью электронной почты. Состоит из двух компонент: «Клиент» и «Банк».

MoneyGram (Маниграмм) – это система международных денежных переводов, реализованная Американской компанией (MoneyGram International Limited). Которая отделилась от Вестерн Юнион. Ее связывает сеть, состоящая из почти 200 тысяч агентов в различных регионах мира, включая страны СНГ, где насчитывается более семи тысяч пунктов обслуживания.

PayTelecom - система, позволяющая принимать платежи за телекоммуникационные услуги, и другие платежи в реальном времени.

Western Union – международная система переводов, функционирущая на рынке денежных переводов и главным его организатором считается американская компания (Western Union). Вестерн Юнион, это глобальная сеть, которая насчитывает более четырехсот пунктов обслуживания почти в двухстах странах мира.

ЛИТЕРАТУРА

Основная литература

1. Наврузова К.Н.,Ортиков О.А. Нақд пулсиз ҳисоб-китоблар ва тўлов тизими: Ўқув қўлланма. Т.: «Iqtisod-Moliya», 2014.

2. Омонов А., Қоралиев Т. Банкларда бухгалтерия ҳисоби: Дарслик. Т.: "Iqtisod-Moliya", 2014. 241 б.

3. Қоралиев Т.М., Абдуллаев Ё.А. Банк иши: Ўқув қўлланма. Т.: «Iqtisod-Moliya», 2009. 580 б.

4. Норқобилов С., Дадабоева Ҳ., Жураев Ў. Халқаро амалиётда банк назорати: Магистрлар учун дарслик. Т.: «Iqtisod-Moliya», 2007. 180 б.

5. Наврузова К., Аллаберганов Р. Бухгалтерский учет в банках: Учебник. Т.: «Iqtisod-Moliya», 2017. 312с.

Дополнительная литература

1. Закон Республики Узбекистан «О Центральном банке Республики Узбекистан». Т., 1995.

2. Закон Республики Узбекистан «О банках и банковской деятельности». Т., 1996.

3. Указ Президента Республики Узбекистан «О Стратегии действий по дальнейшему развитию Республики Узбекистан» от 7 февраля 2017 года № УП-4947.

4. Мирзиёев Ш. Критический анализ, жесткая дисциплина и персональная ответственность должны стать повседневной нормой в деятельности каждого руководителя. Т.: Узбекистон, 2017. 104 с.

5. Муллажонов Ф. Ўзбекистон Республикаси банк тизими. Т.: Ўзбекистон, 2011.

6. Муругова И.А. Операционная техника и учёт в банках: Учебное пособие. Т.: “Iqtisod-Moliya”, 2010. 112 с.

7. Наврузова К.Н., Ортиков О.А. Банкларда ҳисоб ва тўлов тизими: Укув кулланма. Т.: «Iqtisod-Moliya», 2005. 180 б.

8. Муругова И.А., Бабаева Г.Я., Эрназаров Н.С. Проблемы организации учетнно-операционных работ банка: Монография. Т.:Узбекистан, 2017. 128 с.

Интернет сайты

- www.gov.uz – Правительственный портал Республики Узбекистан.
- www.lex.uz – Национальная база данных законодательства Республики Узбекистан.
- www.mf.uz – Официальный сайт Министерства финансов Республики Узбекистан.
- www.cbu.uz – Официальный сайт Центрального банка Республики Узбекистан.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 3

ГЛАВА I. ПЛАТЕЖНАЯ СИСТЕМА И ЕЁ СТРУКТУРА 5
1.1. Понятие платежной системы и её элементы 5
1.2. Платежная система Республики Узбекистан и её образование 9
1.3. Межбанковская платежная система 12
Ключевые слова и понятия 16
Вопросы для самопроверки 16

ГЛАВА II. СИСТЕМА БЕЗНАЛИЧНЫХ РАСЧЕТОВ 17
2.1. Система безналичных платежей и её элементы. Сущность положения «О безналичных расчетах в Республике Узбекистан», его значение и применение на практике 17
2.2. Пластиковые карточки и их место в национальной платёжной системе 23
Ключевые слова и понятия 33
Вопросы для самопроверки 33

ГЛАВА III. СИСТЕМА ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ ..... 35 И ЕЁ РОЛЬ В ОРГАНИЗАЦИИ МЕЖБАНКОВСКИХ РАСЧЕТОВ 35
3.1. Сущность и значение системы электронных платежей, её развитие в Узбекистане и принципы её работы 35
3.2. Технологический процесс передачи информации посредством межбанковской платёжной системы 44
Ключевые слова и понятия 49
Вопросы для самопроверки 49

ГЛАВА IV. ПЛАТЕЖНАЯ СИСТЕМА, ОСНОВАННАЯ НА ЕДИНОМ КОРРЕСПОНДЕНТСКОМ СЧЕТЕ 50
4.1. Понятие единого корреспондентского счета. Бухгалтерская модель организации расчетов между банками 50

4.2. Организация безопасности электронной информации 53
Ключевые слова и понятия 55
Вопросы для самопроверки 55

ГЛАВА V. ПЛАТЕЖНАЯ СИСТЕМА, ОСНОВАННАЯ НА ПРОГРАММНОМ ОБЕСПЕЧЕНИИ «БАНК-КЛИЕНТ» 57
5.1. Программное обеспечение «Банк-Клиент», его значение и основные функции 57
5.2. Порядок проведения расчетов через систему «Банк-Клиент» 60
5.3. Развитие системы «Банк- Клиент» и её связь с системой «Интернет- банкинг» 63
Ключевые слова и понятия 66
Вопросы для самопроверки 67

ГЛАВА VI. ЭЛЕКТРОННАЯ ПЛАТЕЖНАЯ СИСТЕМА «ИНТЕРНЕТ-БАНКИНГ» 68
6.1. Роль электронной платёжной системы "Интернет-банкинг" в банковской деятельности 68
6.2. Развитие Интернет-банкинга в Республике Узбекистан 70
Ключевые слова и понятия 74
Вопросы для самопроверки 75

ГЛАВА VII. НОВЫЕ БАНКОВСКИЕ ТЕХНОЛОГИИ 76
7.1. Развитие Интернет- технологий при предоставлении банковских услуг 76
7.2. Сущность системы платежей посредством телефона - "PhoneBank" и её применение на практике 79
7.3. Банковские технологии в мировой практике и возможности их применения в Узбекистане 82
Ключевые слова и понятия 85
Вопросы для самопроверки 85

ГЛАВА VIII. МЕЖДУНАРОДНАЯ ПЛАТЕЖНАЯ СИСТЕМА СВИФТ 87
8.1. Понятие международной платёжной системы СВИФТ и её организация 87

8.2. Этапы вступления в члены международной платёжной системы СВИФТ 89
8.3. Общий порядок расчётов посредством международной платёжной системы СВИФТ, её преимущества и недостатки 92
Ключевые слова и понятия 94
Вопросы для самопроверки 95

ГЛАВА IX. СИСТЕМЫ НАЛИЧНЫХ ДЕНЕЖНЫХ ПЕРЕВОДОВ 96
9.1. Системы наличных денежных переводов и их основные виды 96
9.2. Другие виды денежных переводов и их особенности 101
Ключевые слова и понятия 104
Вопросы для самопроверки 104

ГЛАВА X. ЦЕЛЬ И ЗАДАЧИ БАНКОВСКОЙ БЕЗОПАСНОСТИ 106
10.1. Понятие и содержание безопасности 106
10.2. Цель и задачи системы безопасности 108
Ключевые слова и понятия 109
Вопросы для самопроверки 109

ГЛАВА XI. ВИДЫ УГРОЗ, ВЛИЯЮЩИХ НА БАНКОВСКУЮ БЕЗОПАСНОСТЬ 110
11.1. Виды угроз и их классификация 110
11.2. Угрозы преступного характера 112
Ключевые слова и понятия 116
Вопросы для самопроверки 116

ГЛАВА XII. ОБЪЕКТЫ БАНКОВСКОЙ БЕЗОПАСНОСТИ 117
12.1. Персонал как объект безопасности банка 117
12.2. Финансовые и материальные средства как объект банковской безопасности 119
12.3. Информация как объект банковской безопасности 121
Ключевые слова и понятия 123
Вопросы для самопроверки 124

ГЛАВА XIII. ПРАВОВЫЕ ОСНОВЫ БАНКОВСКОЙ БЕЗОПАСНОСТИ 125
13.1. Законодательные основы банковской безопасности 125
13.2. Порядок обеспечения безопасности банковской системы 128
Ключевые слова и понятия..... 130
Вопросы для самопроверки..... 130

ГЛАВА XIV. ЗАЩИТА БАНКОВСКОЙ ТАЙНЫ 131
14.1. Понятие и содержание банковской тайны..... 131
14.2. Защита сведений, составляющих банковскую тайну 133
Ключевые слова и понятия..... 136
Вопросы для самопроверки..... 136

ГЛАВА XV. ОРГАНИЗАЦИЯ ЗАЩИТЫ БАНКОВСКОЙ БЕЗОПАСНОСТИ 137
15.1. Служба банковской безопасности, функциональные задачи соотрудников банковской безопасности 137
15.2. Информационно-аналитические способы обеспечения банковской безопасности 142
Ключевые слова и понятия..... 144
Вопросы для самопроверки..... 145

ГЛОССАРИЙ 146
ЛИТЕРАТУРА 156

Муругова Ирина Анатольевна,
Бабаева Гузаль Яшиновна

ПЛАТЕЖНАЯ СИСТЕМА И БАНКОВСКАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Редактор Э.Хуснутдинова
Худ.редактор К.Бойхужаев
Компьютерная верстка О.Фозилова

Лиц. изд. AI 305.
Подписано в печать 23.04.2019.
Формат 60x84 1/16. Усл.печ.л. 9,45. Уч.-изд.л. 9,8.
Тираж 50 экз. Заказ № 11.

Издательство «IQTISOD-MOLIYA».
100000, Ташкент, ул. Амира Темура, 60[a].