МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН

МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛЬ-ХОРЕЗМИ

С.Ю. ЮСУПОВ, Ш.Р. ГУЛОМОВ

ЦИФРОВАЯ КРИМИНАЛИСТИКА

Учебное пособие

ТАШКЕНТ – 2018

УДК: 343.98
ББК 67.51я73

С.Ю. Юсупов, Ш.Р. Гуломов. Цифровая криминалистика: учебное пособие. –Т.: «Fan va texnologiya», 2018, 318 стр.

Учебное пособие посвящено разделу науки под названием «Цифровая криминалистика», в котором изложены основные понятия, виды и задачи цифровой криминалистики, теоретические и практические основы применения компьютерной технологии и компьютерной техники при расследовании компьютерных преступлений и экспертной деятельности.

Учебное пособие предназначено для магистрантов, обучающихся по специальности «Информационная безопасность» и «Криптография и криптоанализ», а также может быть полезно широкому кругу специалистов, деятельность которых связана с обеспечением информационной безопасности и расследованием компьютерных преступлений.

Рецензенты:

Саитбаев Т.Р. - доктор юридических наук, профессор кафедры «Юридические и специальные дисциплины» ФПК Академии МВД РУз.

Мусаев М.М. - доктор технических наук, профессор кафедры «Компьютерные системы» Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми.

ISBN 978-

Изд-во «Fan va texnologiya», 2018.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В последние два десятилетия во всем мире наблюдается широкомасштабный рост преступлений, совершаемых с использованием компьютерной техники и новых информационных технологий. Преступления, совершаемые с использованием компьютерной техники, характеризуются высочайшим уровнем латентности и низким уровнем раскрываемости, что делает «компьютерную преступность» делом очень прибыльным и достаточно безопасным. Отмечаются существенный рост числа зарегистрированных компьютерных преступлений и случаи компьютерного хулиганства со значительным ущербом. В среднем одно компьютерное вторжение в банковскую информационную систему приносит сегодня ущерб в миллионы долларов, в то время как при обычном ограблении из банков в среднем за один раз уносится в пределах несколько десятки тысяч долларов.

Компьютеры, компьютерные сети, цифровая техника становятся объектами незаконных действий:

– несанкционированное вторжение, хакерские атаки;

– модификация, искажение или уничтожение баз данных;

– хищение или копирование информации;

– хищение денежных средств, мошенничество с платежными средствами (банк-клиент и др.);

– использование вирусов и другого вредоносного программного обеспечения;

– использование персональных компьютеров (ПК) для организации атак и других вредоносных действий на другие ПК и локальные сети.

Расследованием этих преступлений занимается раздел науки под названием «Цифровая криминалистика» или с английского «Форензика».

В нашей республике наряду с развитием информационных технологий в органах государственного и хозяйственного управления особое внимание уделяется задачи и предметы цифровой криминалистики, методы и средства исследования криминалистики и способы совершения компьютерных преступлений. В связи с этим были достигнуты ощутимые результаты по восстановление данных, компьютерной экспертизы данных и носителей данных и было начато создание этапы расследования и плана реагирования на инциденты информационной безопасности. Наряду с этим, необходимо требуется совершенствовать методы и средства цифровой стеганографии и способы защиты информации от киберпреступлений. В постановлении Президента Республики Узбекистан Ш.М. Мирзиёева “О мерах по коренному совершенствованию системы распространения актов законодательства” от 8 февраля 2017 года №ПП-2761 и в Стратегии действий по дальнейшему развитию Республики Узбекистан в 2017-2021 годах определены задачи, в том числе, «...совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере»[1] и вопросу раскрытия киберпреступлений уделено особое внимание. Реализации этих задач является одной из важных проблем.

В данном учебном пособии содержится теоретические и практические основы применения компьютерной технологии и компьютерной техники при расследовании компьютерных преступлений и экспертной деятельности.

В первой главе пособия рассматриваются основные понятия, виды и задачи цифровой криминалистики, сферы ее применения и методы исследования криминалистики, а также вопросы контр-форензики – противодействие методам поиска, обнаружения и закрепления цифровых

[1] Указ Президента Республики Узбекистан от 7 февраля 2017 года № УП-4947 «О Стратегии действий по дальнейшему развитию Республики Узбекистан».

доказательств. Представлены средства цифровой криминалистики состоящих из специальных технических средств, криминалистических фотосъемок и видеозаписей и криминалистических информационных систем.

Во второй главе рассматриваются основные направления компьютерных преступлений, их категории, связанные с вмешательством в работу компьютеров и использующие компьютеры как необходимые технические средства, классификация компьютерных преступлений по кодификатору Генерального Секретариата Интерпола, типичные образы компьютерных преступников. Приведены способы совершения компьютерных преступлений и различные виды компьютерных преступлений.

В третьей главе пособия представлены основные группы мер предупреждения компьютерных преступлений, показаны, что большая часть компьютерных преступлений совершается вследствие недостаточности организационных мер в предприятиях и организациях, слабой защитой данных от НСД, недостаточной конфиденциальности, слабой проверки и инструктажа персонала. Здесь дается механизмы предупреждения компьютерных преступлений и их исследования и следы преступления, разделенные на две внешние и внутренние категории.

Четвертая глава посвящена рассмотрению вопросов расследования инцидентов, в которых определяются последствий атаки, причины и способы их появления, сложности при управлении инцидентами. Исследуются категории и классификация инцидента и прецедентный анализ инцидентов информационной безопасности. Здесь же рассмотрены направление классической стеганографии - цифровая стеганография, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты и категории атак против систем скрытной передачи сообщений.

В пятой главе рассматриваются криминалистическое исследование

компьютерных средств и систем, благодаря полученной информации, может быть использовано в качестве доказательства, виды компьютерно-технических экспертиз. Здесь дается две экспертные системы - судебный набор инструментов (FTK), используемым в цифровой криминалистике, которая является единственным процитированным судом цифровым решением для исследований, созданным для быстрого, стабильного и непринужденного использования и вторая, это технология и программы для проведения всех этапов компьютерной экспертизы (EnCase Forensic), которая позволяет экспертам получать данные с помощью широкого спектра готовых фильтров и модулей, выявлять потенциальные доказательства путем криминалистического анализа информации и подготавливать полные отчеты о полученных результатах, сохраняя при этом надежность и целостность полученных доказательств.

Шестая глава посвящена проблемам современной киберпреступности, приведены основные причины роста киберпреступности и деяния, являющиеся киберпреступлениями. Рассмотрены принципы, организации, методы и подходы в области предупреждения киберпреступности.

Учебное пособие рекомендуется для магистрантов, обучающихся по специальности 5А330302-«Информационная безопасность» и 5А330301-«Криптография ва криптоанализ», а также может быть полезно широкому кругу специалистов, деятельность которых связана с обеспечением информационной безопасности и расследованием компьютерных преступлений.

1. ПОНЯТИЕ, ЗАДАЧИ И СРЕСТВА ЦИФРОВОЙ КРИМИНАЛИСТИКИ

1.1.Основные понятия цифровой криминалистики

В конце 70-х гг. прошлого столетия в юридической литературе все отчетливее стали выражаться мнения о том, что появляется новый вид преступлений, связанный с компьютерной информацией, информационными технологиями. Соответственно этому, стало формироваться новое направление криминалистики, охватывающее специфические методы и средства направленные на борьбу с этими видами преступлений.

В то же время отсутствие опыта уголовно-правового регулирования в данной сфере, трудности понимания технических аспектов и особенностей данного вида преступности приводили к тому, что очень долго в криминалистической литературе существовало сразу несколько его названий: «информационное преступление», «компьютерное преступление», «преступление в сфере высоких технологий», «коммуникационное преступление», «сетевое преступление», «машинно-интеллектуальное или технико-интеллектуальное преступление».

Одним из вариантов реагирования на сложившуюся ситуацию стало предложение Н.Н.Федотова о введении понятия «форензика» - с англоязычного термина «computer forensic», производного от «forensic science» или «forensic» - наименования науки, изучающей целый спектр научных дисциплин и технологических приемов исследования окружающей обстановки для сбора судебных доказательств.

Таким образом, ***«Цифровая криминалистика»*** или термин ***«форензика»*** произошел от латинского «foren», что значит «речь перед форумом», то есть выступление перед судом, судебные дебаты. Она является

наукой о выявлении и раскрытии компьютерных преступлений, исследования системных сбоев, об используемых инструментах, а также о способах получения доказательств проникновения злоумышленника и сбора информации.

Цифровая криминалистика (digital forensics) – подраздел криминалистики, прикладная наука о расследовании преступлений (инцидентов) и сборе цифровых доказательств, находящихся на компьютерах, системах хранения данных, в компьютерных сетях, на мобильных и других цифровых устройствах.

Задачей цифровой криминалистики является сохранение, идентификация, извлечение и документирование цифровых доказательств.

Цифровые преступления:

- преступления, направленные против цифровой техники;
- преступления, в которых цифровая техника сохраняет доказательства;
- преступления, совершаемые с помощью цифровой техники.

Сфера применения форензики: анализ и расследование событий, в которых фигурируют компьютерная информация как объект посягательств, компьютер как орудие совершения преступления, а также какие-либо цифровые доказательства. В начале были выделены три направления компьютерных преступлений:

- использование или попытка использования компьютера, вычислительной системы или сети компьютеров с целью получения денег, собственности или услуг;
- преднамеренное несанкционированное действие, имеющее целью изменение, повреждение, уничтожение или похищение компьютера, вычислительной системы, сети компьютеров или содержащихся в них систем математического обеспечение, программ или

информации;

- преднамеренное несанкционированное нарушение связи между компьютерами, вычислительными системами или сетями компьютеров.

За последние годы количество инцидентов увеличиваются в геометрической прогрессии, менялись термины: «информационные преступления», «преступление, совершённое с использованием информационных технологий», «киберпреступление» и на данный момент выделяют три направления компьютерных преступлений:

- преступления против информационной безопасности;
- преступления, где электронная информация является средством совершения другого преступления;
- преступления, совершаемые с использованием компьютерной и иной электронной техники.

Компьютерные преступления представляют серьёзную угрозу национальной и экономической безопасности и начиная с 70-х годов в ведущих странах создаются специальные подразделения по борьбе с компьютерной преступностью, в высших учебных заведениях читают курсы по методики расследования информационных преступлений.

Эти курсы охватывают следующие основные направления борьбы с компьютерной преступностью:

1. Реагирование на инциденты (Incident response)
2. Расследование инцидентов (eDiscovery)
3. Цифровая криминалистика (Digital Forensic)
4. Мониторинг инцидентов (Monitoring Incidents).

Цифровая криминалистика является одним из ключевых направлений расследования компьютерных преступлений. В ходе своей работы специалисты-криминалисты анализируют максимум данных, что позволяет

им установить причины и хронологию инцидента, разобраться в методах и целях осуществления атаки, а также указать на причастных лиц.

Во время анализа цифровых носителей информации специалисты восстанавливают хронологию событий; анализируют журналы файловой системы, операционной системы, приложений; изучают ключи реестра операционной системы; исследуют носитель на наличие вредоносного программного обеспечения. Также следует выделить особое направление в рамках компьютерное криминалистики - вирусную аналитику, нацеленную на изучение функционала, сетевых взаимодействий и алгоритма работы вредоносных программ.

***Сферы применения цифровой криминалистики*:**

1. Раскрытие и расследование уголовных преступлений, в которых фигурируют компьютерная информация как объект посягательства, компьютер как орудие совершения преступления, а также какие-либо цифровые доказательства.

2. Сбор и исследование доказательств для гражданских дел, когда такие доказательства имеют вид компьютерной информации. Особенно это актуально по делам о нарушении прав интеллектуальной собственности, когда объект этих прав представлен в виде компьютерной информации – программа для ЭВМ, иное произведение в цифровой форме, товарный знак в сети Интернет, доменное имя и т.п.

3. Страховые расследования, проводимые страховыми компаниями касательно возможных нарушений условий договора, страхового мошенничества, особенно когда объект страхования представлен в виде компьютерной информации или таким объектом является информационная система.

4. Внутрикорпоративные расследования инцидентов безопасности, касающихся информационных систем, а также работы по предотвращению

утечки информации, содержащей коммерческую тайну и иные конфиденциальные данные.

5. Военные и разведывательные задачи по поиску, уничтожению и восстановлению компьютерной информации в ходе оказания воздействия на информационные системы противника и защиты своих систем.

6. Задачи по защите гражданами своей личной информации в электронном виде, самозащиты своих прав, когда это связано с электронными документами и информационными системами.

Во многих из этих приложений некоторые методы форензики очень тесно интегрированы с методами технической защиты информации.

Таким образом, **«Цифровая криминалистика»** или **«Форензика»** является прикладной наукой о раскрытии и расследовании преступлений, связанных с компьютерной информацией, о методах получения и исследования доказательств, имеющих форму компьютерной информации, о применяемых для этого технических средствах.

1.2. Виды цифровой криминалистики

Цифровую криминалистику можно разделить на три вида (Рис.1):

«Компьютерная криминалистика» – это наука и искусство, она требует использовать специальные методы для восстановления, проверки подлинности и анализа электронных данных, связанных с компьютерными преступлениями. В ней объединяются компьютерные науки, информационные технологии и другие технические вопросы с законом.

«Сетевая криминалистика» – появилась давно, и специалисты по анализу безопасности уже много лет пользуются Ethereal, Wireshark и другими анализаторами трафика. Во-первых, пользователи стали активнее прибегать к инструментам сетевой криминалистики в целях максимально

быстрого обнаружения подозрительных действий. Во-вторых, разработчики систем безопасности создали специализированные решения по обнаружению таких подозрительных действий.

«Мобильная криминалистика» – применительно к темам сотовой связи - возможность извлечения и декодирования цифровых данных мобильных устройств.

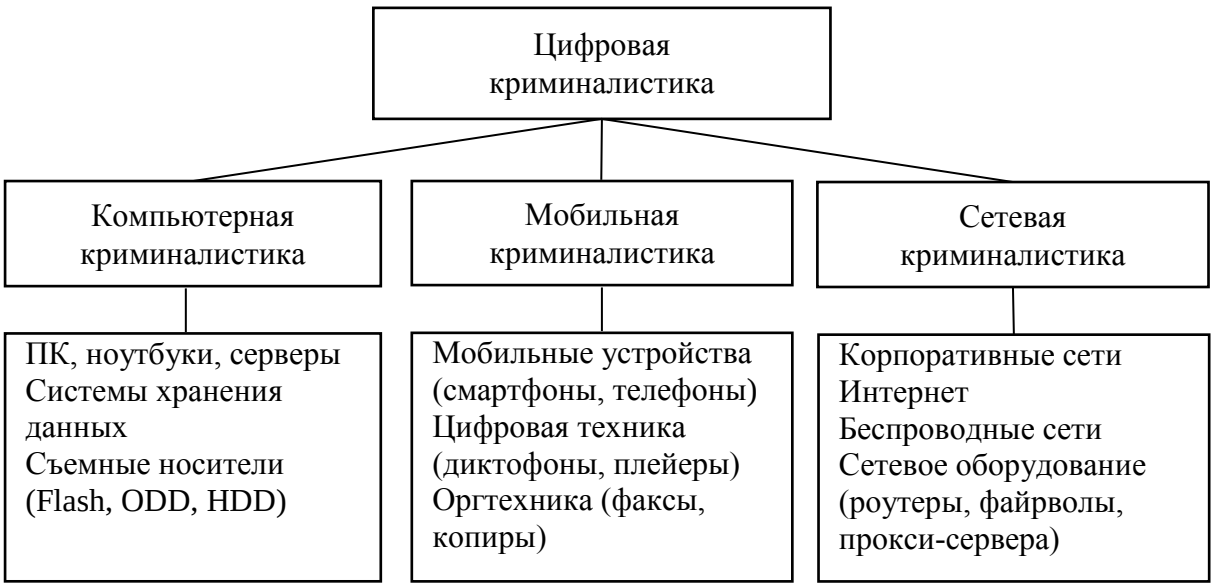


Рис.1. Виды цифровой криминалистики

Рост преступлений, совершаемых с использованием компьютерных средств и новых информационных технологий, объясняются факторами, приведенными на рис.2. Количество и разнообразие преступлений, совершаемых с использованием средств компьютерной техники и новых информационных технологий, постоянно растет. При этом предметы посягательства при совершении таких преступлений можно разделить на две группы:

- сама компьютерная техника и информация;
- объекты, которые могут быть атакованы, с использованием

компьютерной техники и информации, как инструмента преступного посягательства.

Рис.2. Структура роста преступлений, совершаемых с использованием компьютерных средств

В соответствии с этим все преступления, совершаемые с применением средств информации, можно разделить на четыре группы (Рис.3).

Компьютерная техника может выступать предметом преступного посягательства при совершении преступлений против собственности - хищение, уничтожение, повреждение. Предметами посягательств выступают сами технические средства как материальные объекты. Компьютерная техника и информация могут выступать и средством совершения общеуголовных преступлений. В этом смысле компьютер может

рассматриваться в одном ряду с такими орудиями преступления, как оружие или транспортное средство.

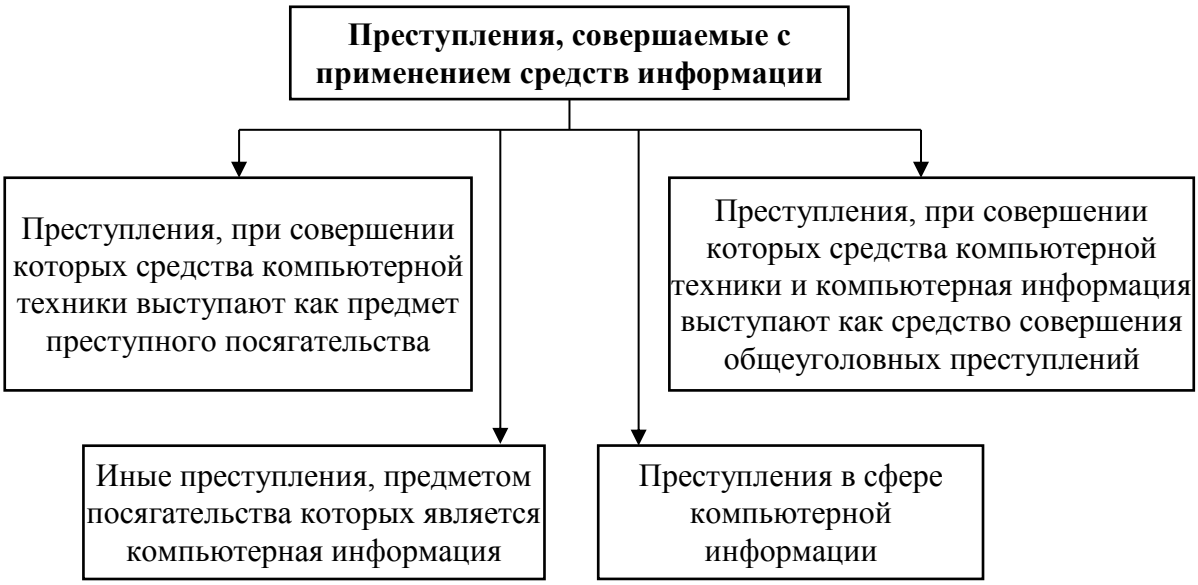


Рис.3. Схема преступления, совершаемые с применением средств информации

К наиболее распространенным преступлениям, при совершении которых в качестве орудия их совершения выступает компьютерная техника и информация, относятся преступления связанные с кражей материальных средств, путем внесения изменений в автоматизированные банки данных, содержащие информацию о праве собственности на данный вид имущества с использованием различных аппаратно-программных средств (например, вредоносных программ), во-вторых, хищение материальных носителей информации.

1.3. Задачи и предметы цифровой криминалистики

Цифровая криминалистика имеет проблемы технического, правового

характера и в области подготовки кадров.

1. Технические:

- съем данных с цифровых носителей;
- восстановление информации;
- поиск, анализ и интерпретация данных;
- обеспечение сохранности цифровых доказательств.

2. Правовые:

- доказательность собранных данных;
- нормативная база.

3. Подготовка специалистов:

- знания физических принципов работы цифровых систем и инструментария компьютерной криминалистики;
- знания технических и правовых аспектов.

Съем данных:

1. Неразрушающее копирование данных (возможность случайной и намеренной модификации данных).
2. Соответствие копии оригиналу (хеширование, выбор хеш-функции).
3. Полнота копии («скрытые» и резервные области, разрушенные данные).
4. Скорость копирования (высокая емкость накопителей).
5. Сохранность копий. Работа в полевых условиях, транспортировка, хранение копий.
6. Защита данных, предотвращение утечек информации.

Восстановление данных:

1. Восстановление разрушенных данных.
   - аппаратные и программные сбои;
   - воздействие вредоносного ПО;

• ошибки и намеренные действия пользователей.

2. Восстановление «закрытых» данных.

• данные, закрытые паролем;

• кодированные и шифрованные данные;

• данные в «скрытых» областях.

3. Восстановление с систем хранения данных.

• RAID системы и внешние DAS системы;

• сетевые хранилища NAS;

• виртуальные и распределенные хранилища данных.

4. Разнообразие технологий хранения данных.

• типы накопителей;

• интерфейсы;

• способы организации хранения данных.

Согласно этих проблем цифровая криминалистика решает следующие задачи:

– разработка тактики оперативно-розыскных мероприятий (ОРМ) и следственных действий, связанных с компьютерной информацией;
– создание методов, аппаратных и программных инструментов для сбора и исследования доказательств компьютерных преступлений;
– установление криминалистических характеристик правонарушений, связанных с компьютерной информацией.

Почти все следы, с которыми приходится работать специалисту по форензике, имеют вид компьютерной информации, регулярной или побочной. Их достаточно легко уничтожить – как умышленно, так и случайно. Часто их легко подделать, ибо «поддельный» байт ничем не отличается от «подлинного».

Фальсификация цифровых доказательств выявляется либо по смысловому содержанию информации, либо по оставленным в иных местах

следам, тоже информационным. Цифровые доказательства нельзя воспринять непосредственно органами чувств человека, но только через посредство сложных аппаратно-программных средств. Поэтому эти следы сложно продемонстрировать другим лицам – понятым, прокурору, судье. Не всегда просто обеспечить неизменность следов при их хранении. И не только обеспечить, но и доказать суду эту неизменность. Вообще, понятие «неизменность» лишь с натяжкой применима к компьютерной информации. На некоторых видах носителей она хранится действительно статически – в виде разной намагниченности участков носителя или вариаций его оптических свойств. Но в других случаях метод хранения информации таков, что предусматривает постоянную смену носителя.

Оперативная память компьютера регенерируется раз в несколько миллисекунд. То есть записанные там сигналы фактически стираются и записываются вновь. При передаче по многим каналам связи используется помехоустойчивое кодирование в расчете на возникающие при передаче ошибки; эти ошибки неизбежно возникают, но исправляются на принимающей стороне линии за счет избыточности кода. В центральном процессоре тоже постоянно происходят ошибки при совершении арифметическо-логических операций, но если их не слишком много, они исправляются благодаря внутренней диагностике. В сетевых протоколах, таких как TCP (Transmission Control Protocol, протокол управления передачей), эта надежность достигнута именно за счет того, что пропавшие в пути датаграммы или иные блоки информации предпосылаются, пока не будет подтвержден их верный прием.

Предметами цифровой криминалистики являются:

- Информационные технологии – возможность использования, как для предотвращения преступлений, так и для их совершения.
- Методы изучения прикладного программного обеспечения.

- Криминальная практика – способы, инструменты совершения соответствующих преступлений, их последствия, оставляемые следы, личность преступника.
- Оперативная, следственная и судебная практика по компьютерным преступлениям
- Методы исследования работы системы.

Что касается влияния форензики на преступность в целом, то оно возможно несколькими путями:

– стремительное развитие информационных технологий предполагает в будущем появление искусственного разума, где проявят себя новые отношения и новые преступления;
– еще недавно достижения информационных технологий не охранялись совсем, сейчас ситуация постепенно меняется, например, доменное имя на сегодняшний день защищено и является объектом интеллектуальной собственности;
– настало время, когда изменились принципы и способы мошенничества, но суть осталась одна: некоторые типы мошенничества сохранили суть, но переместились из реального пространства в виртуальное.

Влияние передовых достижений техники и технологии на преступность возможно тремя путями:

Во-первых, неостановимый технический прогресс дает возможность совершать преступления новыми способами и при помощи новых орудий. Естественно, в той же мере прогресс способствует появлению новых способов раскрытия преступлений – как старых, так и новых. Например, то же старое мошенничество в наш век совершается при помощи сети Интернет. Но суть и предмет посягательства у мошенничества прежние. Новыми являются лишь орудия совершения – веб-сайт, электронная почта, платежная

система.

Во-вторых, достижения информационных технологий порождают принципиально новые общественные отношения, каковые отношения и становятся предметом преступных посягательств. При этом способ посягательства и орудия могут быть как старыми, так и новыми, с учетом достижений ИТ.

Самый яркий пример – доменные имена. Такого общественного отношения, как право распоряжаться доменным именем, до недавних пор просто не существовало. Не было и посягательств. Ныне доменные имена охраняются законом (они причислены к объектам интеллектуальной собственности).

В-третьих, развитие ИТ может привести к появлению не просто новых общественных отношений, но нового субъекта таких отношений. Программа для компьютера еще не рассматривается в качестве субъекта права, но в качестве стихийной силы уже иногда рассматривается. Программам уже дано принимать решения, которые могут существенно влиять на благосостояние и даже жизнь людей. Программы уже могут порождать новые объекты авторского права. Появление принципиально нового субъекта, нового члена общества со своими правами – искусственного интеллекта – не за горами. А его появление вызовет новые правоотношения и, соответственно, новые преступления.

1.4. Методы исследования криминалистики

Научные методы представляют собой способы познания тех явлений, процессов, видов деятельности, которые относятся к объекту и предмету науки. В соответствии с этим методы исследования криминалистики - это система правил, приемов познания закономерностей собирания, исследования, использования доказательственной информации.

К ним относятся и способы разработки криминалистических рекомендаций по установлению действительных обстоятельств исследуемого события, его характера и участников, принятия справедливого решения по уголовному делу.

Среди методов исследования криминалистики различаются **общенаучные и специальные**.

Общенаучными традиционно считаются методы, используемые при проведении исследований не только в криминалистике, но и в других отраслях науки. К основным общенаучным методам относятся прежде всего ***наблюдение, описание, сравнение, обобщение, экстраполяция, моделирование.***

Наблюдение представляет собой целенаправленное восприятие явлений, деятельности. При проведении криминалистических исследований наблюдаются люди (их внешние признаки, реакции на те или иные действиями т.д.); материальные объекты (предметы, документы, следы и их копии), криминальное, посткриминальное поведение участников преступления, действия других участников исследуемого события и уголовного процесса); явления и события (процессы образования и передачи информации, ее трансформации на разных этапах и т.п.). В процессе наблюдения объект воспринимается не только как целое, но и как совокупность свойств, признаков. Наблюдение включает в себя сочетание чувственного и рационального познания системы признаков, исследуемого объекта. Наблюдение может быть непосредственным и опосредованным, осуществляемым через различные носители в которых зафиксирована информация.

Сравнение заключается в одновременном сопоставлении нескольких объектов, свойств каждого изучаемого объекта и установление их сходства или различия. Специфика этого метода состоит в том, что определение

совпадения или отличия качеств объектов осуществляется не столько в процессе раздельного исследования, а в основном при непосредственном сопоставлении. Сравнение возможно при наличии не менее двух сопоставимых объектов, обладающих общими признаками, по которым и делается вывод о сходстве или различии. Типичной целью сравнения является выявление общего у сравниваемых объектов, которые изучаются с конкретных позиций, сторон. В некоторых случаях сравнение проводится в целях выявления индивидуальных свойств, отличающих объект от ему подобных.

Обобщение представляет собой переход от единичного к общему, путем выявления сходства признаков, установление объединяющих связей, тенденций, закономерностей. Обобщение осуществляется при помощи таких логических приемов, как анализ и синтез. Анализ представляет собой мысленное или фактическое расчленение сложного объекта на более простые элементы, выделение существенных. Выявленные общие, взаимосвязанные признаки синтезируются в единое целое. Результатом обобщения является практически все научные понятия и категории криминалистики.

Экстраполяция представляет собой перенос выводов о наличии определенных свойств, признаков одного объекта в других предметах, явлениях, процессах. Переносимые выводы, формулируются, как правило, при наблюдении изученных объектов, сходных с изучаемыми. Например, выявленные в ходе психологических исследований признаки лжи вообще, широко используются при изучении ложных показаний в уголовном процессе и разработке приемов их разоблачения.

Моделирование заключается в создании мысленного или материального аналога, отражающего определенную совокупность признаков оригинала, т.е. реально существующего материального объекта, процесса, действия. Создаваемые в результате модели замещают реально

существующие объекты, изучаемые криминалистикой. Степень сходства модели и оригинала может быть различной, в зависимости от целей и степени учета признаков изучаемых объектов. На начальном этапе исследования сведения об этих объектах характеризуют неполнотой и недостаточной достоверностью. В ряде ситуаций исследователь не располагает информацией для обоснованных и аргументированных суждений, которые носят вероятностный, гипотетический характер и требуют последующей проверки.

Описание понимается как фиксация признаков исследуемого объекта, выявленных другими методами. Например, описываются признаки зафиксированные при непосредственном или опосредованном наблюдении, сравнении, обобщении, эксперименте и т.д. Этот метод научного познания, является с одной стороны средством обозначения, выражения полученных знаний, а с другой – средством их систематизации. Выявленные в результате исследования признаки отдельных объектов сначала описываются, а затем обобщаются, типизируются. При помощи описания фиксируются признаки, свойства объектов, технологического процесса, условий и участников исследования, применяемых методов, полученных результатов и их объяснений.

Специальные методы, это те методы, которые применяются только в криминалистике и они подразделяются на собственно - криминалистические и основанные на данных других наук.

К первым относятся технико-криминалистические методы, используемые чаще всего при проведении исследований в области криминалистической техники. Например, в настоящее время проводятся исследования возможностей диагностики по особенностям почерка психологических свойств, психических аномалий исполнителя документа, оценки при помощи технических средств достоверности и объективности

показаний допрашиваемых и т.д.

К собственно криминалистическим относятся и структурно-криминалистические методы, заключающиеся в построении определенных систем. Содержание этих методов образуют приемы и операции по накоплению и обработке исходной информации, определению направления развертывания предполагаемой структуры, технологии ее использования в практической деятельности.

Специальные методы основанные на достижениях других наук и приспособленные для решения задач криминалистики достаточно разнообразны и классифицируются по тем отраслям научного знания, на которых они базируются.

1.5. Средства цифровой криминалистики

Развитие криминалистики привело к четкому разграничению технических и тактических приемов. Сегодня термин **«криминалистическая техника»** употребляется в двух значениях: как раздел криминалистики и как отрасль общей техники. Криминалистическая техника, являясь составной частью науки криминалистики, призвана обеспечивать решение ее задач с помощью различных технических средств и методов.

Главной задачей криминалистической техники является возможность обнаруживать и изымать невидимые и слабо видимые следы, получать розыскную и доказательственную информацию, облегчают отыскание тайников, обеспечивают высокую степень документальности фиксации обстановки, в которой производится следственное действие, способствуют повышению производительности труда следователя.

В криминалистической практике применяются различные средства фиксации: фотоаппараты, видеокамеры, магнитофоны и видеомагнитофоны,

липкие пленки, слепочные массы и другие.

Компьютерный криминалист вполне может обойтись без специальной криминалистической техники вообще. Компьютер сам по себе – достаточно универсальный инструмент. Среди многообразного периферийного оборудования и программного обеспечения найдутся все необходимые для исследования функции. Некоторые программные инструменты можно легко создать или модифицировать своими руками.

Однако специальная техника сильно облегчает работу. На сегодняшний день на рынке имеются следующие криминалистические инструменты:

- устройства для клонирования жестких дисков и других носителей (в том числе в полевых условиях);
- устройства для подключения исследуемых дисков с аппаратной блокировкой записи на них;
- программные инструменты для криминалистического исследования содержимого дисков и других носителей, а также их образов;
- переносные компьютеры с комплексом программных и аппаратных средств, ориентированных на исследование компьютерной информации в полевых условиях;
- наборы хэшей (hash sets) для фильтрации содержимого изучаемой файловой системы;
- аппаратные и программные средства для исследования мобильных телефонов и SIM-карт;
- программные средства для исследования локальных сетей;
- и некоторые другие.

Аппаратные средства. Учитывая, что современные компьютеры являются универсальными устройствами, в которых используются в основном открытые стандарты и протоколы, специальных аппаратных средств для исследования самих компьютеров и компьютерных носителей

информации не требуется. То есть универсальным инструментом является сам компьютер, а все его функции можно задействовать через соответствующие программные средства.

Аппаратные криминалистические устройства для компьютеров и компьютерной периферии служат лишь удобству специалиста или эксперта. Мобильные телефоны, цифровые фотоаппараты и видеокамеры, бортовые компьютеры, коммутаторы, маршрутизаторы, аппаратные межсетевые экраны – все эти устройства не являются технологически открытыми и вовсе не стремятся к универсальности. Для полного доступа к компьютерной информации, хранящейся в них, не всегда бывает достаточно компьютера и программных инструментов.

Экспертные программы. Такие программы предназначены в основном для исследования содержимого компьютерных носителей информации во время проведения экспертизы. Они работают не только на уровне файловой системы, но и ниже – на уровне контроллера НЖМД, что позволяет восстанавливать информацию после удаления файлов.

Приводим несколько популярных экспертных программ:

- семейство программ ProDiscover *(http://computer-forensics-lab.org/lib/?rid=22).*
- SMART (Storage Media Analysis Recovery Toolkit) *(http://computer-forensics-lab.org/lib/?cid=18).*
- Forensic Toolkit (FTK) фирмы «AccessData» *(http://computer-forensics-lab.org/lib/?rid=26).*
- экспертная система Encase.
- ILook Investigator *(http://www.ilook"forensics.org).*
- SATAN (System Administrator Tools for Analyzing Networks) – средство для снятия полной информации с компьютеров для ОС Unix.

– DIBS Analyzer 2 *(http://www.dibsusa.com/products/dan2.html).*
– Helix – экспертный комплект на загрузочном компакт-диске на основе ОС Linux.

Наборы хэшей. Так называемые «hash sets» – наборы хэшей – предназначены для облегчения исследования содержимого файловой системы больших носителей, в основном компьютерных жестких дисков.

Предположим, эксперту поступил для исследования изъятый при обыске у подозреваемого носителя информации, на котором установлена операционная система и имеются пользовательские данные. Эти данные могут быть разбросаны по различным директориям, могут содержаться внутри файлов с настройками, даже могут быть скрыты методами стеганографии внутри файлов, содержащих с виду совсем другие данные. Современные ОС включают в свой состав тысячи файлов, популярные приложения – тоже сотни и тысячи. Таким образом, в файловой системе обычного компьютера может находиться, например, 30000 файлов, из которых только 500 – это файлы, созданные пользователем или измененные им.

Чтобы отделить это «меньшинство» пользовательских файлов от заведомо не содержащего ничего интересного «большинства», предназначен набор хэшей.

Хэш, хэш-сумма или однонаправленная *хэш-функция* файла представляет собой длинное число, вычисляемое из содержимого файла по особому алгоритму. Хэш-сумма похожа на контрольную сумму, но имеет одно существенное отличие: это однонаправленная функция. То есть по файлу легко вычислить его хэш-функцию, но под заданную хэш-функцию подобрать соответствующий ей файл невозможно.

Хэши известных файлов позволяют, не рассматривая подробно содержание этих файлов, отбросить их и быть уверенным, что эти файлы не

содержат пользовательской информации. После их исключения эксперту остается исследовать относительно небольшое число файлов. Этот тип наборов именуется «knowngoods».

Существуют и наборы хэшей, выполняющие обратную задачу. Они именуются *«knownbads»* и соответствуют не заведомо безобидным файлам, а наоборот, заведомо вредоносным, содержащим порнографию, вирусы или иной криминальный контент. Обычно набор хэшей – это отдельный продукт, приобретаемый у соответствующего производителя и подключаемый к экспертному ПО. Он может содержать сотни тысяч и миллионы хэш-функций с соответствующими сведениями о файлах. Все популярные экспертные системы позволяют подключать и использовать «внешние» наборы хэшей.

Архивирование. Копирование и долговременное хранение копий данных сначала применялось лишь с целью восстановления в случае утраты – так называемое «страховочное копирование» или «холодное резервирование».

В последнее время архивирование применяется и с иными целями – для расследования инцидентов безопасности, могущих произойти или обнаружиться в будущем. То есть данные копируются не по принципу «наиболее ценные, наиболее чувствительные данные, утрата которых нанесет ущерб», а по совсем иному принципу: копируются данные и области носителей, где могут оставаться следы злоумышленных действий. Например, в отношении служебного персонального компьютера для целей восстановления архивируются файлы пользователя и отдельные его настройки. Операционная система и прикладные программы страховочному копированию не подлежат, поскольку легко восстанавливаются из дистрибутива. Все резервное копирование производится на уровне файловой системы. А для целей расследования инцидентов копируется весь жесткий

диск компьютера, причем не на уровне файловой системы, а на уровне контроллера диска, то есть чтобы включалась удаленная и скрытая информация.

Страховочная копия малополезна для расследования инцидентов. Напротив, «инцидентная» копия не подходит для восстановления на случай вирусной атаки или аварии. Это разные копии – и технически, и по назначению. Средства для архивирования на случай расследования инцидентов – это специальные криминалистические средства.

Криминалистическая фотосъемка и видеозапись.

В настоящее время рабочее место следователя предполагает не просто компьютер, но и специальное программное обеспечение, например, «АРМ-следователя» – комплекс индивидуальных технических и программных средств, предназначенных для автоматизации информационной поддержки процесса предварительного следствия, которые позволяют решать множество информационно-аналитических задач в процессе расследования.

Новые технологии предоставляют следователям новые источники криминалистически значимой информации, например, повсеместно распространенные камеры видеонаблюдения или GSM-локализация мобильных телефонов. Однако существует сфера, в которой возможности современных информационных технологий отечественными криминалистами практически не применяются или применяются недостаточно эффективно. Эта сфера - визуальная фиксация следов преступления.

Криминалистическая фотография - один из традиционных разделов криминалистической техники; еще несколько лет назад ученые высказывались против использования цифровой фотографии в криминалистике, однако теперь она практически вытеснила пленочную. Но технологии шагнули дальше и позволяют фиксировать следы преступления,

обнаруженные при производстве различных следственных действий, еще более наглядно и точно.

Среди таких средств фиксации первой стоит назвать видеосъемку. В научной и учебной литературе часто можно встретить мнение, что применение криминалистической видеозаписи при расследовании преступлений необходимо в тех случаях, когда важно запечатлеть какое-либо действие, динамику развития события или явления, иногда – вместе с сопровождающими их звуками, кроме того видеозапись позволяет запечатлевать значительные по протяженности участки местности или с большим нагромождением различных объектов, фиксировать обстановку, которая может быть изменена в ходе самого осмотра, например, при пожарах и катастрофах. То есть основное преимущество видеозаписи по сравнению с фотосъемкой заключается в возможности запечатлевать динамику изменений среды, а также движущиеся, а не статичные объекты.

Видеозапись – при разработке надлежащей методики – позволит наиболее полно и точно зафиксировать ход и результаты осмотра места происшествия. Кроме того, роль видеозаписи при фиксации статичных предметов, статичной обстановки в относительно нормальных условиях – без внешнего воздействия, возможно изменяющего место правонарушения – представляется недооцененной. Видеозапись, как и фотосъемка, позволяет осуществить ориентирующую, обзорную, узловую и детальную фиксацию места происшествия в целом, а также отдельных следов преступления в частности.

Во-первых, можно зафиксировать осмотр места происшествия с точки зрения следователя, его подхода к осмотру. Это важно не только для последующего анализа результатов осмотра в раках данного расследования, но и для оценки действий следователя в случае, если впоследствии появятся сомнения в его компетентности или правомерности его действий: если на

видеозаписи зафиксировано изъятие какого либо вещественного доказательства и его упаковка, то скрыть или исказить его будет довольно сложно. Во-вторых, возможно создание видеомоделей движения преступника во время совершения преступления, его прибытия на место происшествия и пути отхода. Последующий анализ таких моделей может иметь ориентирующее значение, служить для формирования следственных версий, помочь обнаружить новые следы преступления в тех местах, откуда пришел или куда скрылся преступник. В-третьих, видеозапись позволит зафиксировать события, которых следственная группа не ожидает, прибыв на место происшествие: от неожиданного падения предметов, повреждение которых сначала не было очевидным, до неожиданного появления преступника, который не успел покинуть место происшествия и спрятался, надеясь дождаться отъезда следственной группы. В-четвертых, в настоящее время не учитывается возможность использования видеозаписи хода осмотра места происшествия для активизации или восполнения воспоминаний свидетелей или потерпевших, хотя сама тема активизации памяти в последние 20 лет стала предметом активных исследований специалистов.

3D-технологии. Другим современным средством фиксации следов преступления является панорамная 3D-фотография. Такая фотосъемка осуществляется с использованием специальной насадки на фотоаппарат, позволяющей охватить 360º по горизонтали и вертикали. В результате на экране монитора можно получить полный обзор места происшествия с той точки, где был установлен фотоаппарат. Отдельные фрагменты панорамы можно приближать для более детального осмотра. Такие изображения также больше, чем просто наглядная фиксация отдельных деталей. Они могут использоваться следователем как для последующего анализа места происшествия и поиска новых следов, так и для активизации памяти лиц, дающих показания.

Кроме того, наиболее эффективным представляется использование такой фотосъемки в случае, когда событие преступления наблюдали несколько человек (их последующий процессуальный статус может быть различным) с разных точек зрения, возможно, даже не осознавая, что именно они видят. Создание панорамных 3D-фотографий с точек зрения всех очевидцев и их последующий совместный анализ позволит определить слепые зоны, то есть те участки, которые не могли попасть в поле зрения кого-либо или сразу всех очевидцев. Таким образом можно, с одной стороны, проверить достоверность показаний - доказать, что свидетель не мог видеть те событие или предметы, о наблюдении которых утверждает.

Такое сравнение панорамных 3D-фотографий требует компьютерного моделирования, специального программного обеспечения и соответствующих специальных знаний, а результаты сравнения должны представлять собой наглядные модели с указанием на зоны видимости каждого из очевидцев, пересекающиеся зоны видимости, слепые зоны. То есть такое сравнение должно осуществляться в форме судебной экспертизы.

Еще одним средством фиксации следов преступления является *лазерное 3D-сканирование*. В настоящее время этот способ стал довольно активно применяться в США и Западной Европе; применение такого средства фиксации - дело недалекого будущего, основное препятствие здесь - сравнительно высокая стоимость оборудования и отсутствие адекватной задачам расследования преступления методики 3D-фиксации места происшествия.

3D-модель подходит и для работы с лицами, дающими показания по делу, для активизации их памяти, а также для проведения различных компьютерно-технических экспертиз, связанных как с уже описанными задачами, так и с различного рода моделированием – траектории выстрелов, схемы движения участников происшествия, вероятных сценариев развития

событий и т.д. Модель, полученную с помощью лазерного сканирования, возможно использовать и для верификации показаний или восполнения пробелов: убрав из модели отдельные детали обстановки места происшествия либо предположив, что на момент фиксации хода и результатов осмотра на месте происшествия уже не хватало каких-то предметов, - например, они были похищены преступником, сокрыты лицом, первым прибывшим на место происшествия и т.д., - можно предложить лицу, чьи показания проверяются, дополнить модель недостающими предметами, которые можно будет выбирать из библиотеки образов, являющейся частью соответствующего программного обеспечения.

Виртуальная реальность. Кроме того, одним из перспективных направлений для дальнейших исследований представляется перенос такой модели с экрана монитора в виртуальную реальность, создающую эффект присутствия на месте происшествия.

Для создания виртуального места происшествия и его использования необходимо специальное программное обеспечение и шлем виртуальной реальности. Наиболее эффективным использование такой виртуальной модели представляется для работы с лицами, дающими показания по делу. Во-первых, можно предположить, что яркость восприятия обстановки места пришествия в условиях виртуальной реальности будет оказывать более сильное воздействие на память человека, чем фото- или видео-изображение. Во-вторых, виртуальная модель места происшествия, учитывая детализированность изображения, получаемого в результате лазерного 3D-сканирования, и сохранение всех условий, сопутствовавших первоначальному осмотру места происшествия, может быть использована для проверки показаний на месте. Сегодня проверка показаний на месте часто проводится спустя значительный отрезок времени после самого преступления, когда обстановка места происшествия уже нарушена.

Виртуальная модель позволяет вновь оказаться на месте происшествия, каким оно было в момент первоначального осмотра. Однако, безусловно, данное мероприятие не может считаться собственно следственным действием.

Таким образом, использование новых средств и технологий визуальной фиксации следов преступления имеет огромное значение для своевременного раскрытия и полного расследования преступлений.

Криминалистические информационные системы.

Указанные системы не используются напрямую для поиска и изучения доказательств. Они выполняют обеспечивающие функции в работе по раскрытию и расследованию преступлений. Но традиционно относятся к криминалистической технике. Криминалистические информационные системы выполняют ряд близких задач:

– облегчают и/или ускоряют оформление различных документов для оперативно-розыскных мероприятий (ОРМ), предварительного следствия, судебных целей;

– позволяют работникам правоохранительных органов быстрее найти необходимые нормативные акты, комментарии, прецеденты, получить консультации;

– облегчают и ускоряют доступ сотрудников ко всевозможным базам данных, учетам, справочникам – как публичным, так и закрытым;

– ускоряют и автоматизируют проведение ОРМ, связанных с перехватом сообщений.

Криминалистический процесс, который проводят специалисты и эксперты, принято делить на четыре этапа:

1) сбор;
2) исследование;
3) анализ;

4) представление.

На первом этапе происходит сбор как информации самой по себе, так и носителей компьютерной информации. Сбор должен сопровождаться атрибутированием (пометкой), указанием источников и происхождения данных и объектов. В процессе сбора должны обеспечиваться сохранность и целостность (неизменность) информации, а в некоторых случаях также ее конфиденциальность. При сборе иногда приходится предпринимать специальные меры для фиксации недолговечной информации, например, текущих сетевых соединений или содержимого оперативной памяти компьютера.

На втором этапе производится экспертное исследование собранной информации (объектов-носителей). Оно включает извлечение/считывание информации с носителей, декодирование и вычленение из нее той, которая относится к делу. Некоторые исследования могут быть автоматизированы в той или иной степени. Но работать головой и руками на этом этапе эксперту все равно приходится. При этом также должна обеспечиваться целостность информации с исследуемых носителей.

На третьем этапе избранная информация анализируется для получения ответов на вопросы, поставленные перед экспертом или специалистом. При анализе должны использоваться только научные методы, достоверность которых подтверждена.

Четвертый этап включает оформление результатов исследования и анализа в установленной законом и понятной неспециалистам форме.

1.6. Контр-форензика

Противодействие методам поиска, обнаружения и закрепления цифровых доказательств развивается не столь активно, как сама форензика.

Спрос на соответствующие контрметоды ограничен. Почему ограничен? Для понимания этого посмотрим, кому и для чего может потребоваться противодействовать обнаружению компьютерной информации.

Во-первых, то, что первым приходит в голову – ***киберпреступники.*** Те, кто имеет основания опасаться закона и прятать следы своей криминальной деятельности. Понятно, что это очень узкий рынок сбыта, работать на нем сложно, крупные высокотехнологичные компании вряд ли станут выпускать оборудование и ПО для этого сегмента, даже если будет спрос.

Во-вторых, контрметоды являются составной частью защиты информации. Везде, где имеется подлежащая защите конфиденциальная информация, должны использоваться методы для предотвращения ее утечки. Часть этих методов по борьбе с утечками ориентированы на исключение или затруднение восстановления информации противником.

В-третьих, право граждан на тайну частной жизни (приватность) может обеспечиваться в числе прочих и компьютерно-техническими мерами, которые фактически являются мерами ***контр-криминалистическими.*** Правда, применение слишком сложных средств и методов здесь невозможно, поскольку указанная самозащита гражданами своего права на тайну частной жизни ограничена квалификацией среднего пользователя. Соответствующие методы не могут требовать высокой квалификации в области ИТ, соответствующие программы должны быть просты в управлении и работать под ОС «Windows», соответствующее оборудование не может быть дорогим. Поэтому здесь обычно ограничиваются довольно примитивной защитой.

Видно, что значительная часть анти-криминалистической техники – непрофессиональная, а то и вовсе кустарная. Видно, что анти-криминалистический рынок значительно меньше криминалистического. В случае если анти-криминалистическая продукция окажется недоброкачественной, предъявлять претензии к производителю, скорее всего,

будет некому. Для преуспевания на этом рынке вовсе не требуется выпускать качественное, сложное оборудование и ПО. Требуется лишь хорошо рекламировать свою продукцию или услуги. Чем производители и занимаются.

К защитным анти-криминалистическим средствам можно отнести следующие:

- программы и аппаратно-программные устройства для шифрования хранимой информации;
- программы и аппаратно-программные устройства для шифрования трафика;
- программы для очистки дисков и других носителей;
- программы для удаления информации;
- устройства для механического уничтожения информации на магнитных носителях;
- программы для сокрытия присутствия информации на диске (манипуляция с атрибутами файлов, запись в нестандартные места, стеганография);
- системы и сервисы для анонимизации сетевой активности;
- программы и аппаратно-программные устройства для затруднения копирования произведений, представленных в цифровой форме;
- программы для затруднения исследования исполняемого кода и алгоритмов программ.

Основные выводы

Цифровая криминалистика – это прикладная наука о расследовании преступлений (инцидентов) и сборе цифровых доказательств, находящихся на компьютерах, системах хранения данных, в компьютерных сетях, на

мобильных и других цифровых устройствах, о методах получения и исследования доказательств, имеющих форму компьютерной информации (так называемых цифровых доказательств), о применяемых для этого технических средствах.

Задачей цифровой криминалистики является сохранение, идентификация, извлечение и документирование цифровых доказательств.

Сфера применения форензики: анализ и расследование событий, в которых фигурируют компьютерная информация как объект посягательств, компьютер как орудие совершения преступления.

Выделяют три направления компьютерных преступлений: преступления против информационной безопасности; преступления, где электронная информация является средством совершения другого преступления; преступления, совершаемые с использованием компьютерной и иной электронной техники.

Виды цифровой криминалистики: компьютерная криминалистика, сетевая криминалистика, мобильная криминалистика.

Задачи цифровой криминалистики: разработка тактики оперативно-розыскных мероприятий (ОРМ) и следственных действий, связанных с компьютерной информацией; создание методов, аппаратных и программных инструментов для сбора и исследования доказательств компьютерных преступлений; установление криминалистических характеристик правонарушений, связанных с компьютерной информацией.

Предметы цифровой криминалистики: информационные технологии, методы изучения прикладного программного обеспечения, криминальная, оперативная, следственная и судебная практика по компьютерным преступлениям, методы исследования работы систем.

Методы исследования криминалистики разделяются на общенаучные (наблюдение, описание, сравнение, обобщение, экстраполяция,

моделирование) и специальные (собственно - криминалистические и основанные на данных других наук).

Компьютерный криминалист вполне может обойтись без специальной криминалистической техники. Компьютер сам по себе – достаточно универсальный инструмент. Но специальная техника сильно облегчает работу.

Криминалистические информационные системы облегчают и/или ускоряют оформление различных документов для ОРМ; позволяют быстрее найти необходимые нормативные акты, комментарии, прецеденты, получить консультации; облегчают и ускоряют доступ ко всевозможным базам данных, учетам, справочникам – как публичным, так и закрытым; ускоряют и автоматизируют проведение ОРМ, связанных с перехватом сообщений.

Контр-форензика – это противодействие методам поиска, обнаружения и закрепления цифровых доказательств. Значительная часть анти-криминалистической техники – непрофессиональная, а то и вовсе кустарная. Анти-криминалистический рынок значительно меньше криминалистического.

Вопросы для самоконтроля

1. *Что означает термин «форéнзика»?*
2. *Основная задача цифровой криминалистики.*
3. *Назовите три направления компьютерных преступлений.*
4. *Приведите виды цифровой криминалистики.*
5. *Что являются предметами цифровой криминалистики?*
6. *Перечислите сферы применения форензики.*
7. *Сформулируйте группы преступления, совершаемые с применением средств информации.*

8. *Какие задачи решает цифровая криминалистика с учетом проблемы технического и правового характера?*
9. *Как влияют передовые достижения техники и технологии на преступность?*
10. *Назовите методы исследования криминалистики.*
11. *Охарактеризуйте специальные технические средства цифровой криминалистики.*
12. *Для чего предназначены экспертные программы в цифровой криминалистики?*
13. *Раскройте суть криминалистической фотосъемки и видеозаписи.*
14. *Задачи криминалистических информационных систем.*
15. *Сформулируйте понятие контр-форензика?*

2. КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

2.1. Основные направления компьютерных преступлений

В начала 90-х годов в деятельности зарубежных правоохранительных органов все чаще встречается такой термин, как **«computercrime»-компьютерные преступления**, т.е. преступления, связанные с использованием компьютера.

Термин «компьютерные преступления» несколько шире, чем «*преступления в сфере компьютерной информации*». Он также охватывает те преступления, где компьютерная техника, программы, компьютерная информация и цифровые каналы связи являются орудиями совершения преступления или объектом посягательства. К таким преступлениям относятся: мошенничество с применением банковских карт **(кардинг),** мошенничество с выманиванием персональных данных **(фишинг),** незаконное пользование услугами связи и иной обман в области услуг связи **(фрод, кража трафика),** промышленный и иной шпионаж, когда объектом являются информационные системы, и т.д.

Компьютерным можно называть любое преступление, для раскрытия которого используются методы компьютерной криминалистики. В зарубежной литературе и во многих официальных документах вместо «computer crime» также часто употребляется термин «cybercrime» – киберпреступность, киберпреступление.

Часто используют следующее определение:

Компьютерное преступление (киберпреступление*)* – уголовное правонарушение, для расследования которого существенным условием является применение специальных знаний в области информационных технологий.

Компьютер и компьютерная информация могут играть три роли в компьютерных преступлениях:

- объект посягательства;
- орудие совершения;
- доказательство или источник доказательств.

Во всех трех случаях требуются специальные знания и специальные методы для обнаружения, сбора, фиксации и исследования доказательств.

Проблема обеспечения информационной безопасности актуальна с тех пор, как люди стали обмениваться информацией, накапливать ее и хранить. Во все времена возникала необходимость надежного сохранения наиболее важных достижений человечества. Аналогично возникала необходимость обмена конфиденциальной информацией и надежной ее защиты.

Компьютерные преступления - это предусмотренные уголовным кодексом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть.

Компьютерные преступления условно можно разделить на две большие категории:

- преступления, связанные с вмешательством в работу компьютеров;
- преступления, использующие компьютеры как необходимые технические средства.

Перечислим основные виды преступлений, связанные *с вмешательством в работу компьютеров.*

1) Несанкционированный доступ (НСД) к информации. НСД осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и

информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакер, «компьютерный пират», - лицо, совершающее систематические несанкционированные доступы в компьютерные системы и сети с целью развлечения, мошенничества или нанесения ущерба (в том числе и путем распространения компьютерных вирусов). С одной стороны «хакер» - это человек, который прекрасно знает компьютер и пишет хорошие программы, а с другой, - незаконно проникающий в компьютерные системы с целью получения информации.

Английский глагол «to hack» применительно к компьютерам может означать две вещи - взломать систему или починить ее. В основе этих действий лежит нечто общее - понимание того, как устроен компьютер и программы, которые на нем работают.

Таким образом, слово «хакер» совмещает в себе, по крайней мере, два значения: одно - окрашенное негативно («взломщик»), другое - нейтральное или даже хвалебное («ас», «мастер»). Другими словами, хакеров можно разделить на «плохих» и «хороших».

«Хорошие» хакеры двигают технический прогресс и используют свои знания и умения на благо человечества. Ими разработано большое число новых технических и программных систем. Им, как водится, противостоят «плохие»: они читают чужие письма, воруют чужие программы и всеми доступными способами вредят прогрессивному человечеству.

«Плохих» хакеров можно условно разделить на четыре группы.

Первая - **любители**, состоящая в основном из молодежи, - люди, взламывающие компьютерные системы просто ради собственного удовольствия. Они не наносят вреда, а такое занятие весьма полезно для них самих - со временем из них получаются превосходные компьютерные специалисты.

Вторая группа - **пираты.** Они взламывают защиту компьютеров для похищения новых программ и другой информации.

Третья группа - **хакеры**, использующие свои познания действительно во вред всем и каждому. Они уничтожают компьютерные системы, в которые им удалось прорваться, читают чужие письма, а потом издеваются над их авторами. Когда читаешь в телеконференциях их рассказы о взломах, складывается впечатление, что это люди с ущемленным чувством собственного достоинства. Есть и еще одна группа - хакеры, которые охотятся за секретной информацией по чьим-либо заказам.

Среди хакерства выделяются четыре основных типа.

Первый - ***романтики-одиночки.*** Они, как правило, взламывают базы данных из чистого любопытства. В целом они довольно безопасны и бескорыстны, но и наиболее талантливы. Поэтому массовые взломы компьютерных сетей какой-либо фирмы обычно начинаются после того, как на нее набредет кто-то из «романтиков» и похвастается этим в своей сети.

Второй - ***прагматики, или классики.*** Работают как в одиночку, так и группами. Воруют, как говорится, что придется - игры, программы, электронные версии разных изданий.

Третий - ***разведчики.*** Сегодня в любой уважающей себя фирме имеется хакер, оформленный обычно как программист. Его задача - взламывать сети конкурентов и красть оттуда самую разную информацию. Этот тип пользуется сейчас наибольшим спросом.

Четвертый - ***кибергангстеры.*** Это уже профессиональные компьютерные бандиты. Их задачи конкретные - блокировка и развал работы компьютерных сетей, а также кража денег с банковских счетов. Дело это дорогое и небезопасное, зато самое высокооплачиваемое.

2) Ввод в программное обеспечение «логических бомб». Они срабатывают при выполнении определенных условий и частично или

полностью выводят из строя компьютерную систему.

«Временная бомба» - разновидность «логической бомбы», которая срабатывает по достижении определенного момента времени.

Способ *«троянский конь»* состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять прежнюю работоспособность. С помощью «троянского коня» преступники, например, отчисляют на свой счет определенную сумму с каждой операции.

Есть еще одна разновидность «троянского коня». Ее особенность стоит в том, что в безобидно выглядящий кусок программы вставляются не команды, собственно выполняющие «грязную» работу, а команды, формирующие эти команды и после выполнения уничтожающие их. В этом случае программисту, пытающемуся найти «троянского коня», необходимо искать не его самого, а команды, его формирующие. Развивая эту идею, можно представить себе команды, которые создают команды и т.д. (сколь угодно большое число раз), создающие «троянского коня».

3) Разработка и распространение компьютерных вирусов.

4) Преступная небрежность при разработке, изготовлении и эксплуатации программно-вычислительных комплексов. Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима.

5) Подделка компьютерной информации. Этот вид компьютерной преступности является одним из наиболее свежих. Он является разновидностью несанкционированного доступа с той разницей, что

пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, причем имеющий достаточно высокую квалификацию. Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосований, референдумов и т.п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

6) Хищение компьютерной информации. Если «обычные» хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться.

2.2. Классификация компьютерных преступлений

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. Ниже приведены названия способов совершения подобных преступлений, соответствующие кодификатору Генерального Секретариата Интерпола. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен Национальное центральное бюро (НЦБ) более чем 100 стран.

Все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы Q. Для характеристики преступлений может использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

QA - Несанкционированный доступ и перехват:

QAH - *компьютерный абордаж,*

QAI - *перехват,*

QAT - *кража времени,*

QAZ - *прочие виды несанкционированного доступа и перехвата.*

QD - Изменение компьютерных данных:

QDV - *компьютерный вирус,*

QDT - *троянский конь,*

QDW - *компьютерный червь,*

QDZ - *прочие виды изменения данных.*

QF - Компьютерное мошенничество:

QFC - *мошенничество с банкоматами,*

QFF - *компьютерная подделка,*

QFG - *мошенничество с игровыми автоматами,*

QFM - *манипуляции с программами ввода-вывода,*

QFP - *мошенничества с платежными средствами,*

QFT - *телефонное мошенничество,*

QFZ - *прочие компьютерные мошенничества.*

QR - Незаконное копирование:

QRG - *компьютерные игры,*

QRS - *прочее программное обеспечение,*

QRT - *топография полупроводниковых изделий,*

QRZ - *прочее незаконное копирование,*

QS - Компьютерный саботаж:

QSH - *с аппаратным обеспечением,*

QSS - *с программным обеспечением,*

QSZ - *прочие виды саботажа,*

QZ - Прочие компьютерные преступления:

QZB - *с использованием компьютерных досок объявлений,*

QZE - *хищение информации, составляющей коммерческую тайну,*

QZS - *передача информации конфиденциального характера,*

QZZ - *прочие компьютерные преступления*.

Кратко охарактеризуем некоторые виды компьютерных преступлений согласно приведенному кодификатору.

Несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных преступлений:

QAH - *«Компьютерный абордаж» (хакинг - hacking)* - доступ в компьютер или сеть без права на то. Этот вид компьютерных преступлений обычно используется хакерами для проникновения в чужие информационные сети.

QAI - *перехват (interception)* - перехват при помощи технических средств без права на то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств.

При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи.

Для характеристики методов несанкционированного доступа и перехвата информации используется следующая специфическая терминология:

- *"Жучок" (bugging)* характеризует установку микрофона в

компьютере с целью перехвата разговоров обслуживающего персонала;

- *"Откачивание данных" (data leakage)*отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе;
- *"Уборка мусора" (scavening)* характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.д. Электронный вариант требует исследования данных, оставленных в памяти машины;
- *"За дуракам" (piggbacking),* характеризующий несанкционированное проникновение как в пространственные, так и в электронные закрытые зоны. Его суть: если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним;
- *"За хвост" (between the lines entry),* используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний закончит активный режим, осуществлять доступ к системе;
- *"Неспешного выбора" (browsing).* В этом случае НСД к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости;
- *"Поиск бреши" (trapdoor entry),* при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;
- *"Люк" (trapdoor),* являющийся развитием предыдущего. В найденной

"бреши" программа "разрывается", и туда вставляется определенное число команд. По мере необходимости "люк" открывается, а встроенные команды автоматически осуществляют свою задачу;

- *"Маскарад" (masquerading).* В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;
- *"Мистификация" (spoofing),* который используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коду пользователя.

Изменение компьютерных данных (QD) включает в себя следующие виды преступлений:

QDL/QDT - логическая бомба (logic bomb), троянский конь (trojan horse) - изменение компьютерных данных без права на то путем внедрения логической бомбы или троянского коня.

Логическая бомба заключается в тайном встраивании в программа набора команд, который должен сработать лишь однажды, но при определенных условиях.

Троянский конь заключается в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

QDV - вирус (virus) - изменение компьютерных данных или программ без права на то путем внедрения или распространения компьютерного вируса.

Компьютерный вирус - это специально написанная программа, которая может «приписать» себя к другим программам (т.е. «заражать» их),

размножаться и порождать новые вирусы для выполнения различных нежелательных действий на компьютере.

QDW - ***червь*** - изменение компьютерных данных или программ без права на то путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть.

Компьютерные мошенничества (QF) объединяют в своем составе разнообразные способы совершения компьютерных преступлений:

QFC - компьютерные мошенничества, связанные с хищением наличных денег из банкоматов.

QFF - компьютерные подделки - мошенничества и хищения из компьютерных систем путем создания поддельных устройств.

QFG - мошенничества и хищения, связанные с игровыми автоматами.

QFM - манипуляции с программами ввода-вывода - мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них путем манипуляции программами. В этот вид компьютерных преступлений включается метод подмены данных кода (data diddling code change), который обычно осуществляется при вводе-выводе данных. Это простейший и потому очень часто применяемый способ.

QFP - компьютерные мошенничества и хищения, связанные с.платежными средствами. К этому виду относятся самые распространенные компьютерные преступления, связанные с кражей денежных средств, которые составляют около 45% всея преступлений, связанных с использованием ЭВМ.

QFT - телефонное мошенничество - доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.

Незаконное копирование информации (QR) составляют следующие виды компьютерных преступлений:

QRG/QRS - незаконное копирование, распространение или опубликование компьютерных игр и другого программного обеспечения, защищенного законом.

QRT - незаконное копирование топографии полупроводниковых изделий - копирование, без права на то защищенной законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью без права на то топографии или самого полупроводникового изделия, произведенного с использованием данной топографии.

Компьютерный саботаж (QS) составляют следующие виды преступлении:

QSH - саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ; вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы.

QSS - компьютерный саботаж с программным обеспечением - стирание, повреждение, ухудшение или подавление компьютерных данных или программ без права на то.

К прочим видам компьютерных преступлений (QZ) в классификаторе отнесены следующие:

QZB - использование электронных досок объявлений (BBS) для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности;

QZE -хищение информации, составляющей коммерческую тайну - приобретение .незаконными средствами или передача информации, представляющей коммерческую тайну без права на то или другого иконного обоснования с намерением причинить экономический ущерб иди получить незаконные экономические преимущества;

QZS - использование компьютерных систем или сетей для хранения,

обмена, распространения или перемещения информации конфиденциального характера.

2.3. Типичные образы компьютерных преступников

Оценивая вероятного преступника, важнее всего установить уровень его компетенции в области ИТ. Когда квалификация подозреваемого неизвестна, ее следует предполагать высокой.

С той же целью специалисту или следователю имеет смысл до поры скрывать свой собственный уровень познаний в ИТ перед подозреваемым. Приведем пример. Изымая компьютер во время обыска (если застали его включенным), специалист должен решить, следует ли применить штатную процедуру выключения или выключить компьютер грубым прерыванием электропитания. С одной стороны, при грубом обесточивании может пропасть некоторое количество данных, как правило, не очень существенных. Но лучше бы их сохранить. С другой стороны, у некоторых хакеров (в дурном значении этого слова) есть противная привычка оснащать свой компьютер логической бомбой, срабатывание которой связано с командой выключения компьютера (shutdown). Поэтому при использовании штатного выключения есть риск уничтожить все улики собственными руками. Какой вариант выбрать, зависит от того, как мы оцениваем уровень квалификации владельца компьютера. При невозможности оценить этот уровень компьютер выключается прерыванием электропитания, то есть в расчете на наличие логической бомбы.

Приведем описание нескольких типичных образов компьютерных преступников:

1. «Хакер». Основной мотивацией этого типа нарушителей являются: исследовательский интерес, любопытство, стремление доказать свои

возможности, честолюбие. Средства защиты компьютерной информации, ее недоступность они воспринимают как вызов своим способностям. Некоторые исследователи полагают необходимой чертой этого типа хорошие знания в области ИТ и программирования.

2. «Инсайдер». Несколько более распространенным типом компьютерного злоумышленника является человек, не слишком хорошо владеющий знаниями в области ИТ, зато владеющий доступом в информационную систему (ИС) в силу служебного положения. Уже стало общим местом утверждение, что большая часть «взломов» компьютерных систем совершается изнутри. Это действительно так. Поэтому при расследовании неправомерного доступа «инсайдер» – первая версия, которую следует рассматривать. Даже если неправомерный доступ был явно снаружи, скорее всего, он стал возможным из-за сговора с местным сотрудником.

Типичный «инсайдер» совершает компьютерное преступление (лично или в форме подстрекательства, совместно с «внешним» соучастником) с использованием сведений, полученных в силу служебного положения.

3. «Белый воротничок». Этот тип преступника представляет собой давно и хорошо известного казнокрада, но только сменившего инструменты своей деятельности на компьютер. Украсть у государства или у частной компании можно сотней способов. Кроме банального хищения здесь возможны взятки, коммерческий подкуп, незаконное использование информации, составляющей коммерческую тайну, различные виды мошенничества и так далее. В отличие от «инсайдера», этот тип злоумышленника имеет минимальную квалификацию в сфере ИТ и компьютер как орудие совершения преступления не использует. Компьютер здесь выступает только как носитель следов, доказательств совершения преступления.

По своим мотивам «белые воротнички» могут быть разделены на три группы:

1) Злоупотребляющие своим служебным положением из чувства обиды на компанию или начальство. Их следует искать среди долго проработавших сотрудников.
2) Беспринципные расхитители, не имеющие моральных барьеров и ворующие только потому, что представилась такая возможность. Для подобных «белых воротничков» характерен недолгий срок службы на должности до начала злоупотреблений.
3) Квазивынужденные расхитители, попавшие в тяжелое материальное положение, в материальную или иную зависимость от лица, требующего совершить хищение или мошенничество. Как правило, подобные проблемы трудно скрыть от окружающих – крупный проигрыш, наркомания, семейный кризис, неудачи в бизнесе. Эта группа расхитителей менее осторожна, они не могут долго подготавливать свои преступления, как это делают первые и вторые.

4. «E_бизнесмен». Этот тип вероятного преступника не является квалифицированным ИТ-специалистом и не имеет служебного положения, которым можно злоупотребить. С самого начала он планирует именно криминальное предприятие, отлично осознаёт его противозаконность. Решение совершить правонарушение именно в компьютерной (сетевой) среде, а не в офлайне он принял не из-за своих особых знаний в этой области и не из-за внутренней тяги к компьютерам, а исключительно на основе рационального анализа. Чертой личности «е-бизнесмена» является наличие организаторских способностей и предпринимательской инициативы.

5. «Антисоциальный тип». Также отмечались интернет мошенники, которые руководствовались не только извлечением прибыли. Более того, их

преступный доход часто бывал меньше, чем средняя зарплата специалиста той же квалификации. Мотивом для совершения мошенничества являлась антисоциальная психопатия (*социопатия*) таких лиц и их патологическая тяга к ведению подобных «игр».

Социопатия признана отдельным видом психического расстройства и обычно такие типы действуют импульсивно и не склонны к планированию, особенно долгосрочному. Подобное расстройство вообще часто приводит к совершению преступления, не только компьютерного, причем мошенничества чаще, чем насилия.

2.4. Способы совершения компьютерных преступлений

Под способом совершения преступления обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить наиболее оптимальные методы решения задач раскрытия преступления.

Способы совершения компьютерных преступлений можно классифицировать на пять основных групп:

1. Изъятие средств компьютерной техники.
2. Перехват информации.
3. Несанкционированный доступ.
4. Манипуляция данными и управляющими командами.
5. Комплексные методы.

К первой группе относятся традиционные способы совершения

обычных видов преступлений, в которых действия преступника направлены на изъятие чужого имущества. Характерной отличительной чертой данной группы способов совершения компьютерных преступлений будет тот факт, что в них средства компьютерной техники будут всегда выступать только в качестве предмета преступного посягательства.

Ко второй группе относятся способы совершения компьютерных преступлений, основанные на действиях преступника, направленных на получение данных и машинной информации посредством использования методов аудиовизуального и электромагнитного перехвата (Рис.5).

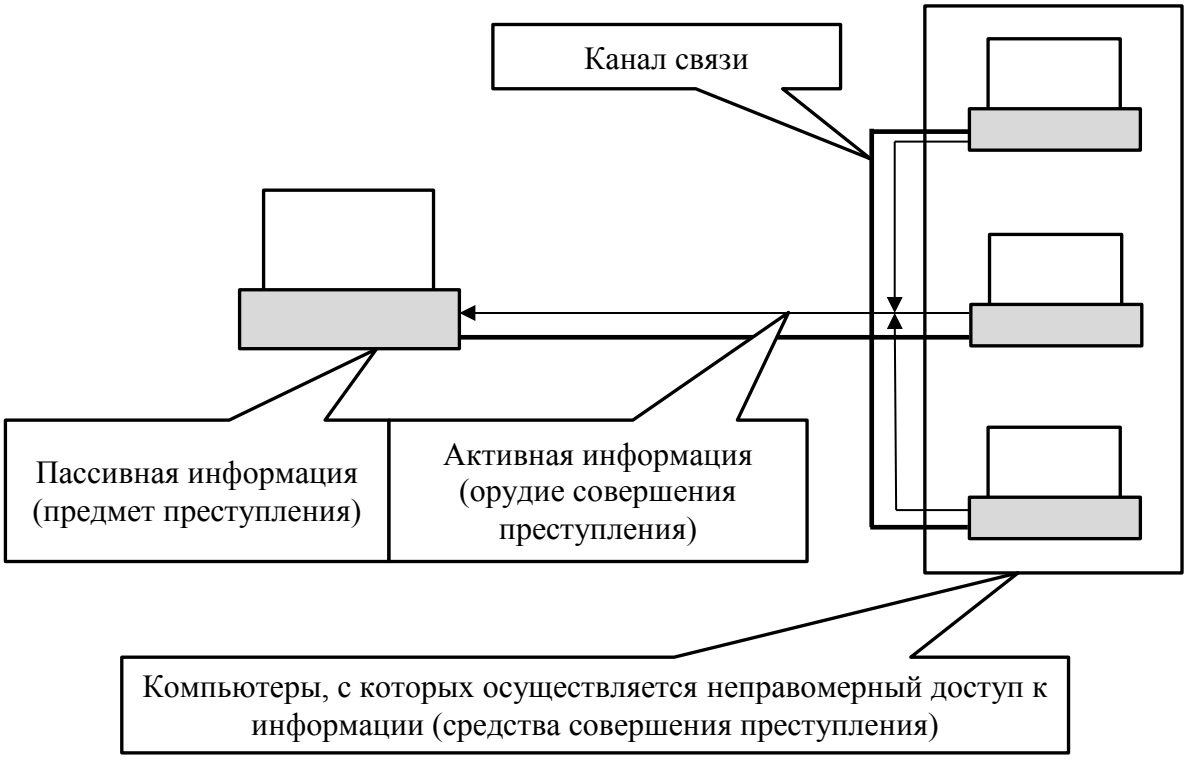


Рис.5. Активный и пассивный перехват

Активный перехват (interception) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера, например линии принтера или телефонному проводу канала связи, либо

непосредственно через соответствующий порт персонального компьютера.

Пассивный перехват (электромагнитный, electromagnetic pickup) основан на фиксации электромагнитных излучений, возникающих при функционировании многих средств компьютерной техники, включая и средства коммуникации. Так, например, излучение электронно-лучевой трубки дисплея можно принимать с помощью специальных приборов на расстоянии до 1000 м.

Аудиоперехват или снятие информации по виброакустическому каналу является опасным и достаточно распространенным способом и имеет две разновидности. Первая заключается в установке подслушивающего устройства в аппаратуру средств обработки информации, вторая - в установке микрофона на инженерно-технические конструкции за пределами охраняемого помещения (стены, оконные рамы, двери и т.п.).

Видеоперехват осуществляется путем использования различной видеооптической техники.

“Уборка мусора” (s*cavening)* представляет собой достаточно оригинальный способ перехвата информации. Преступником неправомерно используются технологические отходы информационного процесса, оставленные пользователем после работы с компьютерной техникой. Например, даже удаленная из памяти и с жестких дисков компьютера, а также дискет информация подлежит восстановлению и несанкционированному изъятию с помощью специальных программных средств.

К третьей группе способов совершения компьютерных преступлений относятся действия преступника, направленные на получение НСД к информации. К ним относятся следующие способы:

1.“Компьютерный абордаж” (*hacking*). Этот способ НСД в компьютер или компьютерную сеть без права на то, используется хакерами

для проникновения в чужие информационные сети.

Преступление осуществляется чаще всего путем случайного перебора абонентного номера компьютерной системы с использованием модемного устройства. Иногда для этих целей используется специально созданная программа автоматического поиска пароля. Алгоритм ее работы заключается в том чтобы, учитывая быстродействие современных компьютеров, перебирать все возможные варианты комбинаций букв, цифр и специальных символов и в случае совпадения комбинаций символов производить автоматическое соединение указанных абонентов.

Эксперименты по подбору пароля путем простого перебора показали, что 6-ти символьные пароли подбираются примерно за 6-дней непрерывной работы компьютера. Элементарный подсчет показывает, что уже для подбора 7-ми символьных паролей потребуется от 150 дней для английского языка и до 200 дней для русского. А если учитывать регистр букв, то эти цифры надо умножить еще на 2. Таким образом, простой перебор представляется чрезвычайно трудновыполнимым. Поэтому в последнее время преступниками стал активно использоваться метод “интеллектуального перебора”, основанный на подборе предполагаемого пароля, исходя из заранее определенных тематических групп его принадлежности. В этом случае программе - *взломщику* передаются некоторые исходные данные о личности автора пароля. По оценкам специалистов, это позволяет более чем на десять порядков сократить количество возможных вариантов перебора символов и на столько же – время на подбор пароля.

Хакеры наиболее эффективно могут быть использованы на этапе сбора разведывательной информации и сведений о компьютерных сетях и системах вероятного противника.

Они уже накопили достаточный опыт в угадывании и раскрытии паролей, использовании слабых мест в системах защиты, обмане законных

пользователей и вводе вирусов, "троянских коней" и т.п. в программное обеспечение компьютеров. Искусство проникновения в компьютерные сети и системы под видом законных пользователей дает хакерам возможность стирать все следы своей деятельности, что имеет большое значение для успешной разведывательной деятельности. Имитация законного пользователя дает возможность хакеру-разведчику сформировать систему слежения в сети противника на правах законного пользователя информации.

2. “За дураком” (*piggybacking*). Этот способ используется преступником путем подключения компьютерного терминала к каналу связи через коммуникационную аппаратуру в тот момент времени, когда сотрудник, отвечающий за работу средства компьютерной техники, кратковременно покидает свое рабочее место, оставляя терминал в активном режиме.

3. “За хвост” (*between-the-lines entry*). При этом способе съема информации преступник подключается к линии связи законного пользователя и дожидается сигнала, обозначающего конец работы, перехватывает его на себя и осуществляет доступ к системе.

4. Неспешный выбор (*browsing*). При данном способе совершения преступления, преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите.

Этот способ чрезвычайно распространен среди хакеров. В Интернете и других глобальных компьютерных сетях идет постоянный поиск, обмен, покупка и продажа взломанных хакерами программ. Существуют специальные телеконференции, в которых проходит обсуждение программ - взломщиков, вопросов их создания и распространения.

5. “Брешь” (*trapdoor entry*). В отличие от “неспешного выбора”, когда производится поиск уязвимых мест в защите компьютерной системы, при данном способе преступником осуществляется конкретизация поиска:

ищутся участки программ, имеющие ошибку или неудачную логику построения. Выявленные таким образом “бреши” могут использоваться преступником многократно, пока не будут обнаружены.

6. “Люк” (*trapdoor*). Данный способ является логическим продолжением предыдущего. В месте найденной “бреши” программа “разрывается” и туда дополнительно преступником вводится одна или несколько команд. Такой “люк” “открывается” по необходимости, а включенные команды автоматически выполняются.

К четвертой группе способов совершения компьютерных преступлений относятся действия преступников, связанные с использованием методов манипуляции данными и управляющими командами средств компьютерной техники. Эти методы наиболее часто используются преступниками для совершения различного рода противоправных деяний и достаточно хорошо известны сотрудникам подразделений правоохранительных органов, специализирующихся по борьбе с компьютерными преступлениями.

Пятая группа способов– комплексные методы – включает в себя различные комбинации рассмотренных выше способов совершения компьютерных преступлений.

Следует заметить, что рассмотренная выше классификация не является, как уже говорилось выше, единственно возможной. Так, по международной классификации в отдельную группу принято выделять такие способы, как ***компьютерный саботаж*** с аппаратным или программным обеспечением, которые приводят к выводу из строя компьютерной системы. Наиболее значительные компьютерные преступления совершаются посредством порчи программного обеспечения, причем часто его совершают работники, недовольные своим служебным положением, отношением с руководством и т.д.

2.5. Виды компьютерных преступлений

Онлайн-мошенничество.

Такая форма торговли, как интернет-магазин, нашла широкое применение среди бизнесменов по целому ряду причин. Он, в частности, отличается низкими затратами на организацию торговли. Стоимость веб-сайта с соответствующим бэк-офисом не идет ни в какое сравнение со стоимостью содержания реальной торговой площади. К тому же зависимость текущих затрат интернет-магазина от его оборота если и не очень близка к пропорциональной, то значительно ближе к ней по сравнению с магазином реальным. Это значит, что при отсутствии (нехватке) покупателей убытки будут невелики. Например, цена готового, стабильно работающего интернет-магазина начинается с 15-20 тысяч долларов. По сравнению с реальным (офлайновым) магазином, тем более в крупном городе, это просто небольшие деньги. Именно эта особенность интернет-торговли привлекла сюда мошенников. Затратив относительно небольшую сумму, злоумышленник может создать видимость нормального торгового предприятия и заняться мошенничеством или обманом потребителей. Десяток-другой жертв вполне окупают сделанные затраты.

Кроме фиктивных интернет-магазинов мошенники используют и другие предлоги для получения платежей:

- лже-сайты благотворительных организаций, религиозных организаций, политических партий и движений, которые якобы собирают пожертвования;
- спам-рассылки и сайты с просьбой о материальной помощи под трогательную историю о бедной сиротке, жертве войны, заложнике и т.п.;
- сайты фиктивных брачных агентств и отдельные виртуальные

невесты;

- мошеннические онлайновые «банки» и «инвестиционные фонды», обещающие дикие проценты по вкладам;
- рассылки и сайты о якобы обнаруженных уязвимостях и черных ходах в платежных системах, позволяющие умножать свои деньги, например, переслав их на особый счет (в том числе мошенничества II порядка, построенные на том, что жертва думает, будто она обманывает обманщика);
- мошеннические сайты и рассылки, предлагающие удаленную работу (на такую чаще всего клюют сетевые эскаписты) и требующие под этим предлогом какой-либо «вступительный взнос».

Схема всех онлайн-мошенничеств такова:

– размещение (рассылка) информации;

– взаимодействие с жертвой;

– получение денежного перевода.

Все три этапа предусматривают оставление обильных следов технического характера. Хотя мошенники, очевидно, постараются предпринять меры для своей анонимизации. Относительно получения денег мошенников кроме анонимизации спасает быстрота: перевод полученных средств между различными платежными системами осуществляется достаточно быстро, но требует много времени для отслеживания.

При размещении мошенниками подложного интернет-магазина можно рассчитывать на обнаружение следующих видов следов:

– регистрационные данные на доменное имя; логи от взаимодействия с регистратором доменных имен; следы от проведения платежа этому регистратору;

– следы при настройке DNS-сервера, поддерживающего домен мошенников;

– следы от взаимодействия с хостинг-провайдером, у которого размещен веб-сайт: заказ, оплата, настройка, залив контента;

– следы от рекламирования веб-сайта: взаимодействие с рекламными площадками, системами баннерообмена, рассылка спама;

– следы от отслеживания активности пользователей на сайте.

При взаимодействии с жертвами обмана мошенники оставляют такие следы:

– следы при приеме заказов – по электронной почте, по ICQ, через вебформу;

– следы от переписки с потенциальными жертвами.

При получении денег мошенники оставляют такие следы:

– следы при осуществлении ввода денег в платежную систему (реквизиты, которые указываются жертве);

– следы при переводе денег между счетами, которые контролируются мошенниками;

– следы от дистанционного управления мошенниками своими счетами, их открытия и закрытия;

– следы от взаимодействия мошенников с посредниками по отмыванию и обналичиванию денег.

DoS и DDoS атаки.

DoS и DDoS атаки или атаки типа «отказ в обслуживании» является одним из видов неправомерного доступа, а именно такого, который приводит к блокированию информации и нарушению работы компьютерных систем и сетей. Иные виды неправомерного доступа (копирование информации, уничтожение информации), а также использование вредоносных программ могут быть этапами осуществления DoS-атаки.

Такие атаки принято разделять на два типа: атаки, использующие какие-либо уязвимости в атакуемой системе и атаки, не использующие

уязвимостей. Во втором случае своеобразным «поражающим фактором» атаки является перегрузка ресурсов атакуемой системы – процессора, ОЗУ, диска, пропускной способности канала.

В настоящее время встречаются DoS и DDoS атаки, как с личными, так и с корыстными мотивами (Рис.6).

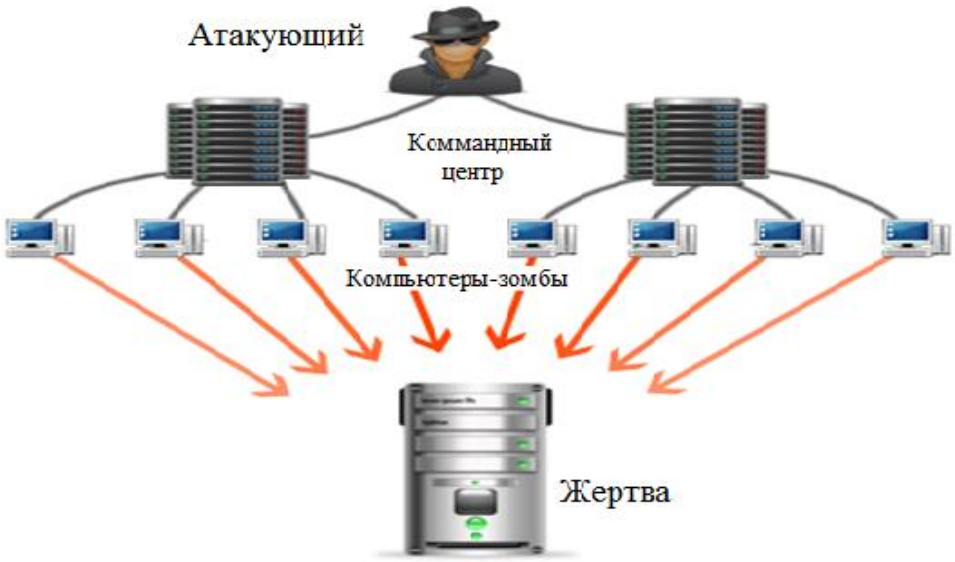


Рис.6. Архитектура DDOS-атаки

В начале личные мотивы превалировали. Но сейчас наблюдается четкая тенденция возрастания числа DoS атак с корыстными мотивами – в целях вымогательства или недобросовестной конкуренции.

Организовать DoS-атаку на типичный веб-сайт не представляет из себя сложной задачи, она под силу ИТ-специалисту средней квалификации, имеющему в своем распоряжении среднее же оборудование и средней ширины канал связи.

Итак, можно выделить два типа преступлений, связанных с DoS-атаками, – с целью доставить неприятности владельцу или пользователям атакуемого ресурса и с целью получить выкуп.

В первом случае, как и при клевете и оскорблениях, следует искать «обиженного». При этом непосредственным исполнителем может быть как он сам, так и нанятый профессионал.

Во втором случае мы имеем дело с хладнокровным криминальным расчетом, и преступление мало чем отличается от офлайнового вымогательства или недобросовестной конкуренции. Тип возможного преступника «е-бизнесмен» описан выше, в главе «Личность вероятного преступника». Потерпевшим в подавляющем большинстве случаев выступает юридическое лицо.

Коммерческие организации редко бывают заинтересованы в официальном расследовании, поскольку для них главное – устранить опасность и минимизировать убытки. В наказании злоумышленника они не видят для себя никакой выгоды. А участие в судебном процессе в роли потерпевшего часто негативно отражается на деловой репутации.

При подготовке и проведении DoS и DDoS атаки образуются следующие следы технического характера:

- наличие инструментария атаки – программных средств (агентов), установленных на компьютере злоумышленника или, чаще, на чужих используемых для этой цели компьютерах, а также средств для управления агентами;
- следы поиска, тестирования, приобретения инструментария;
- логи (преимущественно статистика трафика) операторов связи, через сети которых проходила атака;
- логи технических средств защиты – детекторов атак и аномалий трафика, систем обнаружения вторжений, межсетевых экранов, специализированных антифлудовых фильтров;
- логи, образцы трафика и другие данные, специально полученные техническими специалистами операторов связи в ходе расследования

инцидента, выработки контрмер, отражения атаки;

- следы от изучения подозреваемым (он же заказчик атаки) рекламы исполнителей атак, его переписки, переговоров и денежных расчетов с исполнителями;
- следы от контрольных обращений подозреваемого к атакуемому ресурсу в период атаки, чтобы убедиться в ее действенности.

Анализ аномалий в сетевом трафике – единственный эффективный метод обнаружения DDoS-атаки. С точки зрения защиты, DDoS-атаки являются одной из самых сложных сетевых угроз, поэтому принятие эффективных мер противодействия является исключительно сложной задачей для организаций, деятельность которых зависит от интернета. DDoS-атаку очень сложно выявить и предотвратить, поскольку «вредоносные» пакеты неотличимы от «легитимных». Сетевые устройства и традиционные технические решения для обеспечения безопасности сетевого периметра, такие как межсетевые экраны, маршрутизация в «черные дыры» и системы обнаружения вторжений (IDS), являются важными компонентами общей стратегии сетевой безопасности, однако одни эти устройства не обеспечивают полной защиты от DDoS-атак.

Маршрутизация в «черные дыры». Процесс маршрутизации в «черные дыры» применяется провайдером услуг для блокировки всего трафика, адресованного на целевой объект, в как можно более ранней точке. «Снятый с маршрута» трафик маршрутизируется в «черную дыру» для защиты сети провайдера и других его клиентов. Маршрутизацию в «черные дыры» нельзя назвать удачным решением, поскольку вместе со злоумышленным трафиком атаки отбраковываются и благонадежные пакеты. Жертвы полностью лишаются своего трафика, и хакер празднует победу.

Реакция на атаки DDoS-атаки. Процедуры защиты от атак DDoS, инициируемые вручную, можно охарактеризовать словами «слишком мало,

слишком поздно». Первая реакция жертвы на атаку DDoS, как правило, заключается в том, что он просит ближайшего предшествующего провайдера услуг соединения (это может быть провайдер Интернет-услуг, провайдер услуг хостинга или магистральный) попытаться идентифицировать источник. Если адреса подделаны или их слишком много, этот процесс может оказаться долгим и трудным, и для его реализации будет необходимо объединить усилия многих провайдеров. Хотя источник, возможно, и будет идентифицирован, блокировка этого источника выльется в блокировку всего трафика – и плохого, и хорошего.

Анализ аномалий в сети. Во время обнаружить DDoS-атаку – в этом и заключается главная проблема, если мы не хотим бороться с ней по факту падения ресурсов сети. Наиболее эффективный способ обнаружить DDoS-атаку основан на накоплении статистических данных о прохождении трафика в сети. В качестве источника данных для статистики можно использовать сам трафик или некоторую статистическую информацию о нем. Для этого используются либо дополнительные сенсоры, устанавливаемые на сеть, либо информация, которую могут предоставить существующие сетевые элементы. В случае снятия такой информации непосредственно с маршрутизаторов обычно используется протокол Netflow. Этот протокол был в свое время разработан для оптимизации работы маршрутизаторов, его задача заключалась в том, чтобы не обрабатывать каждый пакет, а перенаправлять его как можно быстрее, если он соответствовал требованиям потока. Протокол оказался неэффективным для решения основной задачи, но очень пригодился для борьбы с DDoS-атаками и шире - для анализа работы сети.

Такие способности протоколу дает заложенная в него возможность формировать таблицу, в которой в динамическом режиме прописываются все статистические данные по пришедшим потокам и пакетам: откуда пришел пакет, куда он направляется, какой у него протокол, порт, какое количество

данных передано. Причем имеется возможность экспорта статистических данных во внешние системы для последующего анализа.

Ситуация, при которой текущий трафик на защищаемый ресурс резко отличается от нормального, считается DDoS-атакой. Стоит подчеркнуть, что система распознает только отклонение от трафика, а чем он вызван – всплеском легитимных обращений к ресурсам (выложили новый патч, прошла рекламная кампания) или DDoS-атакой – может определить только владелец ресурса, ожидал ли он такой объем обращений или нет.

После обнаружения факта аномалии происходит ее классификация и определяется, насколько она серьезна. Если DDoS-атака не грозит возникновением проблем в сети, то лучше наблюдать и ничего не предпринимать, так как возникает вероятность не пустить на ресурс законного пользователя.

Общая схема противодействия DDoS-атакам представлена на рис.7.

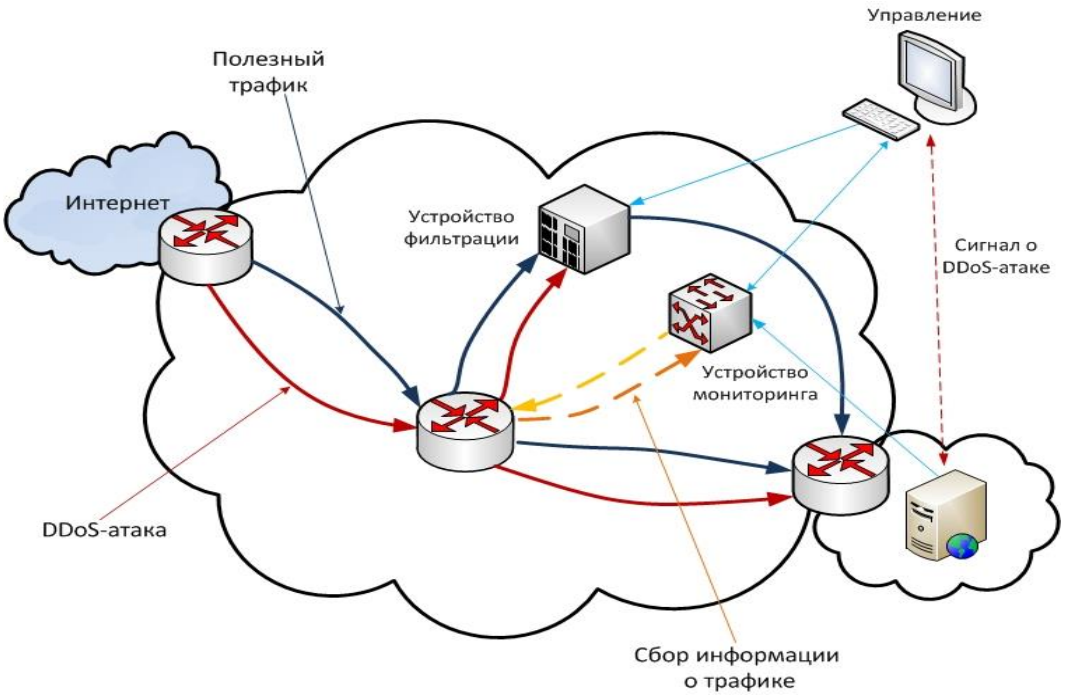


Рис.7. Схема противодействия DDoS-атакам

Техническая реализация данного решения предполагает наличие в сети двух дополнительных устройств, одно из которых осуществляет мониторинг входящего трафика и выявляет проведение DDoS-атаки, а второе фильтрует (очищает) поступающий извне трафик. В нормальном режиме работы данные устройства не должны оказывать никакого влияния на проходящий трафик.

В случае же атаки устройство «очистки» задерживает трафик, идентифицируемый как DDoS-пакеты, не допуская его попадания в относительно узкополосные клиентские каналы и на клиентские ресурсы, тем самым не прерывая предоставление клиенту основной услуги.

Вредоносные программы.

Антивирусные аналитики отмечают явную тенденцию к коммерциализации вредоносного ПО. Еще 10-15 лет назад почти все вирусы и черви создавались без явной корыстной цели, как полагают, из хулиганских побуждений или из честолюбия.

Среди современных вредоносных программ большинство составляют программы, заточенные под извлечение выгоды. Основные их разновидности (с точки зрения предназначения) следующие:

- **троянские программы** для создания зомби-сетей, которые затем используются для рассылки спама, DoS-атак, организации фишерских сайтов и т.п.; нередко они снабжены механизмом самораспространения;
- так называемое **spyware**, то есть черви и троянцы для похищения персональных данных – паролей и ключей к платежным системам, реквизитов банковских карточек и других данных, которые можно использовать для мошенничества или хищения;
- так называемое **adware**, то есть вредоносные программы, скрытно внедряющиеся на персональный компьютер и показывающие пользователю несанкционированную рекламу (иногда к классу

adware причисляют не только вредоносные, но и «законопослушные» программы, которые показывают рекламу с ведома пользователя);

- **руткиты,** служащие для повышения привилегий пользователя и сокрытия его действий на «взломанном» компьютере;
- **логические бомбы**, которые предназначены для автоматического уничтожения всей чувствительной информации на компьютере в заданное время или при выполнении (при невыполнении) определенных условий;
- так называемое **«ransomware»** – подвид троянских программ, которые после скрытного внедрения на компьютер жертвы шифруют файлы, содержащие пользовательскую информацию, после чего предъявляют требование об уплате выкупа за возможность восстановления файлов пользователя.

Как современная вредоносная программа является лишь средством, технологическим элементом для криминального бизнеса, так и современный вирусописатель работает не сам по себе, а исполняет заказы других. Это может быть прямой заказ, когда ***программист-вирмейкер*** получает техническое задание, исполняет его и отдает готовый продукт заказчику. Это может быть непрямой заказ, когда вирмейкер, зная потребности черного рынка, старается их удовлетворить своим продуктом, который затем и реализует (лицензирует пользователям) самостоятельно.

Давно не отмечалось случаев, когда один человек исполнял весь преступный замысел целиком – писал вредоносную программу, применял ее, использовал результат применения для извлечения дохода.

Таким образом, ***создатель*** вредоносной программы – это почти всегда член преступной группы. Его деятельность не имеет смысла в отрыве от заказчиков и пользователей вредоносной программы.

Кроме создания вредоносных программ уголовно наказуемо и их

применение. Лицо, использующее такую программу, тоже в большинстве случаев не реализует результаты своего труда непосредственно, а продает или передает их дальше, другим членам преступной группы.

Наконец, третий тип – это ***реализаторы*** результатов применения вредоносных программ, то есть **спамеры, вымогатели, кардеры, мошенники.**

Приведем примеры типичных криминальных «коллективов».

Спамеры. Первый сообщник создает и совершенствует ПО для скрытного внедрения на компьютеры пользователей (троянцы). Второй, купив у первого право на использование указанной программы, рассылает ее в массовом порядке, принимает сигналы и учитывает успешно внедрившиеся экземпляры троянцев, объединяет их в структурированную зомби-сеть. Готовую сеть (целиком или частично, насовсем или на время) он продает третьему сообщнику, который с ее помощью осуществляет рассылку спама. Заказы на рассылки принимает четвертый сообщник, который ищет заказчиков при помощи того же спама, часть полученных от заказчиков денег перечисляет третьему в оплату его услуг. Пятый занимается сбором и верификацией адресов электронной почты для рассылок. Собранные базы адресов (или подписку на такие базы) он продает либо четвертому, либо третьему сообщнику.

Кардеры. Первый из сообщников занимается *сбором* атрибутов банковских карт. Он может служить продавцом или официантом и незаметно снимать данные с карточек клиентов. Он может быть менеджером в фирме или банке и получать доступ к базе данных карточек в силу служебного положения. Он может получать номера карточек, внедряя вредоносные программы шпионы (spyware) или через фишинг. Добыв некоторое количество номеров (или даже дампов) банковских карт, первый сообщник сбывает их второму. Второй исполняет роль *организатора* криминального

бизнеса.

Он аккумулирует у себя данные и распределяет их исполнителям. Третий сообщник *исполняет* по заказам второго верификацию реквизитов карт, то есть проверяет их действительность и пригодность для платежей. Четвертый сообщник *создает* и поддерживает платный веб-сайт или лже-магазин или интернет-казино с возможностью оплаты услуг карточками. Он имеет несколько договоров с биллинговыми компаниями, время от времени меняет их, а также свою вывеску. Это механизм для отмывания денег. Пятая группа сообщников – так называемые *набивщики*. Они получают от второго партии номеров банковских карт по нескольку десятков и вводят их через отмывочное предприятие четвертого сообщника под видом разных клиентов. При этом они должны при помощи технических средств эмулировать доступ из разных стран и с разных компьютеров. За свою работу они получают сдельную оплату, реже – процент с доходов. Шестой сообщник представляет собой иной канал реализации, он занимается так называемым вещевым *кардингом*. Получая от второго «отборные», наиболее перспективные номера кредиток, он использует их для покупок в настоящих интернет-магазинах. Покупается в основном дорогая, нетяжелая и ликвидная техника - мобильные телефоны, видеокамеры, компьютерные комплектующие и т.п.

Естественно, заказываются они вовсе не на его адрес. Для получения заказов существует седьмая группа сообщников – *дропы.* Это граждане из благополучных стран, поскольку большинство интернет-магазинов не доставляют заказы вне США, Канады и ЕС, а если и доставляют, то проверяют таких покупателей очень тщательно. Работа дропов состоит в том, чтобы подтвердить по телефону сотруднику магазина, что заказ сделал он, получить посылку и тут же переслать ее шестому сообщнику (иногда – другому дропу, для пущего запутывания следов). Дропы вербуются десятками из малообеспеченных слоев общества типа студентов. Обычно

дроп выполняет всего десяток-другой операций с интервалом в несколько недель. Он получает оплату сдельно или в виде процента от стоимости товара. Наконец, восьмой сообщник занимается получением и реализацией посылок от дропов.

Фишеры. Первый сообщник занимается размещением подложных веб-сайтов банков и иных учреждений. В состав программ такого сайта входит система для моментальной отсылки введенных клиентом конфиденциальных данных злоумышленнику, естественно, не напрямую, чтобы трудно было его вычислить. Второй изготавливает эти сайты, составляет подложные письма и рассылает их, но не самостоятельно, а пользуясь для этого услугами спамеров. Третий сообщник занимается реализацией полученных данных (номера карт с пин_кодами или пароли к платежным системам) кардерам или иным криминальным структурам. Бывает, что реализацией пин-кодов преступная группа занимается самостоятельно. Тогда предусмотрен четвертый сообщник, который изготавливает «пластик», то есть копии банковских карт для офлайновых магазинов и банкоматов, а также пятая группа, которая собственно снимает из банкоматов деньги, получая для этого карты и пин-коды у четвертого.

Видно, что вредоносное ПО во всех случаях играет роль инструмента для одного из этапов большого преступного замысла. И создатель, и применитель вредоносных программ также исполняют общий замысел.

Итак, вероятный преступник по делам о создании и использовании вредоносных программ – это член преступной группы, работающий в этой группе на основе найма или за процент от дохода или как самостоятельный создатель орудий преступления. То есть с точки зрения экономики вирусописатель продает в одних случаях свою рабочую силу, в других – свой труд, а в третьих – результат своего индивидуального труда.

Как правило, это профессиональный программист, вставший на

преступный путь уже после выбора профессии. Его движущим мотивом являются деньги.

Мотивы, характерные для типа «хакер», то есть самоутверждение и исследовательский интерес, могут иметь значение лишь на первом этапе, при вовлечении его в преступную деятельность. Корыстный же мотив – всегда основной.

Звонилки (dialers). Одним из видов мошенничества является недобросовестное использование платных телефонных линий. Абонировав соответствующий номер с высокой оплатой за «разговор» со стороны вызывающего абонента, мошенники всяческими способами пытаются спровоцировать вызовы на него со стороны абонентов. Помещают этот номер в заведомо ложной рекламе, отправляют SMS и совершают исходящие вызовы с этого номера, чтобы абонент перезвонил, сами совершают звонки на свой номер, пользуясь несовершенством биллинга оператора, навязывают ложную информацию о вызовах телефонной сети, а также вставляют (загружают) этот номер во вредоносные программы-звонилки (dialer), которые заставляют модем пользователя совершать вызов.

По условиям договора оператор вызывающего абонента платит за такой звонок оператору вызываемого абонента, а потом пытается получить деньги со своего абонента.

Опишем более подробно один из самых распространенных типов такого мошенничества – с использованием вредоносной *программы-звонилки* (dialer, диалер, программа дозвона).

Но на сегодняшний день суды не признают вредоносные программы стихийной силой, а их действия – форс-мажорными обстоятельствами. Поэтому заразившимся такими программами пользователям все же приходится оплачивать звонки. Впрочем, иногда оператор связи склонен «прощать» такую задолженность абонента – не по закону, а по

справедливости.

При изготовлении вредоносных программ можно обнаружить следующие цифровые следы:

- исходный текст вредоносной программы, его промежуточные варианты, исходные тексты других вредоносных или двойного назначения программ, из которых вирмейкер заимствовал фрагменты кода;
- антивирусное ПО различных производителей, на котором создатель вредоносной программы обязательно тестирует свою, а также средства для дизассемблирования и отладки;
- программные средства для управления вредоносными программами (многие из них работают по схеме «клиент-сервер», одна из частей внедряется на компьютер жертвы, а другая часть работает под непосредственным управлением злоумышленника);
- средства и следы тестирования работы вредоносных программ под различными вариантами ОС;
- следы контактирования с заказчиками или пользователями вредоносной программы, передачи им экземпляров и документации, оплаты.

При распространении и применении вредоносных программ можно обнаружить следующие цифровые следы:

- средства и следы тестирования работы вредоносной программы под различными вариантами ОС;
- контакты с создателем или распространителем-посредником вредоносной программы;
- программные средства для управления вредоносной программой, данные о внедрениях этой программы к жертвам, результаты деятельности (пароли, отчеты о готовности, похищенные

персональные данные);

- средства распространения вредоносной программы или контакты с теми, кто подрядился ее распространять.

Лог антивируса, а также следы деятельности вредоносной программы, будучи исследованы в ходе экспертизы, позволят эксперту категорично утверждать, что на исследуемом компьютере была установлена определенная вредоносная программа, хотя исполняемого кода этой программы и не обнаружено. Лучше поручить такую экспертизу предприятию, которое производит или обслуживает соответствующее антивирусное ПО.

Дефейс.

Данное правонарушение состоит в том, что злоумышленник тем или иным способом изменяет внешний вид публичного веб-сайта потерпевшего, чаще всего его титульную страницу. Технически это можно осуществить, получив доступ на запись к директории, где хранятся данные вебсервера. Также часто дефейс производят, воспользовавшись уязвимостью в самом веб-сервере или одном из его CGI-скриптов. Бывает, что злоумышленник изменяет веб-страницу, воспользовавшись штатной функцией, под аккаунтом одного из законных пользователей. Мотивы для дефейса порядке убывания частоты бывают следующие:

- стремление продемонстрировать публично свою квалификацию;
- политические, религиозные, иные идеологические мотивы;
- личная неприязнь, личный конфликт с потерпевшим или кем-либо из его работников;
- стремление дискредитировать владельца веб-сайта, испортить ему деловую репутацию в целях конкурентной борьбы, повлиять на его капитализацию в целях биржевой спекуляции;
- стремление продемонстрировать наличие уязвимости в ПО, привлечь к ней внимание.

Вероятный преступник соответствует модели «хакер» или реже – «инсайдер». На взломанном компьютере следов остается не много, злоумышленник старается по возможности уничтожить их. Больше следов можно найти на компьютерах, которые хакер использует в качестве промежуточных узлов для исследования атакуемого веб-сайта и доступа к нему. Также пригодятся статистические данные транзитных провайдеров. А на собственном компьютере злоумышленника следов должно быть еще больше – там должны найтись переработанная или заново изготовленная веб-страница, а также ее промежуточные варианты, средства для осуществления НСД, средства для поиска и эксплуатации уязвимостей на целевом веб-сайте и промежуточных узлах.

В противном случае акция может остаться незамеченной – измененные сайты недолго остаются в таком состоянии, владелец обычно быстро восстанавливает первоначальный вид. Следовательно, злоумышленник сразу после «взлома» или незадолго до него каким-либо способом оповестит мир о своем преступлении. Это могут быть сообщения по электронной почте, статья в телеконференции или на веб-форуме. Все эти действия оставят дополнительные следы.

Злоумышленник также будет периодически проверять результат дефейса и отслеживать реакцию общественности на него. Эти действия он может совершать со своего компьютера, без особых мер для анонимизации.

Чаще потерпевшим является юридическое лицо. Обычно предприятие-потерпевший не заинтересовано в разглашении информации об инциденте. Но если широкая огласка уже произошла, позиция потерпевшего может измениться, поскольку необходимо чем-то компенсировать ущерб деловой репутации и как-то оправдаться перед акционерами и клиентами. Быстро найти и привлечь к ответственности злоумышленника – это все-таки некоторая компенсация в плане репутации и общественных связей.

Кардерство.

Объем мошеннического рынка в области банковских карт очень велик. Его можно оценить так. В каждом банке установлен лимит приемлемых потерь при карточных операциях. Он колеблется в пределах 0,1-0,5%. Это значит, что не менее 0,1% всего мирового оборота по карточным операциям достается кардерам.

С банковскими (платежными) картами возможно несколько видов мошенничества. Их всех можно уложить в единую схему:

< **получение – распределение – реализация** >

На первом этапе данные о банковских картах получаются разнообразными способами. На втором этапе они сортируются, проверяются, классифицируются, возможно, проходят через оптовых посредников (скупка в розницу, продажа оптом, продажа в розницу). На третьем этапе данные банковских карт реализуются, то есть конвертируются в деньги.

Указанная цепочка никогда не исполняется одним человеком. Каждый из этапов связан со своими особенными навыками, опытом в соответствующей области, служебным положением, доступом к технике. Поэтому криминальная цепочка всегда включает не менее трех сообщников.

Наборы данных банковских карт, которые представляют ценность:

(1) номер, срок действия, имя владельца, код cvv или cvv.

(2) дамп карты.

(3) дамп + пин-код.

Третий вариант – самый привлекательный для кардеров. Этот набор данных можно конвертировать в наличные самым быстрым способом и получить при этом максимальную сумму.

Способы получения данных банковских карт (Рис.8):

Рис.8. Портативные считыватели, используемые мошенниками для скрытного снятия дампа карты в местах оплаты

- дистанционный неправомерный доступ к серверу, на котором такие данные хранятся или обрабатываются, например, к серверу магазина или банка – способ, наиболее часто предполагаемый несведущими людьми, но очень редко встречающийся на практике;
- доступ к таким данным с использованием своего служебного положения и недостатков в системе защиты информации предприятия – очень часто владельцы конфиденциальной информации предпринимают излишние меры защиты от внешних угроз, но пренебрегают защитой от угроз внутренних;
- (редко) перехват интернет-трафика, когда данные карты передаются в открытом виде (по протоколу HTTP или по электронной почте);
- получение данных банковских карт, или снятие дампа при обслуживании клиентов в предприятиях торговли и питания – похож на предыдущий способ, но особенность в том, что информация копируется непосредственно с карты при физическом контакте с ней;

- выманивание данных карт и иногда пин-кодов у владельцев методами фишинга;
- получение дампов и пин-кодов при помощи фальшивых банкоматов или приставок к банкоматам (скиминг);
- получение самой карточки мошенническим способом («ливанская петля» и др.);
- обычная кража карты у ее держателя (бывает, что пин_код записан на ней или на листке, лежащем в том же бумажнике).

Ниже приводятся более подробные пояснения к перечисленным способам приобретения и реализации данных банковских карт.

Скимминг (skimming). Наиболее лакомый кусок для кардеров – это полная копия (дамп) магнитной полосы карты вместе с ее пин-кодом. Такие данные позволяю снять со счета весь остаток средств плюс весь кредитный лимит. Обычно это десятки тысяч долларов. Ради подобного куша кардеры готовы на многое. Даже банковские работники, обнаружив, что имеют доступ к пин-кодам клиентов, не всегда выдерживают искушение связаться с кардерами и совместно очистить клиентские счета. В 1990 годах была популярна установка фальшивых банкоматов и торговых терминалов (Рис.9).

Рис.9. Приставка к банкомату, замаскированная подконструктивную часть

С помощью приставки, замаскированную подконструктивную часть банкомата кардеры осуществляли скрытное копирование магнитной полосы карты клиентов и снимали со счета средства.

Многие из них даже выдавали клиентам деньги или товары. Ныне такие банкоматы встречаются реже.

Более распространены «приставки» к легальным банкоматам, которые незаметно для клиента считывают данные с магнитной полосы и «подсматривают» вводимый пин-код (Рис.10,11).

Рис.10. Видеокамера, осуществляющая снятие вводимого клиентами пин-кода, замаскированная под лоток с рекламой

Рис.11. Накладка на клавиатуру банкомата, снимающая вводимый пин-код

О распространенности подобного способа говорит то, что производители банкоматов сейчас предусматривают в картоприемнике механизм для неравномерного протягивания карты. Карта втягивается в банкомат и экстрагируется из банкомата рывками, чтобы затруднить считывание магнитной полосы возможным шпионским устройством. Впрочем, ответные технические меры уже придуманы.

Реальный пластик. На кардерском жаргоне «реальным пластиком» именуются полноценные твердые копии банковских карт. На них должен присутствовать цветной рисунок, голограмма, иметься эмбоссированное (выдавленное) имя держателя и магнитная полоса с нужными данными.

Для этого способа реализации требуется дамп карты. Пин-код не нужен. По дампу изготавливается твердая копия карты. Она должна не только нести верные данные на магнитной полосе, но и выглядеть соответственно. Рисунок карты, конечно, не обязан совпадать с оригинальным, но он должен присутствовать и быть хорошего качества: не смазываться, не отслаиваться. Желательно, чтобы название банка и карты соответствовало коду (первые 6 цифр номера карты); впрочем, продавцы редко обращают на это внимание.

Белый пластик. Карта, имеющая только записанную магнитную полосу, именуется у кардеров «белым пластиком». Ее изготовление обходится совсем недорого. Однако область использования ограничена лишь банкоматами. Разумеется, необходимо знать пин-код.

Набор дамп карты + пин-код стоит на черном рынке дорого, зато с его помощью можно выжать карточный счет досуха, сняв в банкомате весь остаток и весь кредитный лимит. Многие банки ставят ограничения для банкоматных транзакций – по географии, по максимальной сумме за раз и по максимальной сумме за день. Это несколько усложняет кардерам жизнь. Карту могут успеть заблокировать и занести в стоп_лист, пока еще не все

деньги с нее сняты.

Мошенничество с трафиком. Автоматизированные системы расчетов (билинговые системы), а также средства сбора данных для таких систем (предбилинг, mediation) операторов связи всегда являлись объектом интереса мошенников, казнокрадов и прочих криминальных элементов. Изменив данные в биллинговой системе, можно осуществить мошенничество, хищение, растрату на значительную сумму. Сложность таких систем велика, доступ к ним имеют сразу многие лица из персонала и даже клиентов предприятия, поэтому всегда имеется достаточно технических возможностей получить доступ и изменить данные.

Мошенничество с данными билинга достаточно распространено. Оно распространено настолько, что существуют нормативы списания средств на такие злоупотребления. На рынке есть особые программные продукты для выявления и пресечения подобного рода действий, они именуются «fraud management systems». Само название свидетельствует о том, что речь идет не о предотвращении мошенничества вовсе, а лишь о разумном снижении убытков от такого мошенничества.

Расследование подобных преступлений требует специальных знаний в двух областях. Во-первых, в области бизнеса отрасли связи. Порядок пропуска трафика, его техническая организация, взаиморасчеты между операторами, особенности тарифов – все это область специальных знаний. Во-вторых, требуются знания в области ИТ, поскольку все билинговые системы – это компьютерные информационные системы, и организация НСД к ним является предметом соответствующих специальных знаний.

Фишинг.

Фишинг (phishing) – это выманивание у потерпевших их конфиденциальных данных методами социальной инженерии. Как правило, речь идет о номерах банковских карт, их пин-кодах, паролях к системе

управления банковским счетом (онлайн-банкинг) и другой информации, которую можно потом обратить в деньги. Наибольшей популярностью у фишеров пользуются самые распространенные банки и платежные системы: «Citi bank» «eBay» и «PayPal».

Выманивание данных происходит при помощи подложных сообщений электронной почты и/или подложных веб-сайтов. Как правило, пользователя стараются напугать, например, закрытием его счета или приостановкой оказания услуг, если он не выполнит предложенную мошенником процедуру. Часто, если не всегда, ссылаются на якобы произошедшую аварию, утрату аутентификационных данных, иные чрезвычайные обстоятельства, даже на действия мошенников-фишеров.

Хотя вероятность обмануть каждого адресата невелика, но за счет массовой рассылки и охвата огромной аудитории фишерам удается собрать некоторое количество ценных сведений с каждой рассылки. Фишинг стал экономически выгоден лишь после появления дешевых технологий спам-рассылки. Фишинг после своего возникновения стал необычайно популярен среди мошенников. Исследователи отмечают его высокую доходность, изощренность, глобальность, возможность и выгодность его использования против клиентов самых разнообразных банковских, платежных и даже некоммерческих систем.

Вишинг (vishing) аналогичен фишингу. Только вместо направления жертвы на подложный сайт ее просят позвонить по подложному телефонному номеру, который якобы принадлежит банку или другой доверяемой инстанции. В телефонном разговоре (или при автоматизированном общении с использованием тонального набора) у жертвы выманивают конфиденциальную информацию. В условиях массового перехода на IP-телефонию несложно получить в пользование анонимный трудно отслеживаемый номер телефона. Имеется также возможность

перехватить вызовы на чужой номер, то есть на подлинный номер банка.

Фарминг – разновидность фишинга. Отличие в том, что подлинный ресурс (обычно веб_сайт банка) подменяется на подложный не методами социальной инженерии, а число техническими методами – при помощи атаки на DNS, внедрения пользователю вредоносной программы и т.п. Выманивание персональных данных можно производить и более изощренным способом. Например, злоумышленник создает развлекательный ресурс. При регистрации на этом ресурсе от пользователя требуется сообщить свой адрес электронной почты, а также выбрать пароль. С некоторой вероятностью пользователь использует тот же пароль, что и для своего почтового аккаунта. Это даст возможность злоумышленнику просматривать электронную почту жертвы, в которой могут попасться конфиденциальные данные.

Киберсквоттинг. Этим термином именуется приобретение доменного имени с целью его недобросовестного использования либо с целью не допустить его добросовестного использования другим лицом. Доменное имя в подавляющем большинстве стран является объектом купли-продажи, и стоимость его может существенно возрастать в зависимости от разных факторов. Сразу после появления доменных имен, в 1980-х, они не имели коммерческой ценности. Но с развитием так называемого «е-бизнеса», во второй половине 1990-х годов, стало ясно, что хорошее доменное имя дает существенную прибавку числа клиентов. Следовательно, доменное имя имеет стоимость, является активом компании, может покупаться и продаваться. Оценочная стоимость самых популярных доменных имен достигает десятков миллионов долларов. Зафиксированы реальные сделки с доменными именами на суммы в несколько миллионов. Естественно, в таких условиях появляются желающие заработать на перепродаже доменных имен – киберсквоттеры.

Платежи через Интернет.

Это, конечно же, не вид преступления. Однако некоторые чисто офлайновые преступления превращаются в компьютерные, если для передачи денег используются платежные системы Интернета, либо договоренность о платеже достигается через Интернет. В той части, которая касается такого платежа, расследование должно использовать методы компьютерной криминалистики. С другой стороны, многие компьютерные преступления включают в способ совершения осуществление платежа через подобные системы.

Наряду с банковскими платежными системами и методами платежа, которые подчиняются законодательству той или иной страны и имеют механизмы для расследования проведенных операций, существуют и чисто сетевые платежные системы, которые банками не являются и не столь подвержены контролю со стороны государственных органов. Можно назвать такие системы, как «WebMoney», «PayPal», «E-gold», «Яндекс-Деньги» и другие. Как правило, они связаны между собой различными гейтами и частными посредниками, поэтому можно быстро конвертировать средства из одной системы в другую, затрудняя тем самым отслеживание и блокирование криминальных транзакций. Именно такая квазиа злоумышленников к использованию сетевых платежных систем.

Существуют и вторичные услуги – управление счетами таких платежных систем, ввод и вывод средств из них, в том числе анонимный. Из-за множественности таких систем, их трансграничности, легкости перевода средств из одной в другую существует реальная возможность остаться анонимным как для плательщика, так и для получателя платежа. Конечно, это не принципиальная анонимность, а трудность отслеживания платежей и переводов. Для выпуска карты формально требуется предъявить паспорт или прислать его скан_копию. Но проверка именно формальная, никаких

серьезных препятствий для получения карты на чужое имя не существует. Не говоря уже о том, что аккаунты в таких системах свободно продаются и покупаются, можно воспользоваться чужим аккаунтом для заказа карты, которая высылается по почте. Подобная опция дает злоумышленнику возможность использовать счет «WebMoney» или «E-gold» для получения криминальных платежей, например, доходов от кардерской деятельности, платы от потерпевшего по мошенничеству или вымогательству. Зачисленная на электронный кошелек сумма быстро переводится через два-три промежуточных аккаунта на карточный счет, при этом используется веб-интерфейс управления счетом, который, в принципе, позволяет анонимизировать пользователя. Затем деньги с карты снимаются в банкомате, каковая операция также допускает анонимность.

В порядке противодействия указанным способам, в зависимости от обстоятельств, перед правоохранительными органами могут стоять следующие задачи:

- воспрепятствовать регулярной деятельности злоумышленников, максимально затруднив обналичивание денег с их электронных кошельков;
- воспрепятствовать обналичиванию конкретного платежа на электронный кошелек;
- вернуть конкретный платеж отправителю;
- установить лицо, получающее деньги с конкретного электронного кошелька или получившее конкретный платеж.

Упомянутые выше карты для обналичивания средств с электронных кошельков эмитируются не самими платежными системами (хотя и несут их логотип), а банками. Банки же вполне подконтрольны властям и при наличии судебной санкции не только сообщат всю информацию о карточном счете, но и заблокируют его или вернут платеж.

Основные выводы

Компьютерное преступление (киберпреступление) – уголовное правонарушение, для расследования которого существенным условием является применение специальных знаний в области информационных технологий, в которых машинная информация является объектом преступного посягательства.

Компьютерные преступления условно можно разделить на две большие категории: преступления, связанные с вмешательством в работу компьютеров; преступления, использующие компьютеры как необходимые технические средства.

Виды преступлений, связанные с вмешательством в работу компьютеров: НСД к информации, ввод в ПО «логических бомб», разработка и распространение компьютерных вирусов, преступная небрежность, подделка и хищение компьютерной информации.

Под способом совершения преступления понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить наиболее оптимальные методы решения задач раскрытия преступления.

Способы совершения компьютерных преступлений можно классифицировать на пять основных групп: изъятие средств компьютерной техники, перехват информации, НСД, манипуляция данными и управляющими командами, комплексные методы.

Активный перехват осуществляется с помощью подключения к

телекоммуникационному оборудованию компьютера, например линии принтера или телефонному проводу канала связи, либо непосредственно через соответствующий порт персонального компьютера.

Пассивный перехват основан на фиксации электромагнитных излучений, возникающих при функционировании многих средств компьютерной техники, включая и средства коммуникации.

Виды компьютерных преступлений: онлайн_мошенничество, DoS и DDoS атаки, вредоносные программы, дефейс, кардерство, фишинг, платежи через Интернет.

Схема онлайн-мошенничеств такова: размещение (рассылка) информации; взаимодействие с жертвой; получение денежного перевода.

Дефейс – правонарушение, в котором злоумышленник тем или иным способом изменяет внешний вид публичного веб-сайта потерпевшего, чаще всего его титульную страницу.

Кардерство - мошенничество в области банковских карт.

Фишинг – это выманивание у потерпевших их конфиденциальных данных методами социальной инженерии.

Вопросы для самоконтроля

1. *Дайте определение понятию «компьютерное преступление».*
2. *Основные направления компьютерных преступлений.*
3. *Структура классификации компьютерных преступлений.*
4. *Типичные образы компьютерных преступников.*
5. *Приведите основные виды преступлений, связанные с вмешательством в работу компьютеров.*
6. *Чем отличается активный перехват от пассивного перехвата?*
7. *Какие категорию преступлений существуют, в которых*

компьютер является «средством» достижения цели?

8. *Приведите схему работ онлайн-мошенничество.*
9. *Какие следы технического характера образуются при подготовке и проведении DoS-атаки?*
10. *Вредоносные программы заточенные под извлечение выгоды.*
11. *Какие цифровые следы можно обнаружить при изготовлении вредоносных программ?*
12. *Способы получения данных с банковских карт.*
13. *Что такое Скиминг, Реальный пластик и Белый пластик?*
14. *Что такое киберсквоттинг, фишинг и его разновидности??*
15. *Вид преступления при платежи через Интернет.*
16. *Какие способы совершения компьютерных преступлений существуют?*
17. *Чем отличается изъятие средств компьютерной техники от перехвата информации?*
18. *Основные причины и условия, способствующие совершению компьютерных преступлений.*

3. ПРЕДУПРЕЖДЕНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ И ОПЕРАТИВНО-РОЗЫСКНЫЕ МЕРОПРИЯТИЯ

3.1. Предупреждение компьютерных преступлений

Международный опыт борьбы с преступностью свидетельствует о том, что одним из приоритетных направлений решения задачи эффективного противодействия современной преступной деятельности является активное использование правоохранительными органами различных мер профилактического характера. Большинство зарубежных специалистов прямо указывает на то, что предупредить компьютерное преступление всегда намного легче и проще, чем его раскрыть и расследовать. Обычно выделяются три основные группы мер предупреждения компьютерных преступлений, составляющие в своей совокупности целостную систему борьбы с этим социально опасным явлением: правовые, организационно-технические и криминалистические.

Между тем общеизвестно, что одними правовыми мерами сдерживания не всегда удается достичь желаемого результата в деле предупреждения преступлений. Тогда следующим этапом становится применение мер организационно-технического характера для защиты средств компьютерной техники от противоправных посягательств на них. К сожалению, приходится признать, что большая часть компьютерных преступлений совершается вследствие недостаточности организационных мер в предприятиях и организациях, слабой защитой данных от НСД, недостаточной конфиденциальности, слабой проверки и инструктажа персонала.

Анализ материалов отечественных уголовных дел позволяет сделать вывод о том, что основными причинами и условиями, способствующими совершению компьютерных преступлений в большинстве случаев стали:

1) неконтролируемый доступ сотрудников к пульту управления (клавиатуре) компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе осуществления финансовых операций;

2) бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать компьютеров в качестве орудия совершения преступления;

3) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

4) несовершенство парольной системы защиты от НСД к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

5) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации и ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа;

6) отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности, в т. ч. находящейся в форме машинной информации;

7) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

Наиболее эффективной защитой от компьютерных правонарушений является введение в штатное расписание организаций должности специалиста по компьютерной безопасности (администратора по защите информации) либо создание специальных служб как частных, так и

централизованных, исходя из конкретной ситуации. Наличие такого отдела (службы) в организации, по оценкам зарубежных специалистов, снижает вероятность совершения компьютерных преступлений вдвое.

Организационно-управленческих мер, существенную роль в борьбе с компьютерными преступлениями могут играть меры технического характера (аппаратные, программные и комплексные). Аппаратные методы предназначены для защиты компьютерной техники от нежелательных физических воздействий и закрытия возможных каналов утечки конфиденциальной информации. К ним относятся источники бесперебойного питания, устройства экранирования аппаратуры, шифрозамки и устройства идентификации личности. Программные методы защиты предназначаются для непосредственной защиты информации. Для защиты информации при ее передаче обычно используют различные методы шифрования данных. Как показывает практика, современные методы шифрования позволяют достаточно надежно скрыть смысл сообщения. При рассмотрении вопросов, касающихся программной защиты информационных ресурсов, особо выделяется проблема их защиты от компьютерных вирусов как способа совершения компьютерного преступления. В настоящее время разрабатываемые программные антивирусные средства позволяют с определенным успехом (примерно 97%) опознать зараженные программные средства и их компоненты. Существующие антивирусные программные пакеты (Kaspersky, AIDSTEST, DrWeb, SHERIFF, ADinf, Norton Antivirus и др.) позволяют обнаруживать и уничтожать большинство вирусных программ.

3.2. Установление принадлежности и расположения IP-адреса

Почти в каждом уголовном деле, связанном с сетью Интернет, прису-

тствовала такая задача: по известному IP-адресу установить использующий его компьютер и местоположение этого компьютера.

Как правило, цепочка доказательств выглядит именно таким образом:

(преступление) — (IP-адрес) — (компьютер) — (человек)

При помощи различных технических средств фиксируется IP-адрес, с которого осуществлялась криминальная деятельность. Затем устанавливается компьютер, который использовал данный IP-адрес, факт такого использования закрепляется экспертизой. Затем следует доказать, что этим компьютером в соответствующее время управлял подозреваемый.

IP-адрес является уникальным идентификатором компьютера или иного устройства в сети Интернет. Это значит, что в пределах всей глобальной компьютерной сети в каждый момент времени только один-единственный компьютер может использовать определенный IP-адрес. Из этого правила имеется целый ряд исключений:

- приватные, или так называемые «серые» IP-адреса;
- коллективные, или мульти кастовые (multicast) IP-адреса;
- сетевые и широковещательные (broadcast) IP-адреса;
- не выделенные или не присвоенные регистратором IP-адреса;
- IP-адреса, относящиеся к территориально распределенным кластерам компьютеров.

Если же IP-адрес относится к категории публичных (так называемых «белых») адресов, если он должным образом выделен одним из регистраторов, то этот адрес будет маршрутизироваться. То есть IP-пакет, отправленный на этот адрес из любой точки Интернета, найдет свою цель. Это значит, что данный IP-адрес — уникальный. И возможно установить компьютер, которому принадлежит этот IP-адрес.

Является ли тот или иной IP-адрес уникальным, не принадлежит ли он

к упомянутым исключениям — это устанавливает специалист или эксперт.

Регистраторы. Выделением и регистрацией IP-адресов в Интернете занимаются организации, именуемые регистраторами IP-адресов (IP Registry). Это организации, являющиеся органами самоуправления Интернета. Регистраторы образуют трехуровневую иерархию: IANA — RIR — LIR.

Организация IANA является главным регистратором, она выделяет самые крупные блоки IP-адресов региональным регистраторам и большим организациям.

Региональные регистраторы (RIR) в настоящее время пять (Рис.12).

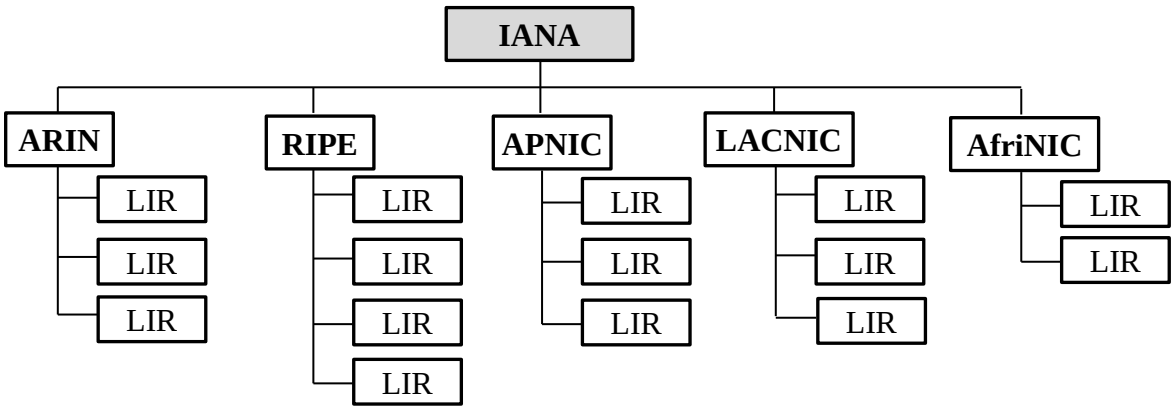


Рис.12. Региональные регистраторы

Это ARIN (Северная Америка), RIPE (Европа и Центральная Азия), APNIC (Азиатско-Тихоокеанский регион), LACNIC (Латинская Америка), AfriNIC (Африка). Они выделяют крупные и средние блоки адресов местным регистраторам (LIR), а также ведут базу данных выделенных IP-адресов и предоставляют доступ к ней.

Местные регистраторы (LIR) выделяют мелкие блоки IP-адресов операторам связи и потребителям и регистрируют их в базе данных своего регионального регистратора. Как правило, роль местного регистратора ис-

полняет оператор связи (Интернет-провайдер). Таких регистраторов — несколько тысяч.

Все выделенные IP-адреса регистрируются в специальной базе данных, которую поддерживает региональный регистратор (RIR). Сведения из этой базы данных (за исключением некоторых полей) доступны любому лицу по протоколу whois. Обратиться к этой базе достаточно просто. При наличии доступа в Интернет надо набрать в командной строке «whois <ip-адрес>». Такая команда имеется в любой операционной системе, кроме Windows. Для тех, кому она недоступна или неудобна, есть многочисленные веб-интерфейсы, то есть веб-страницы, на которых можно ввести запрашиваемый IP-адрес и получить ответ из соответствующей базы данных при помощи браузера.

Можно ли доверять данным, полученным таким способом? Обязанности по внесению, изменению и удалению записей лежат на местных регистраторах (LIR). Но за исполнением этих обязанностей строго не следят. Местный регистратор может несвоевременно обновить запись или же, чтобы облегчить себе работу, зарегистрировать одной записью диапазон адресов, выделенных нескольким разным клиентам. Кроме того, данные о пользователях IP-адресов заносятся, как правило, со слов клиента, без должной верификации. Всё это приводит к тому, что среди записей указанной базы данных встречаются неверные - устаревшие или с неполными, некорректными сведениями.

Поэтому всецело доверять таким сведениям не следует. Как правило, сведения о местном регистраторе (LIR) - верные, поскольку LIR является членом регионального регистратора (RIR), имеет с ним договор, платит членские взносы, постоянно взаимодействует. А сведения о клиенте RIR'a, непосредственном пользователе IP, подлежат дальнейшей проверке.

Неуловимый IP. Приведем еще один интересный пример. Это «зомби-

хостинг», то есть содержание публичных сетевых ресурсов не на серверах, а на компьютерах зомби-сети (ботнета). Зомбированные клиентские компьютеры используются как в качестве веб-серверов, так и в качестве DNS-серверов для соответствующего домена. Зомби-сервер живет недолго - от нескольких часов до нескольких дней. Однако их много. Поэтому можно поддерживать постоянную доступность.

Зафиксировать положение такого сайта невозможно, обнаружить его владельца довольно трудно, доказать факт управления таким сайтом-призраком тоже нелегко.

Описанная технология применяется довольно редко. Подавляющее же большинство веб-сайтов живут на фиксированных IP-адресах, операторы-владельцы которых знают если не о личности владельца сайта, то, по крайней мере, о самом факте размещения.

Пространство и время. IP-адреса могут переходить от одного пользователя к другому. Некоторые из них выделяются на постоянной основе - они именуются статическими. Другие же IP-адреса выделяются только на конкретный сеанс связи и называются динамическими. Для статических IP-адресов период жизни исчисляется месяцами и годами, а для динамических - минутами.

В записях для тех диапазонов IP-адресов, которые используются для динамического выделения, обычно это указывается. Там можно увидеть слова «dynamic», «dialup» или «NAT».

В обоих случаях при установлении принадлежности IP-адресов следует учитывать момент времени, по состоянию на который мы хотим установить пользователя этого адреса. Для динамических IP-адресов этот момент надо указывать с точностью до секунды, поскольку бывают совсем короткие сеансы связи. Кроме времени следует указать часовой пояс и возможную погрешность часов, по которым фиксировалось время.

Документирование. Для уголовного дела, скорее всего, будет недостаточно простой распечатки ответа whois-сервера. Получить же официальную справку от европейского регионального регистратора RIPE будет весьма затруднительно.

Нынешняя практика предусматривает два способа документирования ответа whois-сервера. Первый вариант: распечатка такого ответа может быть заверена каким-либо местным оператором связи, являющимся одновременно местным регистратором (LIR). Второй вариант: получение сведений о принадлежности IP-адреса оформляется рапортом оперуполномоченного; сведения из базы данных регистратора приводятся прямо в тексте рапорта. Иные варианты документирования (экспертиза, нотариальное заверение, справка от RIR) возможны, но до сих пор не применялись на практике.

Принадлежность IP-адреса к конкретному компьютеру все равно должна подтверждаться экспертизой этого компьютера и показаниями сотрудников оператора связи. Поэтому описанная нестрогость в документировании ответа whois-сервера вполне допустима.

Физическое расположение. Из данных регистратора мы узнаем, за кем закреплена соответствующая подсеть или диапазон IP-адресов. Обычно таковым субъектом является оператор связи или его клиент. Очень редко в базе данных регистратора значится непосредственный пользователь IP-адреса.

Получить или уточнить данные о непосредственном пользователе, а также установить его географическое расположение можно у оператора связи, на которого зарегистрирован соответствующий диапазон IP. Бывает, что этот оператор не знает точного местоположения клиента, поскольку между ним и клиентом находится оператор-посредник или оператор последней мили. Бывает, что посредник не единственный. В таком случае придется пройти по всей цепочке операторов.

Понятно, что невозможно не только изложить, но даже просто упомянуть все возможные особенности и трудности в задаче установления принадлежности IP-адресов.

Поэтому при установлении принадлежности и местоположения IP-адреса в ходе ОРМ или предварительного следствия участие технического специалиста обязательно.

3.3. Установление принадлежности доменного имени

Домен - область (ветвь) иерархического пространства доменных имен сети Интернет, которая обозначается уникальным доменным именем. Некоторые юристы относят доменное имя к средствам индивидуализации. Другие не склонны считать его таковым и говорят, что юридическая природа доменного имени пока четко не определена. Есть даже экзотическое мнение, что доменные имена - это ресурс нумерации электросвязи,

В отличие от юридической, техническая природа доменных имен известна хорошо и четко описана в соответствующих технических стандартах.

Для справедливого распределения пространства доменных имен и обеспечения их глобальной уникальности действует система регистрации доменных имен. Подлежат регистрации все доменные имена первого уровня (например, org, info, ru, ua), все доменные имена второго уровня (например, gprf.info, fnn.ru) и некоторые, выделенные доменные имена третьего уровня (например, provider.net.ru, london.co.uk). Прочие доменные имена регистрации не подлежат и распределяются по усмотрению владельца соответствующего домена более высокого уровня (например, домены www.fnn.ru и mail.fnn.ru создаются и используются исключительно по воле владельца домена второго уровня fnn.ru).

Для каждого домена, где предусмотрена обязательная регистрация, назначен регистратор или несколько регистраторов. В последнем случае все регистраторы обязаны использовать единую базу данных для обеспечения уникальности регистрируемых доменных имен. Все базы данных всех регистраторов являются публично доступными по протоколу whois, аналогично регистраторам IP-адресов. Чтобы установить владельца какого-либо доменного имени из числа подлежащих регистрации, следует обратиться к базе данных соответствующего регистратора. Для не подлежащих регистрации доменных имен обращаться нужно к владельцу соответствующего домена более высокого уровня.

Например, нам требуется установить владельца доменного имени 3-го уровня «www.internet-law.ru».

Очевидно, что данный домен 3-го уровня не относится к числу регистрируемых. Он находится в полном распоряжении владельца соответствующего домена 2-го уровня, то есть домена «internet-law.ru», который уже зарегистрирован. Здесь придется сделать допущение, а именно предположить, что указанный домен 3-го уровня в силу стандартности его имени (www) принадлежит тому же владельцу, что и домен 2-го уровня. Чтобы узнать владельца доменного имени «internet-law.ru», обращаемся к базе данных российских регистраторов доменов. Для этого используем команду «whois», имеющуюся в любой ОС (кроме Windows). В качестве аргумента задаем искомое доменное имя, а параметр определяет, какой реестр запрашивать. Следует помнить, что данные о владельце домена заносит в базу регистратор. Как для домена RU, так и для других доменов установлен порядок занесения и изменения записей. Разумеется, присутствуют требования об актуальности и достоверности данных. Однако регистраторы не всегда имеют возможности проводить проверку сообщенных им данных. И не всегда вовремя обновляют устаревшие.

Какие же данные о владельце домена можно считать достоверными? Те, от которых зависит его право распоряжаться доменным именем. Согласно условиям типового договора большинства регистраторов, указание недостоверных данных о владельце доменного имени может повлечь отмену регистрации. Невозможность связаться по указанным контактным данным также может привести к потере права на доменное имя. Многие регистраторы не позволяют передавать доменные имена иному лицу, пока прежний владелец не представит соответствующие документы. Следовательно, указание неверных контактных данных (телефона, почтового адреса, адреса электронной почты) с немалой вероятностью приводит к потере доменного имени. Указание неверного имени (названия) владельца приводит к тому, что домен нельзя будет передать другому владельцу (продать).

Отсюда можно сделать вывод о том, какие из указанных данных о владельце более достоверны, а какие — менее. Немного сложнее обстоит дело с документированием принадлежности домена. Как для уголовного, так и для гражданского процесса необходимо доказать, что-такое-то доменное имя принадлежит такому-то лицу. На практике применяются следующие методы:

1. Оформить получение справки от whois-сервера рапортом оперуполномоченного. Совсем не безупречный способ. Годится только если обвиняемый (ответчик) не намерен отрицать принадлежность доменного имени.
2. Заверить у нотариуса содержимое веб-страницы, представляющей собой веб-интерфейс к команде whois, например, такой, как изображена на последней иллюстрации. Применяется для гражданских дел. Далеко не все нотариусы соглашаются заверять содержимое веб-страниц. Но уж если такого нотариуса удалось найти, то нотариальное заверение производит на суд

положительное впечатление. Но для специалиста такой способ — почти профанация, ведь нотариус не видит, к какой именно базе данных подключен веб-интерфейс. Следовательно, его заверение — не более чем заверение надписи на заборе, сделанной неизвестно кем неизвестно для каких целей.

3. Получить официальный ответ оператора связи (провайдера), который имел отношение к обслуживанию этого доменного имени, например, поддерживал для него DNS-сервер или веб-сайт. Вместо письма провайдера можно взять показания у соответствующего технического сотрудника этого провайдера.
4. Получить показания свидетелей. Например, о том, что интересующее нас лицо совершало определенные действия с доменным именем, доступные только его владельцу.
5. Доказать факт оплаты соответствующим лицом услуг по регистрации или продлению домена. Хотя оплачивать можно и чужой домен, но тем не менее это хорошее косвенное доказательство.
6. Назначить компьютерно-техническую экспертизу, в ходе которой эксперт запросит нужный whois-сервер и о результатах напишет в своем заключении. Способ несложный, но далеко не безупречный. Сомнительна сама возможность проведения компьютерно-технической экспертизы, когда объект исследования (whois-сервер, база данных регистратора) находится не в распоряжении эксперта, а неизвестно где, на другом конце мира.
7. Обнаружить в ходе экспертизы на компьютере соответствующего лица свидетельства соединения и успешной авторизации на интерфейсе регистратора доменов. Практически все регистраторы предоставляют владельцам доменных имен возможность удаленно

управлять своими доменами через веб-интерфейс на веб-сайте регистратора.

8. Получить справку о регистрации доменного имени у соответствующего регистратора или в техническом центре. У иностранного регистратора получить такую справку труднее, придется задействовать Интерпол.

3.4. Принадлежность адреса электронной почты

Сообщения электронной почты фигурируют во многих уголовных и гражданских делах. В некоторых они даже являются центральным доказательством. При помощи электронной почты заключаются сделки, происходит сговор о совершении преступления, совершается вымогательство, передаются существенные для дела сведения. Во всех подобных случаях встает вопрос: кому принадлежит или кем используется тот или иной адрес электронной почты.

Почтовый ящик. В большинстве случаев адрес электронной почты однозначно связан с почтовым ящиком. И все письма, адресованные на этот адрес, попадают в этот ящик, откуда потом пользователь может их забрать.

Однако есть исключения:

- групповые или коллективные адреса, которые представляют собой адрес списка рассылки; все поступающие на этот адрес письма рассылаются определенной группе адресатов; таковыми часто бывают ролевые адреса, например, info@company.ru или noc@provider.net;
- технические адреса, за которыми не стоит ни пользователь, ни почтовый ящик; все поступающие на такой адрес письма обрабатываются программой; например, иногда в качестве обратного

адреса указывается нечто вроде noreply@domain.com - все, что поступает на такой адрес, отправляется почтовым сервером на устройство /dev/null;

– адреса для пересылки (forward) сообщений; все поступающие на такой адрес сообщения не складываются в почтовый ящик, а перенаправляются на другой, заранее заданный адрес.

Передача сообщений. В сообщении электронной почты адрес может быть указан в следующих полях.

Адрес получателя – в полях «To», «Cc» и «Bcc».

Адрес отправителя – в полях «From», «Reply-to» и «Return-path». Парадокс в том, что все эти поля могут не содержать истинного адреса. Все шесть адресов могут быть подложными, но, несмотря на это, сообщение дойдет по назначению.

Установление. Для начала следует установить почтовый ящик, с которым связан адрес. Затем выяснить, кто пользуется этим почтовым ящиком. Так будет установлен владелец адреса. Для установки места расположения почтового ящика исследователь устанавливает первичный MX домена. Во многих случаях ящик находится на этом же сервере. В других случаях сервер пересылает почту на иной сервер, указанный в его настройках. В обоих случаях требуется узнать эти настройки, чтобы определить местоположение почтового ящика.

Для этого потребуется содействие провайдера, обслуживающего сервер. Расположение почтового ящика документируется протоколом осмотра нужного сервера (серверов) или заключением эксперта. В крайнем случае, можно ограничиться получением письменного ответа провайдера на соответствующий запрос, но этот способ доказательства нельзя назвать безупречным. Доказательствами факта использования почтового ящика определенным лицом могут служить:

– наличие на компьютере этого лица настроек для доступа к этому ящику (включая пароль);

– наличие на компьютере этого лица полученных сообщений электронной почты со служебными заголовками, свидетельствующими о прохождении сообщений через этот почтовый ящик;

– наличие на сервере, где расположен ящик, логов об успешном соединении и аутентификации пользователя данного почтового ящика;

– наличие у других абонентов сообщений от этого лица, написанных в ответ на сообщения, отправленные на этот почтовый ящик (в ответе часто цитируется исходное сообщение, а также среди служебных заголовков присутствует заголовок со ссылками на предыдущие сообщения).

3.5. Что такое Who is?

В настоящее время Интернет настолько скрыт, что вы даже не знаете, что вашим собеседником в чате может быть ваш друг за стеной, а самым напористым оппонентом на любимом форуме ваша жена. Но не всегда анонимность бывает скрытой. Существует такой сервис как **Whois**, который разоблачает владельцев Интернет-ресурсов. Что же из себя представляет ***термин Whois?*** На самом деле тут всё просто. Это протокол, через который сервер может передать информацию клиенту о том, на кого зарегистрирован домен или его **IP-адрес.** Данные предоставляются специальными базами, которые содержат информацию о пользователях того или иного домена. Естественно, данная информация может быть устаревшей или недостоверной, так как эта информация предоставляется человеком при регистрации домена. Данная информация так же может быть подробной: в базе содержатся имя пользователя, адрес регистрации, e-mail, номер телефона, название фирмы, зарегистрировавшей этот домен. Всё это

подходит так же для информации об IP-адресах.

С какой целью стал нужен данный протокол Whois? В недавние времена, когда Интернет только начинал свое развитие, и никто не слышал о такой проблеме, как кибersквоттинг, предполагали, что администраторы сайтов с его помощью будут находить необходимую информацию друг о друге и решать различные проблемы. В настоящее время он необходим в большей части для того, чтобы ловить кибersквоттеров и вести с ними борьбу. Чтобы работать с протоколом Whois, есть различные программы (клиенты). Некоторые из них имеют консольный интерфейс, другие - графический, но в основном работают по средством web-интерфейса, т.е. получать информацию о доменах и IP-адресах так, же можно с помощью браузеров. Имеется большое количество **Whois-сервисов,** которые легко найти с помощью Yandex, Google или другой поисковой системой. Большинство сервисов ограничены некоторыми доменными зонами, для которых существует поиск Whois-информации, в связи с особенностями баз данных, содержащих информацию.

Базы данных, которые содержат информацию о пользователях доменов и IP-адресах могут быть распределёнными или, централизованными причём, нет какой- то единой базы с информацией обо всех доменах или IP-адресах в мире. В централизованных базах данных (доменная зона ORG) всё довольно просто: один сервер отвечает на все Whois-запросы, т.к. у него имеется вся необходимая информация.

В случае если база данных децентрализованная (доменная зона COM) сервер направляет запросы на другие сервера, которые обладают информацией об ограниченном числе доменов. В настоящее время, централизованные базы данных используют в доменных зонах, где доменов много, в то время как распределённая более подходит для больших доменных зон (что, в общем, видно на примере ORG и COM).

Если вы зарегистрировали свой домен через коллегу или вашего веб - разработчика, проверьте его на Whois сервисе, действительно ли он вам принадлежит.

Если домен был зарегистрирован через знакомых и важная информация утеряна – пароль, имя пользователя тогда вы можете потерять ваш домен навсегда. Его возможности так же помогут вам контролировать ваших конкурентов и разобраться в их стратегии, которую они используют, а интернете и выработать ответные шаги для их нейтрализации.

3.6. Исследование лог-файлов

Выражения **«лог-файлы»** или просто **«логи»** легко употребляются оперативниками, следователями всеми участниками процесса, однако мало кто из них четко представляет себе, что это такое. Какая информация записывается в лог-файл? Да любая! Какую вы пожелаете, такая и записывается.

Так, что же такое лог-файл или лог?

Лог - это журнал автоматической регистрации событий, которые фиксируются в рамках какой-либо программы. Обычно каждому событию соответствует одна запись в логе. Обычно запись вносится сразу же после события (его начала или окончания). Записи эти складываются в назначенный файл самой программой либо пересылаются ею другой, специализированной программе, предназначенной для ведения и хранения логов.

Как понятно из определения, в логах могут регистрироваться абсолютно любые события - от прихода единичного ethernet-фрейма до результатов голосования на выборах президента. Форма записи о событии также целиком остается на усмотрение автора программы. Формат лога

может быть машинно-ориентированным, а может быть приспособлен для чтения человеком.

Иногда логи ориентированы на цели безопасности и расследования инцидентов. В таких случаях стараются по возможности изолировать логи от системы, события в которой они фиксируют. Если злоумышленник преодолеет средства защиты и получит доступ в систему, он, возможно, не сможет одновременно получить доступ к логам, чтобы скрыть свои следы.

Почти каждое действие, производимое человеком при взаимодействии с информационной системой, может отражаться в логе прямо или косвенно, иногда даже в нескольких логах одновременно. И логи эти могут быть разбросаны по различным местам, о которых неспециалист даже не догадается.

Чтобы узнать о действиях злоумышленника, получить какие-либо данные о нем при помощи логов, необходимо:

- узнать, какие компьютеры и их программы вовлечены во взаимодействие;
- установить, какие события логируются в каждой из вовлеченных программ;
- получить все указанные логи за соответствующие промежутки времени;
- исследовать записи этих логов, сопоставить их друг с другом.

Например, такое обыденное действие, как просмотр одним пользователем одной веб-страницы. Перечислим вовлеченные в это действие системы, которые в принципе могут вести логи событий:

- браузер пользователя;
- персональный межсетевой экран на компьютере пользователя;
- антивирусная программа на компьютере пользователя;
- операционная система пользователя;

- DNS-сервер (*резолвер*), к которому обращался браузер пользователя перед запросом веб-страницы, а также DNS-сервера (держатели зон), к которым рекурсивно обращался этот резолвер;
- все маршрутизаторы по пути от компьютера пользователя до веб-сервера и до DNS-серверов, а также билинговые системы, на которые эти маршрутизаторы пересылают свою статистику;
- средства защиты (межсетевой экран, система обнаружения атак, антивирус), стоящие перед веб-сервером и вовлеченными DNS-серверами;
- веб-сервер;
- CGI-скрипты, запускаемые веб-сервером;
- веб-сервера всех счетчиков и рекламных баннеров, расположенных на просматриваемой пользователем веб-странице (как правило, они поддерживаются независимыми провайдерами);
- веб-сервер, на который пользователь уходит по гиперссылке с просматриваемой страницы;
- прокси-сервер (если используется);
- АТС пользователя (при коммутируемом соединении с Интернетом - по телефонной линии) или иное оборудование последней мили (xDSL,
  Wi-Fi, GPRS и т.д.).

Итого может набраться два-три десятка мест, где откладываются взаимно скоррелированные записи, относящиеся к одному-единственному действию пользователя - просмотру веб-страницы.

При более сложных видах взаимодействия появляется еще больше мест, в которых могут остаться следы действий пользователя. Определить все эти места и указать, к кому именно следует обращаться за соответствующими логами, - это задача для ИТ-специалиста. Даже самый

продвинутый следователь не в состоянии его заменить. Поэтому привлечение специалиста в таких случаях обязательно.

Исследование логов веб-сервера.

Логи веб-сервера, как понятно из предыдущего, являются далеко не единственным источником информации о действиях пользователя. Какие же данные можно найти в логах веб-сервера? Набор таких данных различается в зависимости от типа веб-сервера и его настроек. Чаще всего в логах присутствуют следующие данные:

- IP-адрес клиента;
- время запроса, включая часовой пояс;
- поля HTTP-запроса клиента;
- идентификатор пользователя, если присутствует аутентификация;
- URL запрашиваемой веб-страницы и отдельные его элементы (домен, путь, параметры);
- истинный IP (при доступе через неанонимный прокси-сервер);
- идентификационная строка браузера клиента (включая язык и ОС);
- реферер (referrer), то есть адрес веб-страницы, с которой был осуществлен переход на данную страницу;
- тип контента ответа веб-сервера (MIME type), о любые другие поля;
- код ответа веб-сервера (status code);
- размер ответа веб-сервера (без учета HTTP-заголовка);
- ошибки, происшедшие при доступе к веб-страницам.

Можно ли доверять логам? Какие данные в логах веб-сервера возможно фальсифицировать, не имея доступа к самому веб-серверу?

Только поля HTTP-запроса. Этот запрос полностью формируется на стороне клиента, поэтому при желании злоумышленник может подставить в него любые поля с любыми значениями.

Зафиксированному в логе IP-адресу можно доверять. Конечно, при

этом следует помнить, что это может оказаться IP прокси-сервера или сокс-сервера или иного посредника. Прочие поля - это внутренние данные веб-сервера (код ответа, размер страницы и т.п.), которым также можно доверять.

Для проверки достоверности данных логов веб-сервера применяется сопоставление записей между собой, а также с иными логами. Приведем пример из практики, иллюстрирующий полезность сопоставления различных логов. Сотрудник службы информационной безопасности интернет-казино, анализируя логи веб-сервера, заметил, что браузер одного из игроков, согласно полям его HTTP-запросов, поддерживает русский язык. При этом IP-адрес числился за Кореей. Указания же на корейский язык не было. Это возбудило подозрения. Сотрудник проверил, с каких еще адресов обращался пользователь под этим аккаун-том. Оказалось, что с единственного IP. Тогда он проверил, какие еще пользователи обращались с этого же IP. Оказалось, что больше никто этот корейский IP-адрес не использовал. Но сотрудник службы безопасности не успокоился и проверил, какие еще были обращения от браузера с таким же набором настроек. Оказалось, что с такого же браузера было зарегистрировано больше 10 аккаунтов. Все эти пользователи приходили с IP-адресов разных стран, причем страна соответствовала имени пользователя. Но идентичный набор настроек браузера всех этих пользователей (включая поддержку русского языка) вызывал большие подозрения. Когда же сотрудник сопоставил периоды активности всех подозрительных пользователей, он увидел, что они не пересекаются и более того - примыкают один к другому. Он понял, что имеет дело с кардером, который регистрирует аккаунты по краденым карточкам, пользуясь ***сокс-серверами*** в разных странах. Дальнейшая проверка это подтвердила.

Исследование системных логов.

Логирование событий в операционной системе является одной из трех составляющих безопасности. Имеется в виду модель **«AAA» - authentication,**

authorization, accounting - аутентификация, авторизация, аудит. Запись всех событий, связанных прямо или косвенно с безопасностью системы, и составляет сущность аудита. Логирование само по себе не препятствует злоумышленнику получить несанкционированный доступ к информационной системе. Однако оно повышает вероятность его выявления, а также последующего нахождения и изобличения злоумышленника. Также логирование способствует выявлению уязвимостей защищаемой системы.

Чем более полон аудит, тем проще расследовать компьютерное преступление. Пользуясь записанными данными, специалист или эксперт может извлечь много полезной для дела информации.

Рассмотрим устройство системного аудита событий для различных классов операционных систем.

Системные логи Windows. В операционных системах «Windows» предусмотрено три лога - прикладных программ (application log), системы (system log) и безопасности (security log).

В application log пишутся сообщения и события, генерируемые прикладными программами, а также некоторыми сервисами (службами). В system log помещаются события ядра ОС и важнейших сервисов. В security log записываются также события, генерируемые системными сервисами, относящиеся к отслеживаемой активности пользователей, их аутентификации и авторизации. К этим трем могут добавляться иные логи, если на компьютере работают дополнительные программы, такие как DNS-сервер.

По умолчанию логируются очень немногие события, а в security log - вообще никаких. Чтобы в логах осаждалась более полная информация, администратор должен явно включить аудит и настроить политики аудита.

Все логи Windows просматриваются специальной программой «Event Viewer», которую можно найти в меню «Administrative Tools» или

«Management Console».

В зависимости от того, что именно мы ищем, следы «взлома» исследуемого компьютера или следы противоправной деятельности пользователя, может оказаться полезной разная информация из разных логов.

Системные логи UNIX и Linux. Несмотря на разнообразие UNIX-подобных операционных систем, у всех у них имеется схожая система сбора и хранения системных логов. Логирование событий в операционной системе «MacOS-X» устроено точно таким же образом.

Специальный демон (процесс), называемый syslogd, принимает сообщения о событиях от различных программ и процессов и раскладывает их по соответствующим файлам. Сообщения из одного источника можно направить в разные файлы, сообщения от разных источников можно направить в один и тот же файл - система настраивается довольно гибко. Сообщения о событиях можно принимать как локально, так и через сеть; оба способа используют один и тот же протокол.

Каждое сообщение при его генерации снабжается двумя идентифицирующими признаками – приоритет (priority) и ресурс (facility). Их сочетание служит для последующей сортировки полученных сообщений по файлам.

Принятые syslogd сообщения снабжаются временной меткой и записываются в обычный текстовый файл по принципу одно сообщение - одна строка. Просмотреть эти сообщения можно в любом текстовом редакторе или иной программой, умеющей работать с текстовыми файлами.

Системные логи IOS. Значительная часть (если не большинство) коммутаторов и маршрутизаторов сети Интернет работают под управлением операционной системы IOS. Другие ОС для коммуникационного оборудования схожи с IOS своими чертами, в частности, ведут логи аналогичным образом. К таким типичным устройствам относится

коммуникационное оборудование, выпущенное под марками «Cisco», «Juniper», «Huawei» и некоторыми другими. Оно составляет подавляющее большинство.

В системе IOS логируются следующие события:

- изменение статуса интерфейса или порта;
- авторизация администратора или устройства;
- изменение и сохранение конфигурации устройства;
- прием транзитного пакета, если такой пакет подпадает под правило (ACL entry), отмеченное флагом логирования;
- некоторые другие.

Сообщения о событиях обычно отсылаются на внешний логирующий сервер по протоколу syslog или SNMP. Также несколько последних сообщений хранятся в буфере, в оперативной памяти и могут быть просмотрены соответствующей командой (show logging).

Когда требуется ознакомиться с логами коммуникационного оборудования, следует проделать такие действия:

- получить доступ к текущей конфигурации устройства (конфигурационному файлу), чтобы определить, куда именно отсылаются логи с данного устройства (команда show running-config); сохранить и задокументировать вышеуказанную конфигурацию (или только ее часть, касающуюся логов);
- (опционально) просмотреть содержимое буфера устройства с последними сообщениями;
- определить местоположение логирующего сервера, то есть сервера, принимающего и сохраняющего логи;
- получить доступ к логирующему серверу и ознакомиться с конфигурацией его syslog-демона, чтобы определить, в какой файл складываются логи, принятые от интересующего нас устройства;

сохранить и задокументировать вышеуказанную конфигурацию syslog-демона;

- осмотреть или изъять файл (файлы), в котором сохраняются логи с нужного устройства.

Некоторые коммуникационные устройства, относящиеся к меньшинству, не используют ОС IOS или схожую. В таких нетипичных устройствах логирование может быть устроено иначе. В частности, логи могут храниться локально или передаваться на логирующий сервер по нестандартному протоколу.

3.7. Кейлоггеры

Кейлоггер (англ. ***keylogger, key*** **- клавиша и** ***logger*** **- регистрирующее устройство**) - программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя - нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши.

Виды информации, которые могут контролироваться:

- нажатия клавиш на клавиатуре;
- движения и нажатия клавиши мыши;
- дата и время нажатия.

Дополнительно могут делаться периодические снимки экрана (а в некоторых случаях - даже видеозапись экрана) и копироваться данные из буфера обмена.

Кейлоггером является любой компонент программного обеспечения или оборудования, который умеет перехватывать и записывать все манипуляции с клавиатурой компьютера. Нередко кейлоггер находится между клавиатурой и операционной системой и перехватывает все действия пользователя. Этот инструмент либо хранит перехваченную информацию на

зараженном компьютере, либо, если является частью более крупной атаки, все данные сразу передаются на удаленный компьютер организаторов атаки.

Классификация кейлоггеров.

Программные кейлоггеры принадлежат к той группе программных продуктов, которые осуществляют контроль над деятельностью пользователя персонального компьютера.

Первоначально программные продукты этого типа предназначались исключительно для записи информации о нажатиях клавиш клавиатуры, в том числе и системных, в специализированный журнал регистрации (лог-файл), который впоследствии изучался человеком, установившим эту программу. Лог-файл мог отправляться по сети на сетевой диск, FTP-сервер в сети Интернет, по электронной почте и т. д.

В настоящее время программные продукты, сохранившие «по старинке» данное название, выполняют много дополнительных функций - это перехват информации из окон, перехват кликов мыши, перехват буфера обмена, «фотографирование» снимков экрана и активных окон, ведение учёта всех полученных и отправленных e-mail, отслеживание файловой активности и работы с системным реестром, запись заданий, отправленных на принтер, перехват звука с микрофона и изображения с веб-камеры, подключенных к компьютеру и т.д.

Аппаратные кейлоггеры представляют собой миниатюрные приспособления, которые могут быть прикреплены между клавиатурой и компьютером или встроены в саму клавиатуру. Они регистрируют все нажатия клавиш, сделанные на клавиатуре. Процесс регистрации абсолютно невидим для конечного пользователя. Аппаратные кейлоггеры не требуют установки какой-либо программы на компьютере, чтобы успешно перехватывать все нажатия клавиш. Когда аппаратный кейлоггер прикрепляется, абсолютно не имеет значения, в каком состоянии находится

компьютер — включенном или выключенном. Время его работы не ограничено, так как он не требует для своей работы дополнительного источника питания.

Объёмы внутренней энергонезависимой памяти данных устройств позволяют записывать до 20 миллионов нажатий клавиш, причём с поддержкой юникода. Данные устройства могут быть выполнены в любом виде, так что даже специалист не в состоянии иногда определить их наличие при проведении информационного аудита. В зависимости от места прикрепления аппаратные кейлоггеры подразделяются на внешние и внутренние.

Но вернёмся к программным кейлоггерам. Это семейство клавиатурных шпионов очень разнообразно и очень часто, конкретный экземпляр может быть написан в единственном варианте профессиональным хакером для выполнения определённой задачи. Плюс то, что их достаточно легко скрыть от антивирусов, делает их очень опасной угрозой для личных данных.

Акустические кейлоггеры представляют собой аппаратные устройства, которые вначале записывают звуки, создаваемые пользователем при нажатии на клавиши клавиатуры компьютера, а затем анализирующие эти звуки и преобразовывающие их в текстовый формат.

Программные кейлоггеры часто устанавливаются в составе комплексного вредоносного программного обеспечения. Целевые компьютеры могут быть заражены во время скрытой загрузки при посещении зараженного сайта.

Нередко клавиатурные шпионы могут быть различными способами и под различными предлогами встроены во вполне легальный софт. Аппаратные кейлоггеры устанавливает злоумышленник, имеющий физический доступ к интересующему компьютеру.

Обнаружение и удаление. Обнаружить вредоносные кейлоггеры весьма непросто, так как они ведут себя не всегда так, как многие другие вредоносные программы. Они не выискивают ценную информацию и не пересылают ее на удаленный сервер, они не пытаются уничтожить данные на зараженной машине. Клавиатурные шпионы делают свою работу тихо и незаметно. Антивирусные программы могут сканировать, обнаруживать и уничтожать все известные им варианты клавиатурных шпионов. Однако кейлоггеры, предназначенные для целевой атаки на конкретного пользователя, выявить непросто, так как чаще всего они не зарегистрированы в качестве известного вредоносного софта. Тем не менее рано или поздно, но они обнаруживаются, как только начинают проявлять себя путем несанкционированной отправки данных на удаленный сервер.

Методы защиты от кейлоггеров.

1. Защита от «известных» несанкционированно установленных программных кейлоггеров:

- использование антишпионских программных продуктов и/или антивирусных программных продуктов известных производителей с автоматическим обновлением сигнатурных баз.

2. Защита от «неизвестных» несанкционированно установленных программных кейлоггеров:

- использование антишпионских программных продуктов и/или антивирусных программных продуктов известных производителей, которые для противодействия шпионским программным продуктам используют так называемые эвристические (поведенческие) анализаторы, то есть не требующие наличия сигнатурной базы;
- использование программ, шифрующих вводимые с клавиатуры данные, а также применение клавиатур, осуществляющих такое шифрование на аппаратном уровне;

3. Защита от «известных» и «неизвестных» несанкционированно установленных программных кейлоггеров включает в себя использование антишпионских программных продуктов и/или антивирусных программных продуктов известных производителей, которые для противодействия шпионским программным продуктам используют:

- постоянно обновляемые сигнатурные базы шпионских программных продуктов;
- эвристические (поведенческие) анализаторы, не требующие наличия сигнатурной базы.

4. Защита от несанкционированно установленных аппаратных кейлоггеров:

- тщательные внешний и внутренний осмотры компьютерных систем;
- использование виртуальных клавиатур.

3.8. Перехват и исследование трафика

Перехват трафика может осуществляться:

- обычным «прослушиванием» сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свитчей), в противном случае метод малоэффективен, поскольку на снифер попадают лишь отдельные фреймы);
- подключением снифера в разрыв канала;
- ответвлением (программным или аппаратным) трафика и направлением его копии на снифер;
- через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;
- через атаку на канальном (MAC-spoofing) или сетевом уровне (IP-

spoofing), приводящую к перенаправлению трафика жертвы или всего трафика сегмента на снифер с последующим возвращением трафика в надлежащий адрес.

Термин **снифер** происходит от английского **«to sniff» – нюхать** и представляет собой программу или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

Сниферы применяются как в благих, так и в деструктивных целях. Анализ прошедшего через снифер трафика позволяет:

- обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи (сниферы здесь малоэффективны; как правило, для этих целей используют сбор разнообразной статистики серверами и активным сетевым оборудованием и её последующий анализ);
- выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие (это обычно делают при помощи специализированных сниферов — мониторов сетевой активности);
- перехватить любой незашифрованный (а порой и зашифрованный) пользовательский трафик с целью получения паролей и другой информации;
- локализовать неисправность сети или ошибку конфигурации сетевых агентов (для этой цели сниферы часто применяются системными администраторами).

Wireshark – это анализатор сетевого трафика. Его задача состоит в том, чтобы перехватывать сетевой трафик и отображать его в детальном виде. Анализатор сетевого трафика можно сравнить с измерительным устройством, которое используется для просмотра того, что происходит

внутри сетевого кабеля, как например вольтметр используется электриками для того чтобы узнать что происходит внутри электропроводки (но, конечно, на более высоком уровне). В прошлом такие инструменты были очень дорогостоящими. Однако, с момента появления такого инструмента как Wireshark ситуация изменилась.

Wireshark – это один из лучших анализаторов сетевого трафика, доступных на сегодняшний момент. Wireshark работает на основе библиотеки pcap. Библиотека Pcap (Packet Capture) позволяет создавать программы анализа сетевых данных, поступающих на сетевую карту компьютера.

Разнообразные программы мониторинга и тестирования сети, сниферы используют эту библиотеку. Она написана для использования языка C/C++ так что другие языки, такие как Java, .NET и скриптовые языки использовать не рационально. Для Unix-подобных систем используют libpcap библиотеку, а для Microsoft Windows используют WinPcap библиотеку. Программное обеспечение сетевого мониторинга может использовать libpcap или WinPcap, чтобы захватить пакеты, путешествующие по сети и в более новых версиях для передачи пакетов в сети. Libpcap и WinPcap также поддерживают сохранение захваченных пакетов в файл и чтение файлов содержащих сохранённые пакеты.

Программы написанные на основе libpcap или WinPcap могут захватить сетевой трафик, анализировать его. Файл захваченного траффика сохраняется в формате, понятном для приложений, использующих Pcap.

Для чего используется Wireshark?

- Системные администраторы используют его для решения проблем в сети.
- Аудиторы безопасности используют его для выявления проблем в сети.

- Разработчики используют его для отладки сетевых приложений.
- Обычные пользователи используют его для изучения внутреннего устройства сетевых протоколов.

Возможности Wireshark:

1. Работает на большинстве современных ОС (Microsoft Windows, Mac OS X, UNIX).
2. Перехват трафика сетевого интерфейса в режиме реального времени. Wireshark может перехватывать трафик различных сетевых устройств, отображая его имя (включая беспроводные устройства).
3. Множество протокольных декодировщиков (TELNET, FTP, POP, RLOGIN, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, MSN, YMSG и другие).
4. Сохранение и открытие ранее сохраненного сетевого трафика.
5. Позволяет фильтровать пакеты по множеству критерий.
6. Позволяет искать пакеты по множеству критерий.
7. Позволяет подсвечивать захваченные пакеты разных протоколов.
8. Позволяет создавать разнообразную статистику.

Wireshark – это не система обнаружения вторжений. Он не предупредит о том, если кто-то делает странные вещи в сети. Однако если это происходит, Wireshark поможет понять что же на самом деле случилось.Wireshark не умеет генерировать сетевой трафик, он может лишь анализировать имеющийся. В целом, Wireshark никак не проявляет себя в сети, кроме как при резолвинге доменных имен, но и эту функцию можно отключить.

Интерфейс Wireshark

Интерфейс программы Wireshark представлен на рис.13.

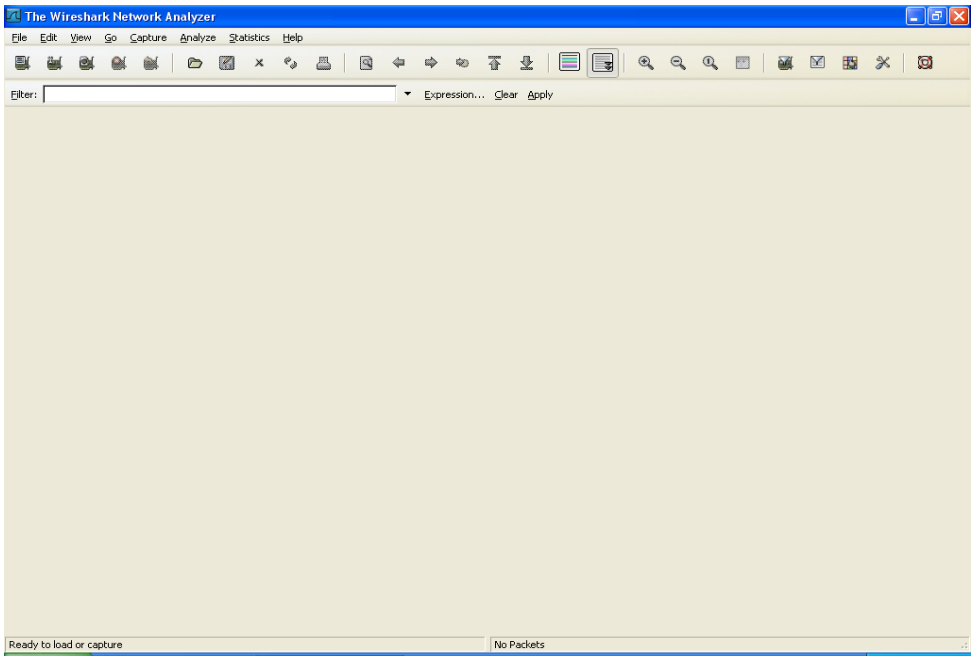


Рис.13. Главное окно программы Wireshark

Сверху находится стандартные для Windows приложений меню и тулбар, на них подробно останавливаться смысла не имеет. Далее следует фильтр, в нем можно задавать критерии фильтрации пакетов. Следом идет окошко со списком всех перехваченных пакетов.

В нем доступна такая информация как: номер пакета, относительное время получения пакета (отсчет производится от первого пакета; параметры отображения времени можно изменить в настройках), IP адрес отправителя, IP адрес получателя, протокол, по которому пересылается пакет, а также дополнительная информация о нем. Как можно заметить, разные протоколы подсвечены разными цветами, что добавляет наглядности и упрощает анализ.

Далее видно окно, в котором представлена детальная информация о пакете согласно сетевой модели OSI. Ну, и самое нижнее окно показывает нам пакет в сыром HEX виде, то есть побайтово. Конфигурация интерфейса может быть легко изменена в меню View.

Например, можно убрать окно побайтового представления пакета (оно

же Packet Bytes в меню View), так как в большинстве случаев (кроме анализа данных в пакете) оно не нужно и только дублирует информацию из окна детального описания.

Перехват трафика является одной из ключевых возможностей Wireshark. Движок Wireshark по перехвату предоставляет следующие возможности:

- перехват трафика различных видов сетевого оборудования (Ethernet, Token Ring, ATM и другие);
- прекращение перехвата на основе разных событий: размера перехваченных данных, продолжительность перехвата по времени, количество перехваченных пакетов;
- показ декодированных пакетов во время перехвата;
- фильтрация пакетов с целью уменьшить размер перехваченной информации;
- запись дампов в несколько файлов, если перехват продолжается долго.

Чтобы начать перехват трафика нужно иметь права Администратора на данной системе и выбрать правильный сетевой интерфейс. Чтобы выбрать сетевой адаптер, с которого будет выполняться перехват нужно нажать на кнопку Interfaces на тулбаре, либо их меню Capture > Interfaces.

После нажатия на одну из этих кнопок появится окно со списком сетевых интерфейсов, доступных в системе (Рис.14).

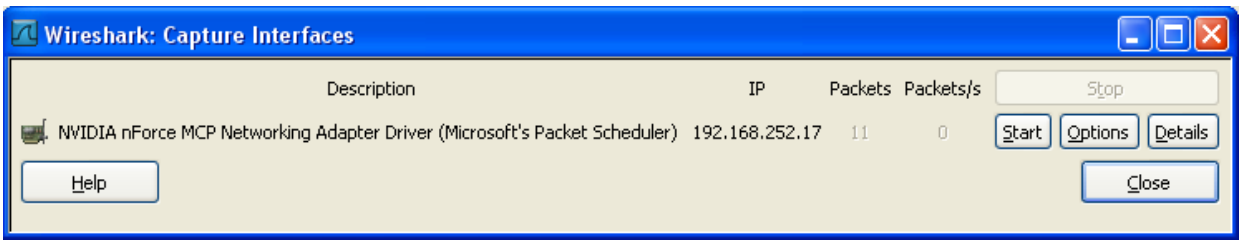


Рис.14. Список сетевых интерфейсов

На этом списке можно увидеть такую информацию как название интефейса, IP адрес интерфейса, сетевая активность интерфейса (представлена в виде общего количества пакетов с момента появления окна и количество пакетов в секунду). Также из этого окна можно посмотреть настройки перехвата и информацию об интерфейсе.

В настройках перехвата можно изменять такие параметры как фильтрация пакетов, запись дампа в несколько файлов, прекращение перехвата по разным критериям (количество пакетов, количество мегабайт, количество минут), опции показа пакетов, резолвинг имен. В большинстве случаев эти параметры можно оставить по умолчанию. Итак, всё готово к началу перехвата, осталось нажать кнопку Start.

После нажатия на кнопку Start начался перехват пакетов. Если сетевая активность высокая, то можно сразу увидеть массу непонятных входящих или исходящих пакетов. Теперь мы займемся изучением известной утилиты ping.

Утилита ping.

Нажмем Win+R и введем в строке выполнить cmd. Откроется консоль, введем там команду ping <IP адрес>. IP адрес следует писать, исходя из конфигурации конкретной сети. Теперь, если опрос хоста прошел так же успешно, откроем окно Wireshark, чтобы посмотреть на это более подробно. Там скорее всего увидим сложности и разбираться в этом нужно будет очень долго. Тут нам на помощь и придут фильтры.

Утилита ping работает по протоколу ICMP, поэтому впишем название этого протокола в строку фильтра и нажмем Apply. Должно получиться нечто похожее на рис.15. Здесь можем наблюдать как происходит Echo Request и Echo Reply в протоколе ICMP изнутри: какие тестовые данные посылаются, какие флаги символизируют о том, что это именно Echo Request, и другую не менее важную информацию.

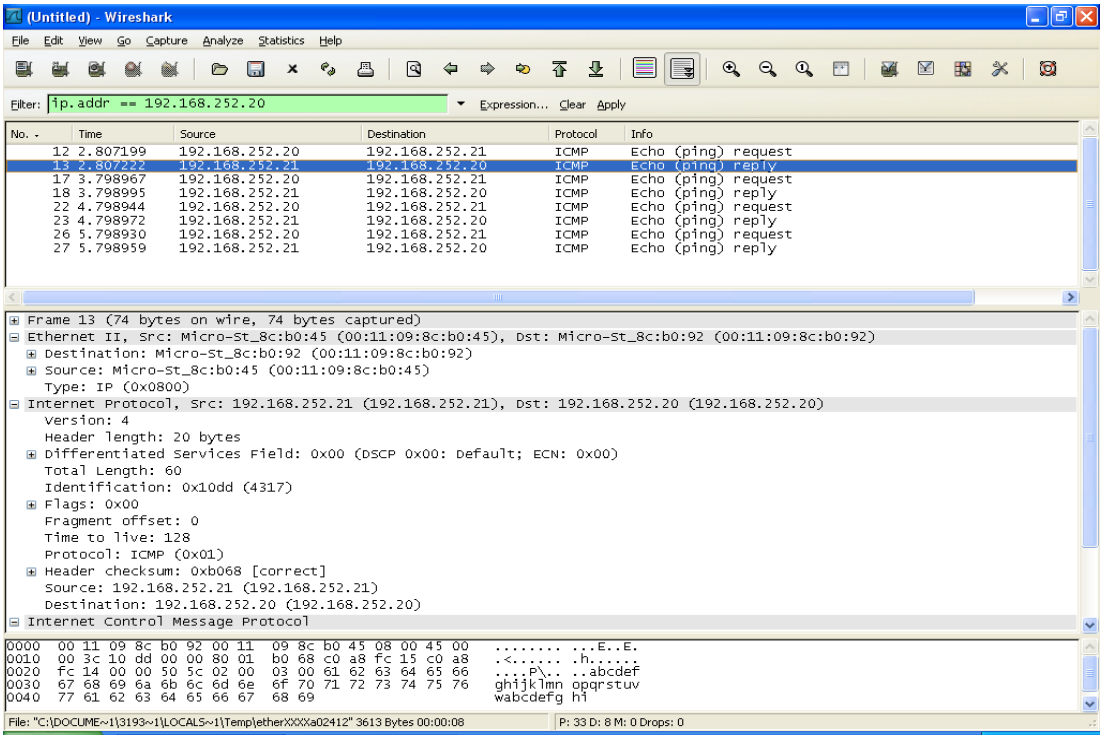


Рис.15. Фильтрация по протоколу ICMP

Перехват FTP трафика. В этом пункте рассматривается перехват документа, передающегося по протоколу FTP без шифрования, и убедимся, что при использовании шифрования на основе TLS ничего полезного мы перехватить не сможем. В качестве FTP сервера используется Cerberus FTP Server, в качестве клиента – любой браузер, например, Internet Explorer (в данной работе использовался плагин к Mozilla Firefox под названием FireFTP).

Запускаем захват пакетов в Wireshark и делаем фильтр по протоколу FTP для удобства (набираем «ftp or ftp-data» без кавычек). Набираем в строке адреса браузера адрес нашего FTP сервера: ftp://<IP адрес сервера> и жмем Enter. На сервере будет лежать текстовый документ под названием test.txt, скачиваем его. Теперь посмотрим, что произошло в снифере, и какие пакеты мы перехватили. Перехватить можно не только данные, которые передаются

по протоколу, но и логин с паролем. Теперь найдем в перехваченных пакетах содержание нашего документа. Несколько слов о процессе передачи файлов по протоколу FTP: в самом начале сервер посылает клиенту баннер приветствия (в данном случае это 220-Welcome to Cerberus FTP Server), пользователь проходит аутентификацию на сервере с помощью команд USER и PASS, получает список директорий с помощью команды LIST и запрашивает нужный файл с помощью команды RETR. Команду RETR мы и будем искать в списке пакетов. Для этого нужно нажать Ctrl+F, выбрать в опциях поиска Find by String и Search in Packet Bytes, в строке поиска ввести RETR и нажать Enter. Будет найден пакет, в котором клиент посылает эту команду серверу, если файл существует, то сервер пришлет ответ 150 Opening data connection, а в следующем пакете и будет содержимое документа. Проблема снифинга была актуальной раньше – в сетях основанных на концентраторах (хабах) – она остается актуальной и сейчас для сетей на коммутаторах (свитчах), благодаря такой технологии как ARP spoofing. Более того, сегодня семимильными шагами развивается технологии беспроводных сетей, где снифинг возможен даже в пассивном режиме.

Единственным решением, препятствующим снифингу, является шифрование. Нельзя допускать использования фирменных небезопасных прикладных протоколов или унаследованных протоколов, передающих данные явным образом. Замена небезопасных протоколов (таких как telnet) на их надежные шифрованные аналоги (такие как SSH) представляется серьезным барьером от перехвата. Замена всех небезопасных протоколов в большинстве случаев маловероятна.

3.9. Особенности раскрытия компьютерных преступлений

Для того чтобы обнаружить компьютерных преступников (хакера),

требуется:

- хорошее программное обеспечение текущего контроля;
- регулярная проверка системных журналов;
- «следящая» система.

Предположив, что программное обеспечение находится в порядке, наиболее очевидные следы преступления могут быть разделены на две категории: ***внешние и внутренние.***

Внешними следами, связанными с попытками внедриться в коммуникационную линию связи, являются:

- выведенные из строя сигнальные устройства на кабелях связи;
- усиление затухания сигналов в оптической линии связи;
- изменения в напряжении, емкости, сопротивлении или частоте.

Внутренними следами, связанными с попыткой получить доступ через обычный входной набор или по дистанционному тракту, являются:

- телефонные звонки различной длительности в комнату, когда после ответа можно услышать посылки модема, указывающие на атаку, проводимую путем последовательного автоматического набора диска;
- повторяемые безуспешно попытки входа в систему;
- повторяющая передача управляющих команд;
- частое использование подсказок;
- неразрешенная или незапланированная работа;
- оскорбительные или клеветнические сообщения;
- уничтоженная или испорченная информация;
- перемещенные или измененные файлы и вновь созданные справочники;
- жалобы заказчиков, поставщиков и пользователей на возникающие время от времени ошибки и трудности входа и работы в системе.

Организация должна постараться хоть на один шаг опередить хакера. Информация о начинающем преступнике может быть собрана, например, с помощью:

- обращения к местному почтовому ящику, чтобы проверить наличие учетной информации о фирме в секции злоумышленника;
- поддержания связи с отделом кадров, занимающимся проблемами недовольных или чем-то обеспокоенных служащих;
- использования других хакеров в качестве информаторов без ознакомления их с деталями системы данной фирмы, например, через третьих лиц.

Чтобы обнаружить потенциальную активность промышленного шпиона или профессионального хакера, фирма должна освоить самые разные методы:

– обнаружить попытки кражи можно, например, скрытой камерой, направленной на мешки с распечатками, приготовленными к вывозу;
– проверить благонамеренность всех посетителей, в частности специалистов по средствам связи, электриков, водопроводчиков, а также торговых агентов.

Особо опасными местами являются арендованные несколькими фирмами помещения, где нередко в течение дня можно увидеть 10-15 разного рода специалистов, стремящихся получить доступ в главный узел связи. При этом идентификационные карточки, удостоверяющие личность, проверяются крайне редко. Известно, что, используя коридоры и переходы в зданиях, специалисты проводят в помещения посторонних лиц.

От специалистов следует требовать предъявления стандартной идентификационной карточки с фотографией и документа, показывающего, какого рода работу выполняет данное лицо.

Всегда следует сверять по телефону заранее подготовленный шифр или

код получившего отказ сообщения. От специалиста необходимо требовать, чтобы он фиксировал шифр входа в главный узел связи, отмечая в журнале:

- дату и время посещения;
- фамилию, имя;
- название фирмы, для которой выполняется работа;
- факт проверки идентификационной карточки.

Регистрационный журнал должен периодически проверяться. Все посетители должны быть идентифицированы. Если пришедший покупатель или специалист по маркетингу, он должен предъявить удостоверение своей фирмы и номер телефона, по которому непосредственно можно навести справки. Штат должен быть предупрежден о том, каких посетителей следует остерегаться. Подозрительными могут быть:

- посторонние лица, утверждающие, что они ищут в данном здании человека или фирму, которой нет в перечне учреждений, арендующих данное помещение;
- потенциальные клиенты, желающие в деталях узнать о данной фирме, но вместе с тем, однако, упомянув о цели своего визита - большом заказе, старающиеся не вдаваться в подробности относительно их фирмы.

Штат секретарей обычно плохо обучен тому, как распознать и какие предпринять действия против энергичного, настойчивого посетителя, не желающего уходить без информации, за которой он пришел. В подобных случаях секретарю нужно проявить твердость и выпроводить посетителя или вызвать помощников. Однако чаще в этих случаях информация выдается секретарем раньше, чем возникает подозрение. Чтобы предотвратить утечку секретной информации, должна осуществляться политика «чистых столов»: никакие документы не должны оставаться на столах после окончания рабочего времени, и все ненужные бумажки должны быть разорваны перед

выбросом их в корзину.

Система реагирования должна быть устроена таким образом, чтобы все жалобы, поступившие от посетителей, просителей и пользователей, сопоставлялись и анализировались. В этом должны помочь пакеты статистического анализа, которые контролируют такие необычные явления, как, например:

- каждый вечер в одно и то же время системы начинают давать сбой;
- появляются ошибочные сообщения;
- наблюдаются ошибки при передаче;
- наблюдается расхождение результатов.

Как только возникают подозрения, что возможны разведывательные действия или преступление, должно быть предпринято полномасштабное расследование.

Предупреждение преступлений хакеров. Большое число преступлений можно предотвратить, если следовать основным правилам:

- фирма не должна публиковать телефонные номера коммутируемых портов и обязана иметь адрес бывшего директора в системе коммутации;
- после установления связи и до момента входа пользователя в систему, последняя не должна выдавать никакой информации;
- в системе необходимо использовать пароли, состоящие не менее чем из семи знаков, и коды пользователей должны отличаться от предлагаемых фирмой-изготовителем;
- должна быть реализована программа динамических паролей для гарантии их постоянной смены при увольнении служащих из данной фирмы;
- функции терминалов должны быть точно определены, например платежные ведомости должны вводиться только через

определенные терминалы.

Чтобы помешать преступникам, политикам, ведущим подрывную деятельность, экстремистам получить несанкционированный доступ, необходимо технологию защиты увязать с технологическими процессами организации. Должна быть проведена оценка риска, с тем чтобы затраты на средства управления и контроля соответствовали степени риска, с тем чтобы затраты на средства управления и контроля соответствовали степени риска. Организация должна искать средства для снижения мотивации преступлений в системе путем введения:

- паролей и процедур персональной идентификации;
- средств контроля за операционной системой;
- контроля доступа;
- контроля за базой данных;
- контроля за сетью.

Основные выводы

Предупредить компьютерное преступление всегда намного легче и проще, чем его раскрыть и расследовать.

Выделяются три основные группы мер предупреждения компьютерных преступлений, составляющие в своей совокупности целостную систему борьбы с этим явлением: правовые, организационно-технические и криминалистические.

Большая часть компьютерных преступлений совершается вследствие недостаточности организационных мер в предприятиях и организациях, слабой защитой данных от НСД, недостаточной конфиденциальности, слабой проверки и инструктажа персонала.

Домен - область (ветвь) иерархического пространства доменных имен

сети Интернет, которая обозначается уникальным доменным именем.

Термин Whois - это протокол, через который сервер может передать информацию клиенту о том, на кого зарегистрирован домен или его IP-адрес.

Лог - это журнал автоматической регистрации событий, которые фиксируются в рамках какой-либо программы. Обычно каждому событию соответствует одна запись в логе и запись вносится сразу же после события.

Логирование событий в ОС является одной из трех составляющих безопасности:- authentication, authorization, accounting - аутентификация, авторизация, аудит.

Кейлоггером является любой компонент ПО или оборудования, который умеет перехватывать и записывать все манипуляции с клавиатурой компьютера. Нередко кейлоггер находится между клавиатурой и ОС и перехватывает все действия пользователя.

Программные кейлоггеры принадлежат к той группе программных продуктов, которые осуществляют контроль над деятельностью пользователя персонального компьютера.

Аппаратные кейлоггеры представляют собой миниатюрные приспособления, которые могут быть прикреплены между клавиатурой и компьютером или встроены в саму клавиатуру.

Акустические кейлоггеры представляют собой аппаратные устройства, которые вначале записывают звуки, создаваемые пользователем при нажатии на клавиши клавиатуры компьютера, а затем анализирующие эти звуки и преобразовывающие их в текстовый формат.

Перехват трафика может осуществляться: «прослушиванием» сетевого интерфейса; подключением снифера в разрыв канала; ответвлением (программным или аппаратным) трафика и направлением его копии на снифер; через анализ побочных электромагнитных излучений; через атаку на канальном (MAC-spoofing) или сетевом уровне (IP-spoofing).

Снифер представляет собой программу или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов и он применяется как в благих, так и в деструктивных целях.

Wireshark – это анализатор сетевого трафика и его задача состоит в том, чтобы перехватывать сетевой трафик и отображать его в детальном виде.

Wireshark используется для решения проблем в сети, для отладки сетевых приложений, для изучения внутреннего устройства сетевых протоколов.

Следы преступления могут быть разделены на две категории: внешние и внутренние.

Внешними следами являются: выведенные из строя сигнальные устройства на кабелях связи; усиление затухания сигналов в оптической линии связи; изменения в напряжении, емкости, сопротивлении или частоте.

Внутренними следами являются: телефонные звонки, повторяемые безуспешно попытки входа в систему; частое использование подсказок; оскорбительные или клеветнические сообщения; уничтоженная или испорченная информация; перемещенные или измененные файлы.

Вопросы для самоконтроля

1. *Перечислите основные причины и условия, способствующие совершению компьютерных преступлений.*
2. *Какие организационные мероприятия предупреждения компьютерных преступлений существуют?*
3. *Каковы механизмы установления принадлежности и расположения IP-адреса?*
4. *Каковы механизмы установления принадлежности доменного*

имени?

5. *Что такое Who is?*
6. *Что означает лог-файл?*
7. *Какие данные в логах присутствуют?*
8. *Какие же данные можно найти в логах веб-сервера?*
9. *Что необходимо, чтобы узнать о действиях злоумышленника, получить какие-либо данные о нем при помощи логов?*
10. *Различия системных логов операционных систем Windows, UNIX и Linux.*
11. *Сформулируйте классификацию кейлоггеров.*
12. *Назовите методы защиты от кейлоггеров.*
13. *Как осуществляется перехват трафика?*
14. *Для чего используется Wireshark?*
15. *Что требуется для того чтобы обнаружить компьютерных преступников (хакера)?*
16. *Какие категории следов преступления могут быть?*

4. РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ И СТЕГАНОГРАФИЯ В ЦИФРОВОЙ КРИМИНАЛИСТИКЕ

4.1. Этапы расследования инцидента

В организации и компании отсутствует методика определения инцидентов, а сотрудники не знают, какие события являются инцидентами. Это особенно важно в случае инцидентов информационной безопасности - они не всегда мешают нормальной работе. Например, инцидентом безопасности будет оставление без присмотра на столе конфиденциальных документов, на что никто может и не обратить внимания, а злоумышленник (который может быть сотрудником компании) такие документы заметит. На этапе расследования инцидентов основную роль играют: ведение журналов регистрации событий, четкое разделение полномочий пользователей, ответственность за выполненные действия – важны доказательства того, кто участвовал в инциденте и какие действия он выполнял. Как только последствия инцидента устранены и бизнес-процессы восстановлены, дальнейшие действия по расследованию инцидента и осуществлению корректирующих и превентивных мер не выполняются.

Инцидент – любое событие, которое не является частью стандартных операций сервиса и вызывает или может вызвать прерывание обслуживания или снижение качества сервиса (Рис.16).

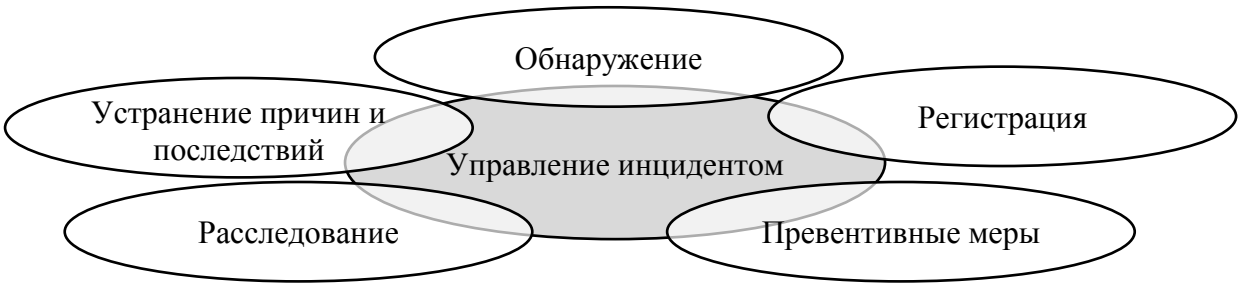


Рис.16. Инцидент информационной безопасности

Расследование инцидентов преследует несколько основных целей:

- локализация и ликвидация последствий инцидентов ИБ;
- установление виновных лиц и их мотивации, обеспечение возможности привлечения их к ответственности;
- анализ инцидентов и принятие мер по предотвращению подобных в будущем.

Могут быть сформулированы и другие, частные цели, преследуемые конкретным расследованием конкретного инцидента. Единой методики проведения расследования не существует, но в общем случае в ходе расследования выполняются следующие действия:

- сбор свидетельств и их анализ;
- выявление виновных и установление меры их ответственности;
- установление причин, давших возможность инциденту произойти;
- вынесение рекомендаций по принятию мер по предотвращению инцидентов;
- хранение и защита материалов расследования.

Остановимся подробнее на некоторых важных этапах.

Сбор свидетельств инцидента ИБ – важнейшая часть процесса независимо от того, в каких целях проводится расследование. От качества собранных свидетельств в немалой степени зависит его успех, поэтому свидетельства должны отвечать ряду обязательных требований:

- полнота (свидетельств достаточно для объективного суждения об инциденте);
- относимость (свидетельство имеет отношение к инциденту);
- достоверность (свидетельства получены из доверенных источников и неизменны);
- допустимость (свидетельства должны быть получены легальным способом).

На начальном этапе проведения расследования сложно сказать, будут ли иметь свидетельства судебные перспективы (ведь о природе инцидента, виновнике и наличии умысла еще неизвестно), поэтому к обеспечению допустимости, достоверности и полноты следует относиться со всей серьезностью, руководствуясь принципом "дьявол прячется в мелочах". Кроме того, необходимо иметь в виду, что в случае производства по уголовному делу сбор доказательств может осуществляться только следователем или оперуполномоченным, поэтому нужно быть готовым к быстрому установлению контактов с правоохранительными органами в случае необходимости.

Основная цель проведения расследования инцидентов, вирусных заражений заключается в точном определении последствий атаки, причин и способов ее появления. Определив причины и способы возникновения атаки можно принимать корректирующие воздействия для предотвращения повторных атак и заражений. Опыт специалистов ИБ показывает, что подвергнувшаяся атаке или заражению организация не всегда может корректно определить границы случившегося инцидента, а значит оценить последствия и устранить все последствия. К сожалению, в настоящее время не существуют универсальных рекомендаций, о том, как устранять последствия атак и заражений.

Расследование инцидентов является неотъемлемой и одной из наиважнейших задач области в безопасности. Для начала следует детально рассмотреть процесс расследования инцидентов информационной безопасности. В общем случае он выглядит следующим образом (Рис.17):

Стадия №1: Оценка. На данном этапе происходит подготовка к сбору данных, имеющих отношение к инциденту информационной безопасности, т. е. исследуется возможность проведения расследования (получается разрешение на проведение расследования, анализируются применимые

политики и законы); определяется состав группы, которая будет проводить расследование; изучается топология сети, в которой произошел инцидент; определяются источники криминалистически значимой информации и т. д.

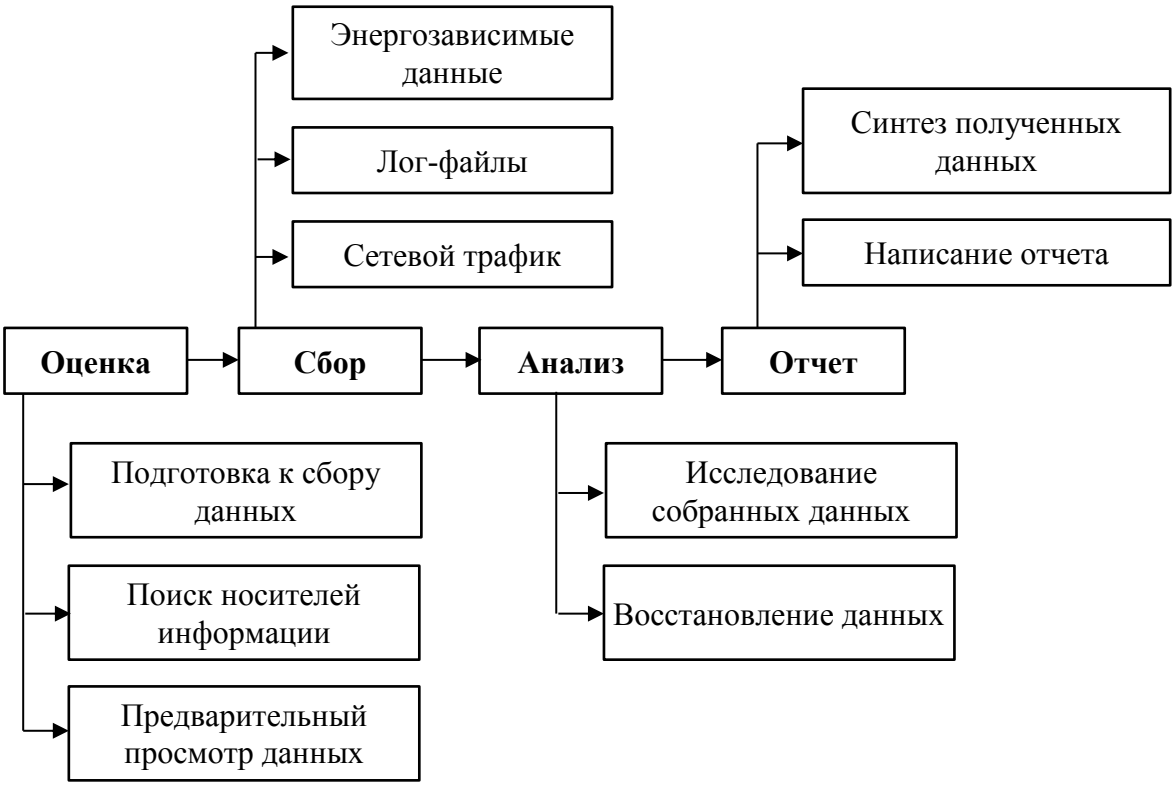


Рис.17. Процесс расследования инцидентов информационной безопасности

Кроме того, на этапе оценки определяется круг компьютерных носителей информации, имеющих отношение к инциденту.

Стадия №2: Сбор. На этой стадии собираются все данные, имеющие отношение к инциденту. Они включают в себя:

- содержимое энергонезависимых носителей информации (жесткие диски, компакт-диски, накопители USB Flash и т.п.);
- содержимое энергозависимых носителей информации (оперативная память);
- лог-файлы сетевого оборудования, серверов;

- сетевой трафик.

Сбор вышеперечисленных данных заключается в создании их копии специализированными средствами.

Содержимое энергонезависимых носителей информации. Перед созданием копии энергонезависимого носителя информации необходимо обеспечить целостность (неизменность) его содержимого, для чего применяются программные и аппаратные блокираторы записи, а также специализированные операционные системы. Если компьютер, в котором установлен носитель информации, который нужно скопировать (или изъять), работает, то его работа завершается прерыванием электропитания после сбора энергозависимых данных, либо сразу, если энергозависимые данные собирать не надо; в особых случаях (например, при невозможности отключения критически важных серверов) допустимо копировать энергонезависимые данные с работающей системы.

Блокираторы записи позволяют подключить исследуемый носитель информации без риска записи на него каких-либо данных по вине операционной системы или сторонних программ.

Аппаратные блокираторы записи выполняют свои функции вне зависимости от применяемых для чтения данных операционных систем и программ. Специализированные операционные системы, как правило, применяются для копирования носителей информации без их извлечения из исследуемого компьютера за счет загрузки на его аппаратном обеспечении доверенной (криминалистической) программной среды. Обычно такие операционные системы загружаются с CD или накопителей USB Flash и включают в себя программные блокираторы записи, запускаемые в процессе загрузки. Примеры таких операционных систем:

- grml;
- CAINE Live CD;

- DEFT Linux;
- e-fense Helix3 Pro.

Для непосредственного копирования данных могут применяться следующие программы:

- dd (входит в состав почти всех дистрибутивов Linux);
- dc3dd- модифицированная версия dd;
- aimage;
- FTK Imager.

Следует отметить, что копирование содержимого энергонезависимых носителей информации перед исследованием не является обязательным шагом - в случаях, когда обеспечивается целостность содержимого оригинальных носителей (т.е. в случаях исправности носителей и при использовании блокираторов записи), исследование копий вместо оригиналов проводить нецелесообразно.

Сбор энергозависимых данных производится с работающих систем перед их выключением. Как правило, процесс сбора энергозависимых данных заключается в копировании:

- содержимого оперативной памяти компьютера;
- содержимого примонтированных зашифрованных файловых систем и сетевых хранилищ;
- списков работающих процессов и сервисов;
- списков текущих сетевых соединений и открытых портов;
- сетевой конфигурации исследуемой системы;
- переменных окружения;
- изображения, которое видит пользователь на экране монитора (создание снимка экрана).

Для копирования этих данных к работающей исследуемой системе может подключаться внешний носитель, с которого производится запуск

специализированной программы, собирающей данные. Иногда специализированная программа загружается в систему по сети. Скопированные данные могут сохраняться на внешний носитель или передаваться по сети на доверенный сервер.

Копирование логов может производиться несколькими способами:

- копированием только записей, имеющих отношение к инциденту (например, относящихся к определенному IP-адресу или промежутку времени);
- копированием лог-файлов целиком;
- копированием всего носителя информации.

Основными факторами при выборе того или иного способа копирования являются: степень доверия логам и, соответственно, объем исследования, направленного на определение степени корректности и неизменности лог-файлов. Если вероятность злонамеренного изменения или фальсификации лог-файлов мала, то допустимо копировать только лог-файлы или отдельные их записи. В противном случае целесообразно копировать содержимое всего носителя информации (для дальнейшего поиска следов несанкционированного доступа к системе, следов модификации лог-файлов и т.д.).

Стадия №3: Анализ. На этом этапе производится анализ всех собранных данных, который может проводиться по следующему алгоритму:

- получение общих сведений об исследуемом объекте (диске, копии диска, дампе сетевого трафика и т. п.);
- исследование данных в явном виде;
- исследование данных в неявном (удаленном, скрытом, зашифрованном) виде.

Исследование энергонезависимых носителей информации и их копий в большинстве случаев заключается в исследовании содержимого файловых

систем и в восстановлении данных. Криминалистическое исследование файловых систем заключается в анализе различного рода информационных следов, возникающих в результате действий злоумышленника, работы программного и аппаратного обеспечения исследуемой системы. Количество таких следов (как источников криминалистически значимой информации) в файловых системах велико, в связи с чем отсутствуют какие-либо исчерпывающие методики и алгоритмы проведения криминалистических исследований файловых систем при расследовании инцидентов.

Для криминалистического исследования файловых систем могут применяться следующие программные продукты:

- EnCase Forensic;
- Forensic Toolkit;
- The Sleuth Kit.

Для восстановления данных могут применяться следующие программы:

- Foremost;
- PhotoRec.

Анализ дампов сетевых пакетов может использоваться:

- для определения характеристик сетевых пакетов и соединений (например, с целью поиска скрытых каналов передачи данных);
- для извлечения сообщений, передаваемых по сети (например, с целью поиска каналов утечки информации).

В первом случае могут применяться анализаторы сетевых пакетов, например:

- Wireshark;
- Network Miner.

Во втором случае, как правило, используются не анализаторы сетевых пакетов, а системы легального перехвата, которые позволяют

автоматизировать процессы поиска, выделения и сохранения сетевых сообщений различных типов (сообщений электронной почты, Интернет-пейджеров и т. д.), а также производить поиск по ключевым словам и другим критериям в перехваченных данных.

Стадия №4: Отчет. На данной стадии производится синтез всей информации, полученной на этапе анализа, с последующим написанием отчета в форме, понятной аудитории, для которой он предназначен. Отчет может включать в себя:

- сведения о причинах возникновения инцидента;
- сведения о лицах, причастных к инциденту;
- хронологию инцидента;
- детальное описание следов (доказательств), обнаруженных на этапе анализа;
- сведения об использованных в процессе расследования методиках, программных и аппаратных средствах, обстоятельствах их применения;
- рекомендации по предотвращению подобных инцидентов в будущем.

Информирование об инцидентах. Сперва необходимо получить информацию об инциденте. Этот момент необходимо продумать ещё на этапе формирования политики безопасности и создания презентаций по ликбезу в ИБ для сотрудников.

Основные источники информации:

1. ***Helpdesk.*** Как правило (и это хорошая традиция) о любых неполадках, неисправностях или сбоях в работе оборудования звонят или пишут в хелпдеск вашей IT-службы. Поэтому необходимо заранее «встроиться» в бизнес-процесс хелпдеска и указать те виды инцидентов, с которыми заявку будут переводить в отдел информационной безопасности.

2. ***Сообщения непосредственно от пользователей.*** Организуйте

единую точку контакта, о чём сообщите в тренинге по ИБ для сотрудников. На данный момент отделы ИБ в организациях, как правило, не очень большие, зачастую из 1-2 человек. Поэтому будет несложно назначить ответственного за приём инцидентов, можно даже не заморачиваться с выделением адреса электрон почты под нужды IS Helpdesk.

3. ***Инциденты, обнаруженные сотрудниками ИБ.*** Тут всё просто, и никаких телодвижений для организации такого канала приёма не требуется.

4. ***Журналы и оповещения систем.*** Настройте оповещения в консоли антивируса, IDS, DLP и других систем безопасности. Удобнее использовать аггрегаторы, собирающие данные также из логов программ и систем, установленных в организации. Особое внимание нужно уделить точкам соприкосновения с внешней сетью и местам хранения чувствительной информации.

4.2. Управление инцидентами

Управление инцидентами - одна из важнейших процедур управления информационной безопасностью и в цифровой криминалистики. Прежде всего, важно правильно и своевременно устранить последствия инцидента, а также иметь возможность проконтролировать, какие действия были выполнены для этого. Необходимо также расследовать инцидент, что включает определение причин его возникновения, виновных лиц и конкретных дисциплинарных взысканий. Далее, как правило, следует выполнить оценку необходимости действий по устранению причин инцидента, если нужно – реализовать их, а также выполнить действия по предупреждению повторного возникновения инцидента. Кроме этого, важно сохранять все данные об инцидентах информационной безопасности, так как статистика инцидентов информационной безопасности помогает осознавать

их количество и характер, а также изменение во времени. С помощью информации о статистике инцидентов можно определить наиболее актуальные угрозы для компании и, соответственно, максимально точно планировать мероприятия по повышению уровня защищенности информационной системы компании. Здесь приведены только основные причины необходимости создания отдельной документированной и утвержденной процедуры управления инцидентами информационной безопасности, но и их достаточно, чтобы осознать всю важность данной процедуры. Во многих компаниях не всегда возможно проследить за изменением количества и характера инцидентов информационной безопасности – отсутствует процедура управления инцидентами. Часто отсутствие инцидентов не указывает на то, что система управления безопасностью работает правильно, а означает только, что инциденты не фиксируются или не определяются. Как правило, основные сложности при управлении инцидентами вызывают следующие моменты.

Оповещение о возникновении инцидента. Сотрудники компании зачастую не осведомлены о том, кого и в какой форме следует ставить в известность при возникновении инцидента, – например, не определены ни формы отчетов, ни перечень лиц, которым необходимо отправлять отчеты об инцидентах. Даже если сотрудник заметит, что его коллега уносит для работы домой конфиденциальные документы компании, он не всегда знает, какие действия следует предпринимать в данной ситуации.

Регистрация инцидента. Ответственным лицам часто не предоставляется методика регистрации инцидентов – не существует специальных журналов их регистрации, а также правил и сроков заполнения. В качестве примера инцидентов можно привести такие события, как неавторизованное изменение данных на сайте компании, оставление компьютера незаблокированным без присмотра, пересылка

конфиденциальной информации с помощью корпоративной или личной почты. Поскольку инцидентом, в первую очередь, является неразрешенное событие, оно должно быть кем-то запрещено, следовательно, необходимо наличие документов, четко описывающих все действия, которые можно выполнять в системе и которые выполнять запрещено. Например, в одной из компаний сотрудник хранил на мобильном компьютере конфиденциальные сведения компании без применения средств шифрования. После работы он забрал компьютер домой и забыл его в машине, которую оставил под окнами дома, а ночью машину взломали, и компьютер был украден. Злоумышленники получили доступ к конфиденциальной информации компании и могли продать ее конкурентам. Кроме этого, на компьютере хранилась ценная информация, которая не была зарезервирована на другом носителе. Такой инцидент мог произойти в результате того, что в компании не были разработаны процедуры обращения с мобильными компьютерами и хранения на них информации. Вынос компьютера за пределы офиса компании, отсутствие средств шифрования и резервного копирования информации – возможные нарушения, а следовательно, причины инцидентов.

Однако пока документально не зафиксировано, что это нарушения (т.е. в соответствующих документах не описано, что это запрещено), сотрудника невозможно привлечь к ответственности и предотвратить повторное выполнение неправомерных действий. Важно, чтобы были налажены такие процедуры, как мониторинг событий, своевременное удаление неиспользуемых учетных записей, контроль и мониторинг действий пользователей, контроль над действиями системных администраторов и пр. В одной из компаний был зафиксирован следующий инцидент: при увольнении с работы системный администратор украл разрабатываемый в компании программный продукт и передал его конкурентам, которые выпустили

программу на рынок под своим товарным знаком. Кроме этого, он внес изменения в информационную систему, в результате которых после его ухода функционирование определенных ее компонентов было нарушено. Привлечь администратора к ответственности в данном случае оказалось невозможно, так как, во-первых, не выполнялась регистрация его действий, во-вторых, администратор мог удалить все доказательства своих неправомерных действий и, в-третьих, не была налажена процедура сбора улик об инциденте. Кроме этого, в компании просто не знали, как следует поступать в таких случаях.

Обнаружение и регистрация инцидента. Инцидент информационной безопасности может заметить пользователь или администратор системы. Как правило, администраторы знают, что следует делать в случае обнаружения инцидентов, чего не всегда можно сказать о пользователях. Для пользователей следует разработать инструкцию, которая, как правило, содержит описание, в каком виде сотрудник должен сообщить о возникновении инцидента, координаты ответственных лиц, а также перечень действий, которые сотрудник может выполнить самостоятельно (или предупредить о том, что выполнять какие-либо действия самостоятельно запрещено). Такой отчет должен содержать подробное описание инцидента, перечисление сотрудников, вовлеченных в инцидент, фамилию сотрудника, зафиксировавшего инцидент и дату возникновения и регистрации инцидента. Таким образом, каждый сотрудник получает инструкцию, определяющую, каковы должны быть его действия, например, в случае, если он продолжил работу с документом и заметил, что с прошлого раза в его документ были внесены изменения, не соответствующие действительности, при этом автор изменений неизвестен.

Далее требуется разработать инструкцию для специалиста, в обязанности которого входит регистрация инцидента. Сотрудник,

обнаруживший инцидент, связывается с сотрудником, ответственным за регистрацию инцидента и выполнение дальнейших действий. В небольших компаниях сотрудники обращаются напрямую к специалисту, который может устранить последствия и причины инцидента. В достаточно крупных компаниях, как правило, выделяют сотрудника, который регистрирует инцидент и передает информацию об инциденте соответствующим специалистам. Такая инструкция может содержать, например, правила и срок регистрации инцидента, перечень необходимых первоначальных инструкций для сотрудника, обнаружившего инцидент, кроме того, описание порядка передачи информации об инциденте соответствующему специалисту, порядок контроля за устранением последствий и причин инцидента.

Обнаружение инцидента всегда сопряжено со стрессом. Сотрудники должны знать все необходимые действия, шаг за шагом ведущие к устранению инцидента (Рис.18).

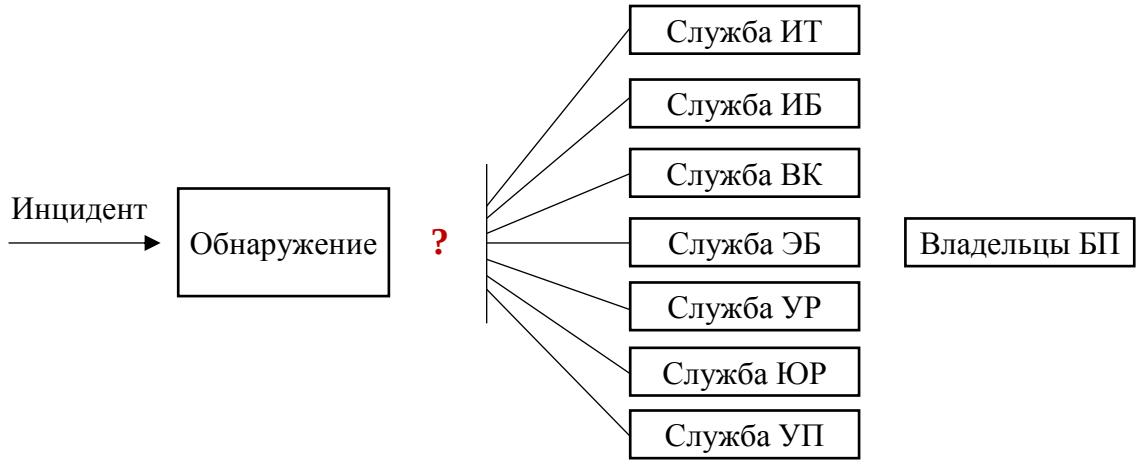


Рис.18. Обнаружение инциденты информационной безопасности

ИТ-служба информационных технологий.

ИБ-служба информационной безопасности.

ВК-служба внутреннего контроля.

ЭБ-служба экономической безопасности.

УР-служба управления рисками.

ЮР-юридическая служба.

УП-служба управления персоналом.

БП-владельцы бизнес-процессов.

В подобной ситуации, при отсутствии четких инструкций и должного уровня обучения, процесс реагирования на инциденты превращается в стохастические попытки выявления и устранения инцидентов. Зачастую функции, которые чётко должен выполнять один человек, «размазываются» между несколькими сотрудниками, которые в результате действуют параллельно и лишь теряют драгоценное время.

Устранение причин и последствий инцидента и его расследование. Инструкция по устранению причин и последствий инцидента включает описание общих действий, которые необходимо предпринять (конкретные действия для каждого вида инцидента определять трудоемко и не всегда целесообразно), а также сроки, в течение которых следует устранить последствия и причины инцидента. Сроки устранения последствий и причин инцидента зависят от уровня инцидента. Следует разработать классификацию инцидентов — определить количество уровней критичности инцидентов, описать инциденты каждого уровня и сроки их устранения. Документ, определяющий, какие события в компании следует считать инцидентом, также может описывать и уровни инцидентов.

Таким образом, инструкция по устранению последствий и причин инцидента может включать: описание действий, предпринимаемых для устранения последствий и причин инцидента, сроки устранения и указание на ответственность за несоблюдение инструкции.

Расследование инцидента включает в себя определение виновных в его возникновении, сбор доказательств и улик инцидента, определение

соответствующих дисциплинарных взысканий. В крупных компаниях, как правило, выделяют комиссию по расследованию инцидентов информационной безопасности (в состав которой может входить сотрудник, регистрирующий инциденты). Инструкция по расследованию инцидентов должна описывать: действия по расследованию инцидента (в том числе определение виновных в его возникновении), правила сбора и хранения улик (особенно в случае, если может потребоваться использование улик в судебных органах) и правила внесения дисциплинарных взысканий.

4.3. Категорирование и классификация инцидента

Хоть инциденты безопасности разнообразны и многообразны, их довольно легко разделить на несколько категорий, по которым проще вести статистику.

1. Разглашение конфиденциальной или внутренней информации, либо угроза такого разглашения. Для этого необходимо иметь, как минимум, актуальный перечень конфиденциальной информации, рабочую систему грифования электронных и бумажных носителей. Хороший пример - шаблоны документов, практически на все случаи жизни, находящиеся на внутреннем портале организации или во внутренней файлопомойке, по умолчанию имеют проставленный гриф «Только для внутреннего использования».

2. Несанкционированный доступ. Для этого необходимо иметь список защищаемых ресурсов. То есть тех, где находится какая-либо чувствительная информация организации, её клиентов или подрядчиков. Причём желательно внести в эту категорию не только проникновения в компьютерную сеть, но и несанкционированный доступ в помещения.

3. Превышение полномочий. В принципе можно объединить этот

пункт с предыдущим, но лучше всё-таки выделить, объясню почему. Несанкционированный доступ подразумевает доступ тех лиц, которые не имеют никакого легального доступа к ресурсам или помещениям организации. Это внешний нарушитель, не имеющий легального входа в вашу систему. Под превышением полномочий же понимается несанкционированный доступ к каким-либо ресурсам и помещениям именно легальных сотрудников организации.

4. Вирусная атака. В этом случае необходимо понимать следующее: единично заражение компьютера сотрудника не должно повлечь за собой разбирательство, так как это можно списать на погрешность или пресловутый человеческий фактор. Если же заражен ощутимый процент компьютеров организации, то необходимо разворачивать полновесную отработку инцидента безопасности с необходимыми поисками источников заражения, причин и т.д.

5. Компрометация учетных записей. Этот пункт перекликается с 3. Фактически инцидент переходит из 3 в 5 категорию, если в ходе расследования инцидента выясняется, что пользователь в этот момент физически и фактически не мог использовать свои учётные данные.

Основной целью проведения ***классификации инцидентов ИБ*** является повышение степени системности и минимизация субъективности при реализации процессов реагирования на инциденты, осуществляемые путем определения и фиксации атрибутов инцидента для дальнейшего их использования в ходе реагирования на инцидент, а также при анализе системы менеджмента инцидентов ИБ.

Инциденты ИБ рекомендуется классифицировать по следующим признакам:

- по степени вероятности повторного возникновения инцидента;
- по видам источников угроз, вызывающих инциденты;

- по преднамеренности возникновения инцидента (случайный, намеренный, ошибочный);
- по видам объектов информационной инфраструктуры, задействованных (пораженных) при реализации инцидента;
- по уровню информационной инфраструктуры, на котором происходит инцидент;
- по нарушенным свойствам информационной безопасности (конфиденциальность, целостность, доступность);
- по типу инцидента (свершившийся инцидент, попытка осуществления инцидента, подозрение на инцидент);
- по области распространения и действия инцидента;
- по сложности обнаружения инцидента;
- по сложности закрытия инцидента.

Инциденты под следствием. Утечки данных неизменно вызывают тревогу не только у специалистов ИБ, но и у владельцев бизнеса и топ-менеджеров. Они заинтересованы в том, чтобы предотвращать утечки, и вместе с тем предпочитают обходиться достаточно простыми и не очень затратными способами защиты. В частности, снизить риски утечек помогает взвешенный подход к выбору основных инструментов сотрудников, посредством которых они получают доступ к корпоративной информации.

Опасности, связанные с утечкой корпоративных данных, делятся на внешние и внутренние. В первом случае мы имеем дело с несанкционированным доступом или кражей данных, которые осуществил человек, не являющийся сотрудником организации. Во втором случае вольной или невольной причиной утраты, подделки или утечки данных явился сотрудник организации – инсайдер. Даже если произошла серьезная потеря денежных средств, службы безопасности банков, как правило, не желают делиться внутренней информацией с посторонними. При

возникновении инцидента первой задачей является максимально быстрое пресечение негативного влияния события на различные системы. Ключевая идея такого реагирования в том, что сам по себе инцидент не так важен, как использованный в данном инциденте канал, дающий злоумышленникам возможность получить в один момент тысячу повторений инцидента. Уже после этого проводится внутреннее расследование (или «обработка» инцидента) с выявлением существующих уязвимостей. Важнейшая задача на этом этапе - исключить повторение данного события в дальнейшем.

4.4. Элементы расследования инцидентов

Расследование инцидента включает в себя определение виновных в его возникновении, сбор доказательств и улик инцидента, определение соответствующих дисциплинарных взысканий. В крупных компаниях, как правило, выделяют комиссию по расследованию инцидентов информационной безопасности (в состав которой может входить сотрудник, регистрирующий инциденты). Инструкция по расследованию инцидентов должна описывать: действия по расследованию инцидента (в том числе определение виновных в его возникновении), правила сбора и хранения улик (особенно в случае, если может потребоваться использование улик в судебных органах) и правила внесения дисциплинарных взысканий.

Рассмотрим 5 элементов расследования компьютерных инцидентов.

Элемент 1. Что взломано?

Важно определить,

- *какая именно система пострадала в результате инцидента;*
- *какой именно сервис был скомпрометирован;*
- *какие именно данные были скомпрометированы.*

Оказывается, для этой цели можно использовать заранее

подготовленный пакет утилит оперативного реагирования, который поможет определить, что именно взломано в результате инцидента. Какие именно утилиты будут входить в этот пакет и как именно будут использоваться.

Во-первых, нужно уметь идентифицировать и собрать данные, которые могут *исчезнуть* в короткий промежуток времени, это могут быть временные файлы, cookies, но не только.

Во-вторых, нужно научиться анализировать *сетевые подключения* и активность системы на предмет наличия отклонений от обычного состояния.

В-третьих, нужно научиться анализировать *процессы*, в них выполняется код, а так как процессы выполняют код, расположенный в исполняемых файлах и библиотеках, здесь же обратим внимание на целостность этих файлов.

В-четвертых, процессы используют хранилище параметров, *реестр*, его анализ может открыть больше информации, и нам помогут различные утилиты просмотра реестра.

В-пятых, все процессы выполняются в *памяти*, поэтому анализ памяти также важен для расследования.

Сложностью является то, что память большая, а вредоносные данные небольшие и легко теряются в шестнадцатеричном дампе.

Компрометация или нарушение целостности данных может быть замечена также системой *аудита* и системой *мониторинга* сетевого трафика.

Элемент 2. Посредством чего взломано?

Важно определить,

- *была ли ошибка в конфигурации;*
- *была ли ошибка в приложении;*
- *была ли ошибка в системе;*
- *была ли ошибка в протоколе.*

Под каждую тему отведем модуль, чтобы детально изучить, чем могут

помочь информация о процессах, ключах реестра, файлах, всевозможные дампы и журналы.

Здесь нужно научиться одной важной вещи: соотношению событий, записей журналов и конфигурации системы. Для этого нужно понимать, что журналы могут быть у каждого сервиса свои, храниться могут как локально, так и на удаленном сервере, а также разные платформы могут использовать разные форматы журналов.

Элемент 3. Кто взломал?

Важно определить,

- *через какую систему произошло вторжение;*
- *какова была конечная цель атаки;*
- *с какого компьютера началась атака.*

Снова пригодится умение соотносить информацию разных журналов с событиями, сопровождающими инцидент безопасности. Но на этом этапе нужно уметь из собранной на предыдущих шагах информации выделить идентификаторы злоумышленника. Это не обязательно должен быть IP, это может быть адрес электронной почты, учетная запись в приложении, медиа-файл.

Элемент 4. На компьютере подозреваемого.

Важно определить,

- *какое программное обеспечение использовалось;*
- *какие файлы использовались;*
- *в какой последовательности совершалась атака.*

Действия зависят от того, включен компьютер подозреваемого, или нет. Если выключен, то, согласно методологии, больше не включаем, а дублируем образ диска и затем с помощью таких инструментов, как AccessData FTK и EnCase обнаруживаем улики и составляем отчет. Возможен и вариант нахождения улик не на компьютере, а на любом другом

оборудовании, ксероксе, принтере, мобильном устройстве.

Элемент 5. Обоснование предыдущих элементов.

Важно определить,

- *что является уликой;*
- *как собирать улики;*
- *как анализировать улики;*
- *как оформить отчет о расследовании.*

Дампы, журналы, файлы – компьютерные термины. Чтобы их можно было приобщить к формализованному процессу расследования, они должны быть оформлены как улики, и обрабатываться в соответствии с процедурами, сохраняющими юридическую значимость улик.

Суть расследования такова: специалисты организации обнаруживают инцидент, и, либо своими силами оперативно реагируют на инцидент, анализируют данные и передают результаты анализа руководству, либо нанимают аутсорсера по расследованию компьютерных инцидентов, который обеспечит техническое и юридическое сопровождение расследования до передачи дела правоохранительным органам и в суд.

Даже если организация не имеет намерения проводить юридически значимые расследования инцидентов, знание и умение применить методологию расследования хакерских инцидентов повысит общую защищенность информационной системы предприятия.

4.5. Прецедентный анализ инцидентов

Прецедентный анализ. В прецедентных системах поиск решения базируется на понятии аналогии (поиск от частного к частному). Прецедент и текущая ситуация представляются объектами, для которых необходимо обнаружить аналогию и благодаря переносу фактов, справедливых для

прецедента, сделать некоторое заключение относительно рассматриваемого инцидента. Как правило, прецедент состоит:

- из описания проблемной ситуации;
- совокупности действий, предпринимаемых для устранения данной проблемы (решения задачи);
- и в некоторых случаях – результата (или прогноза) применения решения.

В качестве наиболее очевидной структуры прецедента можно привести параметрическое представление многомерным вектором:

$$CASE = (x_1, x_2, \dots x_p, R),$$

где, $x_1, x_2, \dots x_p -$ параметры ситуации, описываемой данным прецедентом;

$R -$ одно или множество решений данной задачи (диагноз, рекомендации).

Вывод на основе прецедентов включает в себя четыре основных этапа, образующих CBR-цикл (цикл рассуждения на основе прецедентов), которыми являются:

- извлечение подобных прецедентов для сложившейся ситуации из базы прецедентов;
- повторное использование прецедента для попытки решения текущей проблемы;
- пересмотр и адаптация решения в соответствии с текущей проблемой;
- сохранение вновь принятого решения как части нового прецедента.

С учетом специфики конкретной предметной области и решаемых задач может использоваться упрощенный CBR-цикл. Таким образом, основная цель использования аппарата прецедентов заключается в выдаче готового решения оператору. Извлечение прецедентов основывается на

определении функции подобия (метрики) F, значение которой определяет сходство прецедента и текущей ситуации. В пространстве признаков определяется точка, соответствующая целевой проблеме, и в рамках используемой метрики выбирается ближайший прецедент.

Формально аналогия прецедента

$g = (x_{g1}, x_{g2}, \dots x_{gp})$ и текущей ситуации;

$k = \left(x_{k1}, x_{k2}, \dots x_{kp}\right)$ описывается функцией вида.

$$SIM(g,k) = F(sim\left(x_{g1}, x_{k1}\right), \dots, sim(x_{gp}, x_{kp})),$$

где $sim(x_{gi}, x_{ki})$ локальная схожесть значений $i-$го признака прецедента g и $i-$го признака текущей ситуации (инцидента) k. Функция F выражает полную схожесть прецедента с текущей ситуацией. В случае отсутствия аналогичных прецедентов в базе данный подход не приведет к необходимому решению для возникшей ситуации. Данная проблема может быть разрешена, если в CBR-цикле будет предусмотрена возможность пополнения базы непосредственно в процессе рассуждения (вывода). Концепция применения прецедентного анализа. Первым шагом управления инцидентами информационной безопасности является непосредственно регистрация инцидентов. Дальнейшие действия предполагают применение стратегий реагирования для каждого инцидента с учетом класса. На данном этапе можно выделить следующие проблемы:

- не всегда классификация инцидентов производится корректно;
- не существует единой стратегии реагирования на инциденты определенного класса в силу того, что каждый инцидент в той или иной мере индивидуален;
- имеют место инциденты, не имевшие место ранее и, следовательно, для таких инцидентов отсутствуют подходящие стратегии реагирования.

Концепция применения прецедентного анализа для совершенствования

процесса управления инцидентами заключается в следующем. Имеется множество G известных инцидентов, множество R определенных стратегий реагирования. Отображение $G \to R$ есть прецедент, т.е. пара, содержащая описание инцидента и соответствующей ему стратегии реагирования. При регистрации нового инцидента, для него находится подобный прецедент, после чего решение прецедента применяется для данного инцидента. Логическая структура системы, реализующей данный подход, приведена на рис.19.

Инциденты, не известные ранее и для которых нет определенной стратегии реагирования, будем называть аномальными инцидентами.

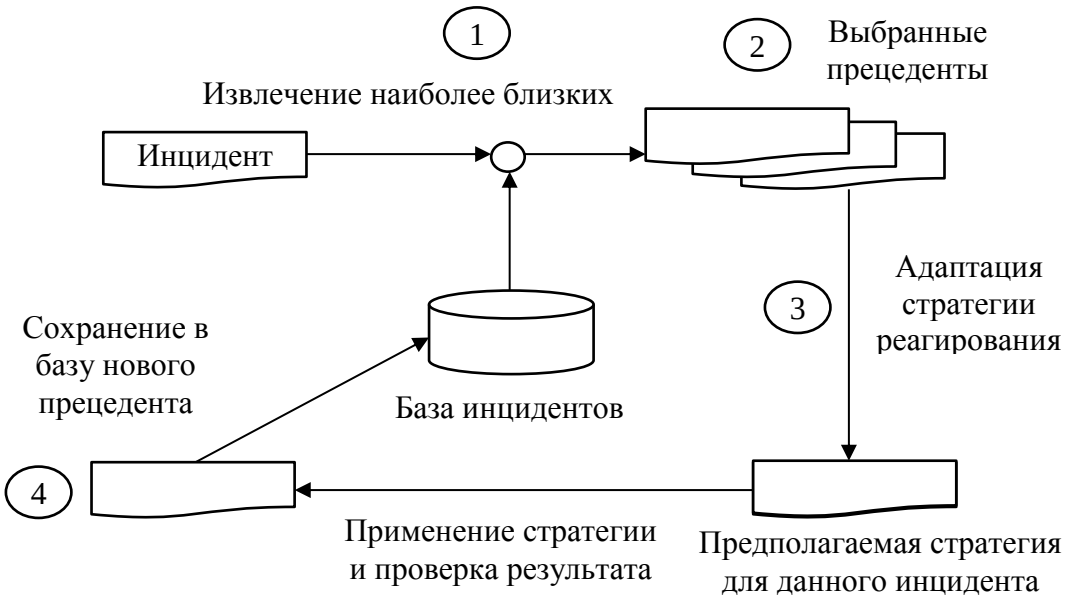


Рис.19. Логическая структура системы прецедентного анализа

Другими словами, под аномальным инцидентом понимается инцидент, не имеющий аналогов в рамках класса, к которому он отнесен средством защиты. Заключение об аномальности инцидента дает повод для детального анализа. С учетом этого прецедентный анализ сводится к классификации

инцидентов на нормальные и аномальные исходя из количества найденных аналогий:

$G = \{g_1, \dots, g_n\} -$ множество прецедентов; $g_i = (x_1, \dots, x_p, r_i) -$ единичный прецедент; $K = \{k_1, \dots, k_m\} -$ множество зарегистрированных инцидентов; $k_j = \{x_1, \dots, x_p\} -$ единичный инцидент; $F(g_i, k_j) -$ функция подобия; $G_1 = \{g_i : F(g_i, k_j) \le d_{lim}\} -$ множество подобных прецедентов.

Таким образом, условие отнесение инцидента к множеству прецедентов формулируется следующим образом: $k_j \in G \leftrightarrow |G_1| \ge a_{lim}$

Как видно, результат классификации напрямую зависит от предельного расстояния d_{lim} и предельного количества аналогий a_{lim}.

Модель алгоритма прецедентного анализа. В качестве метрического классификатора применялся метод k −ближайших соседей. Тестовый сценарий алгоритма реализован в аналитической платформе Deductor Studio Academic и включает в себя следующие этапы (Рис.20):

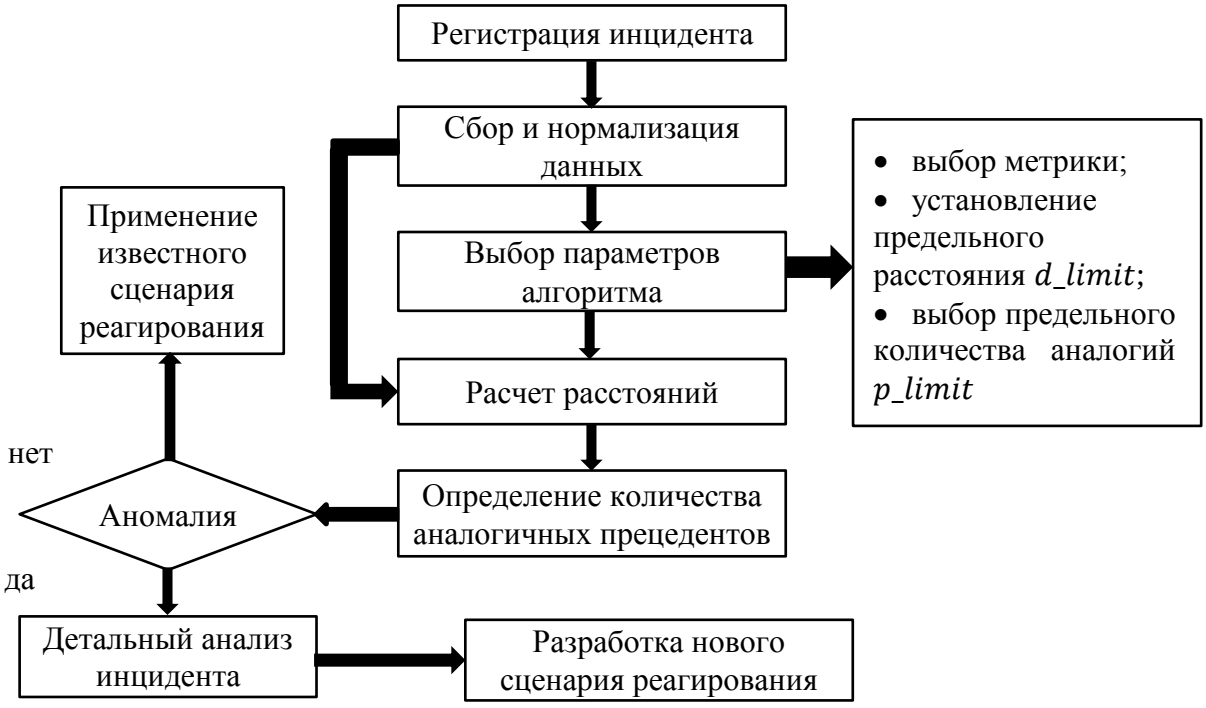


Рис.20. Внедрение анализа инцидентов в процесс управления

После регистрации инцидента проводится его нормализация:

$$x_{\text{норм}} = \frac{x - x_{min}}{x_{max} - x_{min}}.$$

1. Инициализация параметров алгоритма: выбор метрики, определение предельного расстояние d_{lim} и предельного значения аналогий a_{lim}. В качестве начального значения d_{lim} принято расстояние по классу, где среднее расстояние единичного прецедента до класса

$$d_{cp} = \frac{\sum_{i=1}^{n} d_{i_{cp}}}{n},$$

2. Расчет расстояний между объектами по метрики

$$d_{i_{cp}} = \sqrt{\sum_{i=1}^{p} (x_{gi} - x_{ki})^2}.$$

3.Определение пар объектов, для которых справедливо $d_{gk} \leq d_{lim}$ (прецедент g и инцидент k считаются подобными).

4. Для каждой инцидента k_j рассчитывается число a прецедентов, для которых выполняется

$$d_{gk} \leq d_{lim}.$$

5. Инцидент k_j рассматривается как аномалия при $a \leq a_{lim}$.

6. Принимаются дальнейшие действия исходя из результата классификации: детальный анализ инцидентов либо применение стратегии реагирования, соответствующей наиболее аналогичному прецеденту. Параметры алгоритма варьируются в ходе функционирования системы, за счет чего совместно с пополнением базы прецедентов реализуется обучение системы.

Архитектура системы прецедентного анализа. С точки зрения программной реализации система прецедентного анализа имеет модульную структуру и включает в себя следующие компоненты (Рис.21):

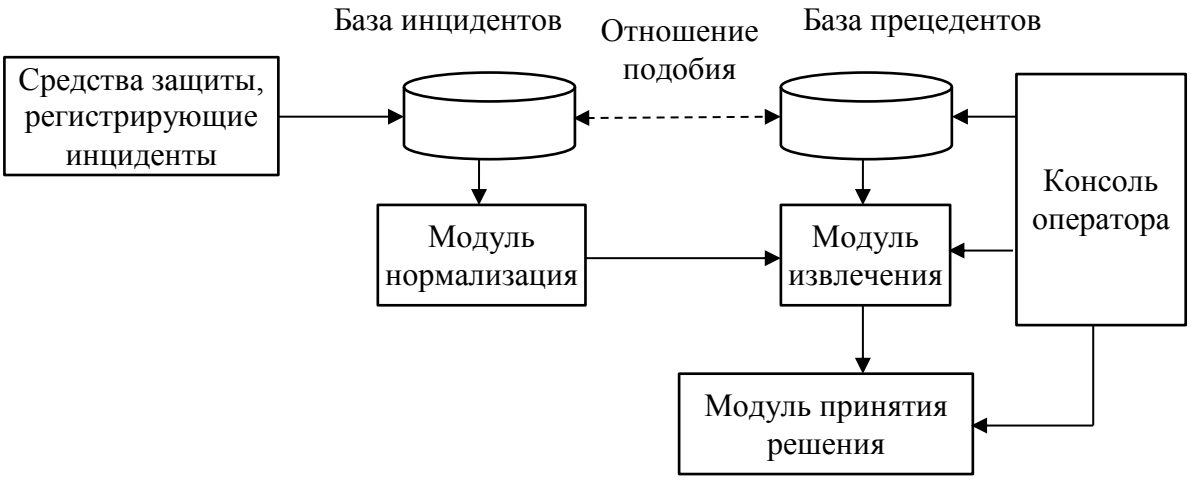


Рис.21. Архитектура системы прецедентного анализа

1) базу инцидентов, содержащая записи о зарегистрированных инцидентах, ожидающих дальнейшей обработки;
2) модуль нормализации данных, преобразовывающий базу зарегистрированных инцидентов в соответствии со структурой базы прецедентов;
3) модуль принятия решений, определяющий результат классификации и ставящий инцидент в соответствие одному или нескольким прецедентам на основе рассчитанных мер подобия;
4) консоль оператора, предназначенная для коррекции процесса анализа и адаптации выработанной стратегии под ранее неизвестные условия.

Таким образом, применение концепции прецедентного анализа, в качестве инструмента, совершенствующего процесс управления инцидентами информационной безопасности, позволит повысить оперативность реагирования на инциденты, путем многократного применения накопленного опыт. Кроме того, данный подход позволяет решить задачу обнаружения аномальных инцидентов, являющихся наиболее критичными и требующих детального изучения.

4.6. Цифровая стеганография

Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. Уже в древнем мире выделилось два основных направления решения этой задачи, существующие и по сегодняшний день. Для защиты информации уже придумано множество методов и алгоритмов, которые можно отнести к одному из двух направлений: криптография, стеганография.

Целью криптографии является скрытие содержимого сообщений за счет их шифрования. В отличие от этого, при стеганографии скрывается сам факт существования тайного сообщения.

Слово **«стеганография»** имеет греческие корни и буквально означает **«тайнопись».** Исторически направление стенографического скрытия информации предшествовало криптографии. Однако со временем исследования в области стеганографии значительно сократились, и данная наука во многих сферах была вытеснена криптографией. Тайнопись осуществляется самыми различными способами. Общей чертой этих способов является то, что скрываемое сообщение встраивается в некоторый безобидный, не привлекающий внимание объект. Затем этот объект открыто транспортируется адресату. При криптографии наличие шифрованного сообщения само по себе привлекает внимание противников, при стеганографии же наличие скрытой связи остается незаметным.

Развитие средств вычислительной техники в последнее десятилетие дало новый толчок для развития компьютерной стеганографии. Появилось много новых областей применения. Сообщения встраивают теперь в цифровые данные, как правило, имеющие аналоговую природу. Это – речь, аудиозаписи, изображения, видео.

Стеганография - это метод организации связи, который собственно

скрывает само наличие связи. В отличие от криптографии, где неприятель точно может определить является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.

Стеганографическая техника является одним из разделов общего направления по сокрытию информации. Стеганографии существуют и другие направления, изучающие методы сокрытия информации. Это - криптография, всевозможные сигнальные системы и условные знаки, маскировка и введение в заблуждение, наконец, различные толкования одних и тех же фраз и др.

Выделяется несколько направлений стеганографии:

- классическая стеганография;
- компьютерная стеганография;
- цифровая стеганография.

Классическая стеганография представляет собой различные методы сокрытия сообщения без использования компьютера, и, как правило, без использования сложных технических средств.

На сегодняшний день классическая стеганография использует целый ряд методов сокрытия информации в передаваемых и хранимых документах. Это невидимые чернила, микроточки, акростих, трафареты и т.д.

Компьютерная стеганография изучает способы сокрытия информации в компьютерных данных, представляющих собой различные файлы, программы, пакеты протоколов и т.п. С учетом общей компьютеризации всех областей человеческой деятельности, в настоящее время очень трудно провести различие между цифровой и компьютерной стеганографией. Подобно тому, как в системах связи аналоговые сигналы (аудио, видео) преобразуются в форму дискретных последовательностей или потоков, которые разбиваются на пакеты и передаются по сети,

компьютерные данные, соответствующие изображениям, звуковым или видеофрагментам, представляются в виде файлов или передаются в виде пакетов по компьютерной сети.

Примеры - стеганографическая файловая система StegFS для Linux, скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганография и т.д. Приведём некоторые примеры:

- Использование зарезервированных полей компьютерных форматов файлов - суть метода состоит в том, что часть поля расширений, не заполненная информацией о расширении, по умолчанию заполняется нулями. Соответственно мы можем использовать эту «нулевую» часть для записи своих данных. Недостатком этого метода является низкая степень скрытности и малый объём передаваемой информации.
- Метод скрытия информации в неиспользуемых местах гибких дисков - при использовании этого метода информация записывается в неиспользуемые части диска, к примеру, на нулевую дорожку. Недостатки: маленькая производительность, передача небольших по объёму сообщений.
- Метод использования особых свойств полей форматов, которые не отображаются на экране - этот метод основан на специальных «невидимых» полях для получения сносок, указателей. К примеру, написание чёрным шрифтом на чёрном фоне. Недостатки: маленькая производительность, небольшой объём передаваемой информации.
- Использование особенностей файловых систем - при хранении на жёстком диске файл всегда занимает целое число кластеров. К примеру, в ранее широко используемой файловой системе FAT32 стандартный размер кластера – 4 КБ. Соответственно для хранения 1 КБ информации на диске выделяется 4 КБ памяти, из которых 1 КБ

нужен для хранения сохраняемого файла, а остальные 3 ни на что не используются - соответственно их можно использовать для хранения информации. Недостаток данного метода: лёгкость обнаружения.

Цифровая стеганография - направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа-объектами и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов. Кроме того, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования; далее, при воспроизведении этих объектов появляется дополнительный аналоговый шум и нелинейные искажения аппаратуры, все это способствует большей незаметности сокрытой информации.

Сетевая стеганография. В последнее время приобрели популярность методы, когда скрытая информация передается через компьютерные сети с использованием особенностей работы протоколов передачи данных. Такие методы получили название «сетевая стеганография». Типичные методы сетевой стеганографии включают изменение свойств одного из сетевых протоколов. Кроме того, может использоваться взаимосвязь между двумя или более различными протоколами с целью более надежного сокрытия передачи секретного сообщения. Сетевая стеганография охватывает широкий спектр методов, в частности:

- **WLAN-стеганография** основывается на методах, которые используются для передачи стеганограмм в беспроводных сетях (Wireless Local Area Networks). Практический пример WLAN-стеганографии — система HICCUPS (Hidden Communication System for Corrupted Networks).

- **LACK-стеганография** — скрытие сообщений во время разговоров с использованием IP-телефонии. Например: использование пакетов, которые задерживаются или намеренно повреждаются и игнорируются приемником (этот метод называют LACK — Lost Audio Packets Steganography) или сокрытие информации в полях заголовка, которые не используются.

В настоящее время методы компьютерной стеганографии развиваются по двум основным направлениям:

1. Методы, основанные на использовании специальных свойств компьютерных форматов;
2. Методы, основанные на избыточности аудио и визуальной информации.

Первое направление основано на использовании специальных свойств компьютерных форматов представления данных, а не на избыточности самих данных. Специальные свойства форматов выбираются с учетом защиты скрываемого сообщения от непосредственного прослушивания, просмотра или прочтения. Основным направлением компьютерной стеганографии является использование избыточности аудио и визуальной информации. Цифровые фотографии, цифровая музыка, цифровое видео — представляются матрицами чисел, которые кодируют интенсивность в дискретные моменты в пространстве и/или во времени. Цифровая фотография — это матрица чисел, представляющих интенсивность света в определенный момент времени. Цифровой звук — это матрица чисел, представляющая интенсивность звукового сигнала в последовательно идущие моменты времени. Все эти числа не точны, т.к. не точны устройства оцифровки аналоговых сигналов, имеются шумы квантования. Младшие разряды цифровых отсчетов содержат очень мало полезной информации о текущих параметрах звука и визуальнного образа. Их заполнение ощутимо не

влияет на качество восприятия, что и дает возможность для скрытия дополнительной информации.

Стеганографическая система или **стегосистема** - совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

При построении стегосистемы должны учитываться следующие положения:

– противник имеет полное представление о стеганографической системе и деталях её реализации. Единственной информацией, которая остаётся неизвестной потенциальному противнику. Является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;
– если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения в других данных до тех пор, пока ключ хранится в тайне;
– потенциальный противник должен быть лишён каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

Обобщённая модель стегосистемы представлена на рис.22.

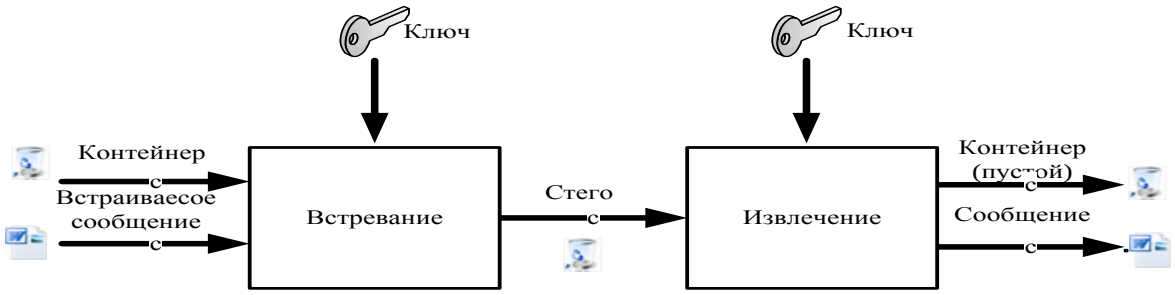


Рис.22. Обобщенная модель стегосистемы

В качестве данных может использоваться любая информация: текст, сообщение, изображение и т.п. В общем же случае целесообразно использовать слово «сообщение», так как сообщением может быть как текст или изображение, так и, например, аудиоданные. Далее для обозначения скрываемой информации, будем использовать именно термин сообщение.

Контейнер - любая информация, предназначенная для сокрытия тайных сообщений.

Пустой контейнер - контейнер без встроенного сообщения; заполненный контейнер или стего - контейнер, содержащий встроенную информацию.

Встроенное (скрытое) сообщение - сообщение, встраиваемое в контейнер.

Стеганографический канал или просто стегоканал - канал передачи стего.

Стегоключ или просто ключ - секретный ключ, необходимый для сокрытия информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.

По аналогии с криптографией, по типу стегоключа стегосистемы можно подразделить на два типа:

- с секретным ключом;
- с открытым ключом.

В стегосистеме с секретным ключом используется один ключ, который должен быть определен либо до начала обмена секретными сообщениями, либо передан по защищенному каналу.

В стегосистеме с открытым ключом для встраивания и извлечения сообщения используются разные ключи, которые различаются таким образом, что с помощью вычислений невозможно вывести один ключ из

другого. Поэтому один ключ (открытый) может передаваться свободно по незащищенному каналу связи. Кроме того, данная схема хорошо работает и при взаимном недоверии отправителя и получателя.

Цифровая стеганография как наука родилась буквально в последние годы. По нашему мнению она включает в себя следующие направления:

1) встраивание информации с целью ее скрытой передачи;
2) встраивание цифровых водяных знаков (watermarking);
3) встраивание идентификационных номеров (fingerprinting);
4) встраивание заголовков (captioning).

4.7. Цифровые водяные знаки

Цифровые водяные знаки (ЦВЗ) могут применяться, в основном, для защиты от копирования и несанкционированного использования. В связи с бурным развитием технологий мультимедиа остро встал вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде. Примерами могут являться фотографии, аудио и видеозаписи и т.д. Преимущества, которые дают представление и передача сообщений в цифровом виде, могут оказаться перечеркнутыми легкостью, с которой возможно их воровство или модификация. Поэтому разрабатываются различные меры защиты информации, организационного и технического характера. Один из наиболее эффективных технических средств защиты мультимедийной информации и заключается во встраивании в защищаемый объект невидимых меток — ЦВЗ. Разработки в этой области ведут крупнейшие фирмы во всем мире.

Слово «незаметном» в нашем определении цифровой стеганографии подразумевает обязательное включение человека в систему стеганографической передачи данных. Человек здесь может рассматриваться

как дополнительный приемник данных, предъявляющий к системе передачи достаточно трудно формализуемые требования.

прекодер - устройство, предназначенное для преобразования скрываемого сообщения к виду, удобному для встраивания в сигнал-контейнер. (Контейнером называется информационная последовательность, в которой прячется сообщение);

стегокодер - устройство, предназначенное для осуществления вложения скрытого сообщения в другие данные с учетом их модели;

стегодетектор - устройство, предназначенное для определения наличия стегосообщения;

декодер - устройство, восстанавливающее скрытое сообщение.

В стегодетекторе происходит обнаружение ЦВЗ в защищенном ЦВЗ изображении. Это изменение может быть обусловлено влиянием ошибок в канале связи, операций обработки сигнала, преднамеренных атак нарушителей. Во многих моделях стегосистем сигнал-контейнер рассматривается как аддитивный шум. Тогда задача обнаружения и выделения стегосообщения является классической для теории связи. Однако такой подход не учитывает двух факторов: неслучайного характера сигнала контейнера и требований по сохранению его качества. Эти моменты не встречаются в известной теории обнаружения и выделения сигналов на фоне аддитивного шума. Их учет позволит построить более эффективные стегосистемы.

Различают стегодетекторы, предназначенные для обнаружения факта наличия ЦВЗ и устройства, предназначенные для выделения этого ЦВЗ (стегодекодеры). В первом случае возможны детекторы с жесткими (да/нет) или мягкими решениями. Для вынесения решения о наличии/отсутствии ЦВЗ удобно использовать такие меры, как расстояние по Хэммингу, либо взаимную корреляцию между имеющимся сигналом и оригиналом (при

наличии последнего, разумеется). А что делать, если у нас нет исходного сигнала? Тогда в дело вступают более тонкие статистические методы, основанные на построении моделей исследуемого класса сигналов. В последующих главах этот вопрос будет освещен подробнее.

Наибольшее применение могут иметь открытые стегосистемы ЦВЗ, которые аналогичны системам скрытой передачи данных. Наибольшую устойчивость по отношению к внешним воздействиям имеют закрытые стегосистемы I типа.

Рассмотрим подробнее понятие контейнера. До *стегокодера* - это пустой контейнер, после него - заполненный контейнер, или стего. Стего должен быть визуально неотличим от пустого контейнера. Различают два основных типа контейнеров: *потоковый и фиксированный*.

Потоковый контейнер представляет собой непрерывно следующую последовательность бит. Сообщение вкладывается в него в реальном масштабе времени, так что в кодере неизвестно заранее, хватит ли размеров контейнера для передачи всего сообщения. В один контейнер большого размера может быть встроено и несколько сообщений. Интервалы между встраиваемыми битами определяются генератором псевдослучайной последовательности с равномерным распределением интервалов между отсчетами.

У фиксированного контейнера размеры и характеристики заранее известны. Это позволяет осуществлять вложение данных оптимальным в некотором смысле образом. В книге мы будем рассматривать, в основном, фиксированные контейнеры.

Контейнер может быть выбранным, случайным или навязанным. Выбранный контейнер зависит от встраиваемого сообщения, а в предельном случае является его функцией. Этот тип контейнера больше характерен для стеганографии. Навязанный контейнер может появиться в сценарии, когда

лицо, предоставляющее контейнер, подозревает о возможной скрытой переписке и желает предотвратить ее. На практике же чаще всего сталкиваются со случайным контейнером.

ЦВЗ могут быть трех типов: *робастные, хрупкие и полухрупкие (semifragile).*

Под робастностью понимается устойчивость ЦВЗ к различного рода воздействиям на стегосистем.

Хрупкие ЦВЗ разрушаются при незначительной модификации заполненного контейнера. Они применяются для аутентификации сигналов. Отличие от средств электронной цифровой подписи заключается в том, что хрупкие ЦВЗ все же допускают некоторую модификацию контента. Это важно для защиты мультимедийной информации, так как законный пользователь может, например, пожелать сжать изображение. Другое отличие заключается в том, что хрупкие ЦВЗ должны не только отразить факт модификации контейнера, но также вид и местоположение этого изменения.

Полухрупкие ЦВЗ устойчивы по отношению к одним воздействиям и неустойчивы по отношению к другим. Вообще говоря, все ЦВЗ могут быть отнесены к этому типу. Однако полухрупкие ЦВЗ специально проектируются так, чтобы быть неустойчивыми по отношению к определенного рода операциям. Например, они могут позволять выполнять сжатие изображения, но запрещать вырезку из него или вставку в него фрагмента.

Важной проблемой является определение подлинности полученной информации, то есть ее аутентификация. Обычно для аутентификации данных используются средства цифровой подписи. Однако, эти средства не совсем подходят для обеспечения аутентификации мультимедийной информации. Дело в том, что сообщение, снабженное электронной цифровой подписью, должно храниться и передаваться абсолютно точно, «бит в бит».

Мультимедийная же информация может незначительно искажаться как при хранении (за счет сжатия), так и при передаче (влияние одиночных или пакетных ошибок в канале связи). При этом ее качество остается допустимым для пользователя, но цифровая подпись работать не будет. Получатель не сможет отличить истинное, хотя и несколько искаженное сообщение, от ложного. Кроме того, мультимедийные данные могут быть преобразованы из одного формата в другой. При этом традиционные средства защиты целостности работать также не будут. Можно сказать, что ЦВЗ способны защитить именно содержание аудио-видео сообщения, а не его цифровое представление в виде последовательности бит. Кроме того, важным недостатком цифровой подписи является то, что ее легко удалить из заверенного ею сообщения, после чего приделать к нему новую подпись. Удаление подписи позволит нарушителю отказаться от авторства, либо ввести в заблуждение законного получателя относительно авторства сообщения. Рассмотрим основные области применения водяных знаков для защиты данных:

1. Широковещательный контроль.
2. Идентификация владельца.
3. Доказательство права собственности.
4. Отслеживание взаимодействий.
5. Аутентификация данных.
6. Контроль незаконного копирования.
7. Управление устройством.
8. Совместимость разных технологий.

Широковещательный контроль.

Играет немаловажную роль в телерадиовещании. Так, например, в Японии в 1997 году разразился скандал по поводу трансляции телевизионной рекламы. Рекламодатели платили деньги за показ реклам, которая не

транслировалась в эфире телевизионных станций. Этот обман рекламодателей длился более чем 20 лет, так как не было систем контроля трансляции реклам.

Рассмотрим два основных типа контроля вещания: пассивные и активные системы контроля:

- Активные системы контроля направлены на определение соответствия информации, транслируемой вместе с контентом;
- Пассивные системы контроля реализуется посредством распознания содержания передач.

Проанализируем различия между двумя этими типами. В пассивных системах контроля компьютер осуществляет процесс контролирования вещания. В ходе этого процесса он сравнивает полученные сигналы со своей базой данных, включающей данные каких-либо известных телепередач, фильмов, песен и т.д. При обнаружении совпадений происходит идентификация и данные (фильм, реклама и т.д.) поступают в эфир.

Пассивные системы контроля имеют свои недостатки. Процесс определения компьютером совпадений между поступающим сигналом и его базой данных не является тривиальным. Стоит отметить также, что само транслирование сигнала может его ухудшить. Поэтому такая система контроля не способна определить точного соответствия между сигналом и своей базой данных. Если даже удастся отладить процесс поиска в базе данных, то само хранение и управление ей может оказаться слишком дорогим из-за ее большого размера. Стоит отметить, что компании не использует пассивные системы контроля из-за их недостаточно точной системы распознавания. Рассмотрим теперь активные системы контроля, которые проще реализуется, чем пассивные системы. В данном методе компьютер передает идентификационные данные вместе с контентом. Для осуществления такой системы контроля в отдельной области транслируемого

сигнала размещается идентификационная информация. У данного метода тоже существуют недостатки. Так, например, при добавлении дополнительных данных в сигнал, он вряд ли выдержит преобразования его формата от аналогового к цифровому. Данные преобразования требуют наличия специального аппаратного обеспечения, которые смогут выполнить данные модификации. Для решения такой проблемы есть альтернативный способ кодирования идентификационной информации — это водяные знаки. Они могут находиться внутри контента, не используя сегмент сигнала транслирования. Немаловажным преимуществом этого способа является тот факт, что водяные знаки полностью совместимы с базой вещательного оборудования, которые включают аналоговые и цифровые передачи. Тем не менее, этот способ тоже имеет свои недостатки. Реализация встраивания водяного знака сложнее, чем размещение дополнительных данных. Также может оказаться, что водяные знаки могут повлиять на качество передаваемых данных, например, это может привести к ухудшению качества аудио или видео данных.

Идентификация владельца.

Многие создатели оригинальных данных используют только текстовые уведомления об авторских правах, но, не задумываясь, что они могут быть легко удалены как намеренно, так и ненамеренно. Затем такие данные, с удаленными авторскими правами, могут попасть к законопослушному гражданину, и он не сможет определить имеются ли у этих данных авторские права. Процесс установления авторских прав очень трудоемкий и не всегда удается найти автора. Для решения проблемы защиты авторских прав стали использовать водяные знаки, так как они незаметны и неразрывно связаны с данными. В таком случае автора будет легко определить по водяному знаку, используя детекторы, предназначенные для этого.

Доказательство права собственности.

Злоумышленники могут использовать чей-либо водяной знак, чтобы заявить себя обладателем каких-либо данных. Чтобы избежать подобных ситуаций, следует ограничить доступность детектора. Злоумышленник, не имея доступ к детектору, не сможет удалить водяной знак, так как это нелегкий процесс.

Отслеживание взаимодействий.

Суть данного типа заключается в следующем: водяной знак, принадлежащий определенным данным, записывает количество копирований и однозначно определяет каждую копию. Например: обладатель каких-либо данных будет ставить на каждую их копию разные водяные знаки и, в случае утечки данных, он сможет определить, кто виноват в этом.

Аутентификация данных.

Для защиты подлинности данных используют цифровые подписи, в которых находятся зашифрованные сообщения. Только правообладатель знает ключ, необходимый для создания такой подписи. У таких подписей есть недостаток — их потеря при эксплуатации. Впоследствии работа без цифровой подлинности не может пройти проверку подлинности. Решение данной проблемы заключается в непосредственном встраивании подписи в данные, защищенные водяным знаком. Такие встроенные подписи называются знаком аутентификации. Если правообладатель изменит данные, то знак аутентификации изменится вместе с ними. Благодаря такой особенности можно определить, каким способом нарушитель пытался подделать данные. Например, исследователи выдвигали такую идею: если изображение может быть разбито на блоки, каждый из которых имеет собственный встроенный знак аутентификации, то возможно определить какие фрагменты изображения были подвержены изменениям, а какие остались подлинными.

Контроль незаконного копирования.

Рассмотренные выше способы применения водяных знаков вступают в силу только после совершения каких-либо действий правонарушителя. Эти технологии позволяют обнаружить нарушителя только после совершения каких-либо незаконных действий. Поэтому этот тип рассматривает другую технологию, которая сможет помешать правонарушителю сделать незаконную копию данных, защищенную авторскими правами. Лучший контроль над незаконным копированием могут обеспечить водяные знаки, которые встроены в сами данные.

Управление устройством.

По мнению пользователей, данный тип отличается от рассмотренного выше тем, что он добавляет новые возможности к данным и не огранивает их применение. Рассмотрим пример использования такого типа. Компанией Digimarc’s Mobile System было предложено встраивать уникальные идентификаторы в изображения, используемые в газетах, журналах, рекламах и т.д. Затем, пользователь фокусирует камеру телефона на данном изображении, которая способна считать водяной знак изображения с помощью специального программного обеспечения. Идентификатор в свою очередь перенаправляет веб-браузер телефона на соответствующий сайт.

Совместимость разных технологий.

Пользователям каких-либо больших систем иногда может потребоваться их обновление для получения улучшенного функционала. Тем не менее, обновление может оказаться несовместимым со старой системой. Для решения проблемы совместимости двух разных систем и продолжения их уже совместной работы используются цифровые водяные знаки.

4.8. Атаки против систем скрытной передачи сообщений

Можно выделить следующие категории атак против стегосистем:

1. ***Атаки против встроенного сообщения*** — направлены на удаление или порчу ЦВЗ путем манипулирования стего. Входящие в эту категорию методы атак не пытаются оценить и выделить водяной знак. Примерами таких атак могут являться линейная фильтрация, сжатие изображений, добавление шума, выравнивание гистограммы, изменение контрастности и т.д.
2. ***Атаки против стегодетектора*** — направлены на то, чтобы затруднить или сделать невозможной правильную работу детектора. При этом водяной знак в изображении остается, но теряется возможность его приема. В эту категорию входят такие атаки, как аффинные преобразования (то есть масштабирование, сдвиги, повороты), усечение изображения, перестановка пикселов и т.д.
3. ***Атаки против протокола использования ЦВЗ*** — в основном связаны с созданием ложных ЦВЗ, ложных стего, инверсией ЦВЗ, добавлением нескольких ЦВЗ.
4. ***Атаки против самого ЦВЗ*** — направлены на оценивание и извлечение ЦВЗ из стегосообщения, по возможности без искажения контейнера. В эту группу входят такие атаки, как атаки сговора, статистического усреднения, методы очистки сигналов от шумов, некоторые виды нелинейной фильтрации и другие.

В соответствии с этой классификацией все атаки на системы встраивания ЦВЗ могут быть разделены на четыре группы:

- атаки, направленные на удаление ЦВЗ;
- геометрические атаки, направленные на искажение контейенера;
- криптографические атаки;
- атаки против используемого протокола встраивания и проверки ЦВЗ.

Атаки, направленные на удаление ЦВЗ. К этой группе относятся такие атаки, как очистка сигналов-контейнеров от шумов, перемодуляция,

сжатие с потерями (квантование), усреднение и коллизии. Эти атаки основаны на предположении о том, что ЦВЗ является статистически описываемым шумом. Очистка от шума заключается в фильтрации сигнала с использованием критериев максимального правдоподобия или максимума апостериорной вероятности. В качестве фильтра, реализующего критерий максимального правдоподобия, может использоваться медианный (для ЦВЗ, имеющего распределение Лапласа) или усредняющий (для гауссовского распределения) фильтр, которые применены в программном пакете StirMark. По критерию максимума апостериорной вероятности наилучшим будет адаптивный фильтр Винера (в случае если в качестве модели контейнера используется нестационарный гауссовский процесс), а также пороговые методы очистки от шума (мягкий и жесткий пороги) (модель — обобщенный гауссовский процесс), которые имеют много общего с методами сжатия с потерями.

Сжатие с потерями и очистка сигналов от шумов значительно уменьшают пропускную способность стегоканала, особенно для гладких областей изображения, коэффициенты преобразования которых могут быть «обнулены» без заметного снижения качества восстановленного изображения.

Перемодуляция - сравнительно новый метод, который является специфичным именно для атак на ЦВЗ. В настоящее время известны ее различные варианты, в зависимости от используемого в стегосистеме декодера. В построении атаки имеются свои нюансы для стегосистемы М−ичной модуляции, стегосистемы, использующей помехоустойчивые коды, использующей корреляционный декодер. В любом случае считается, что ЦВЗ внедрен в изображение с применением широкополосных сигналов и размножен на все изображение. Так как оцениваемый декодером ЦВЗ коррелирован с истинным, появляется возможность обмана декодера. Атака

строится следующим образом. Вначале ЦВЗ «предсказывается» путем вычитания фильтрованной версии изображения из защищенного изображения. «Предсказанный» ЦВЗ подвергается ВЧ фильтрации, усекается, умножается на два и вычитается из исходного изображения. Кроме того, если известно, что при внедрении ЦВЗ умножался на некоторую маску для повышения незаметности встраивания, то атакующий оценивает эту маску и домножает на нее ЦВЗ. В качестве дополнительной меры по «обману» декодера представляется эффективным встраивание в высокочастотные области изображения шаблонов, имеющих негауссовское распределение. Таким образом будет нарушена оптимальность линейного корреляционного детектора.

Такая атака будет эффективной лишь против высокочастотного ЦВЗ, поэтому реальные ЦВЗ строятся так, чтобы их спектр соответствовал спектру исходного изображения. Дело в том, что достоверная оценка получается лишь для высокочастотных компонент ЦВЗ. После ее вычитания низкочастотная компонента ЦВЗ остается неизменной и дает в детекторе положительный корреляционный отклик. Высокочастотная же составляющая даст отрицательный отклик, что в сумме даст нуль, и ЦВЗ не будет обнаружен. В качестве другого противодействия этой атаке было предложено выполнение предварительной низкочастотной фильтрации.

Еще одна эффективная атака на ЦВЗ называется ***мозаичной***. Эта атака направлена на поисковые системы, отслеживающие незаконно распространяемые изображения. Изображение разбивается на несколько частей, так что поисковая система ЦВЗ не обнаруживает. Интернет-броузер демонстрирует фактически несколько кусочков изображения, вплотную расположенных друг к другу, так что в целом изображение выглядит неискаженным. Для противодействия такой атаке ЦВЗ должен обнаруживаться даже в малых частях изображения. Это очень трудно

выполнимое требование, даже более тяжелое, чем робастность к обрезанию краев изображения, так как в последнем случае атакующий ограничен необходимостью сохранения качества изображения. Наверное, более выполнимым было бы создание интеллектуальных поисковых систем, способных «собрать» изображение из кусочков и проверить наличие в нем ЦВЗ.

Геометрические атаки. В отличии от атак удаления геометрические атаки стремятся не удалить ЦВЗ, но изменить его путем внесения пространственных или временных искажений. Геометрические атаки математически моделируются как аффинные преобразования с неизвестным декодеру параметром. Всего имеется шесть аффинных преобразований: масштабирование, изменение пропорций, повороты, сдвиг и усечение. Эти атаки приводят к потере синхронизации в детекторе ЦВЗ и могут быть локальными или глобальными. При этом возможно вырезание отдельных пикселов или строк, перестановка их местами, применение каких-то преобразований и т.д. Подобные атаки реализованы в программах Unsign (локальные атаки) и Stirmark (локальные и глобальные атаки).

Существуют и более «интеллектуальные» атаки на применяемый метод синхронизации ЦВЗ. Основная идея этих атак заключается в распознавании метода синхронизации и разрушения его путем сглаживания пиков в амплитудном спектре ЦВЗ. Атаки эффективны в предположении о том, что в качестве механизма синхронизации используются периодические шаблоны. При этом для обеспечения синхронизации могут использоваться два подхода: встраивание пиков в спектральной области, либо периодическое внедрение последовательности ЦВЗ. В обоих случаях в спектре образуются пики, которые разрушаются в рассматриваемой атаке. После разрушения можно применять другие геометрические атаки: синхронизации уже нет.

Криптографические атаки. Криптографические атаки названы так

потому, что они имеют аналоги в криптографии. К ним относятся атаки с использованием оракула, а также взлома при помощи «грубой силы».

Атака с использованием оракула позволяет создать незащищенное ЦВЗ изображение при наличии у нарушителя детектора. Метод заключается в экспериментальном изучении поведения детектора для выяснения того, на какие изображения он реагирует, на какие - нет. Например, если детектор выносит «мягкие» решения, то есть показывает вероятность наличия стего в сигнале, то атакующий может выяснить, как небольшие изменения в изображении влияют на поведение детектора. Модифицируя изображение пиксел за пикселом, он может вообще выяснить, какой алгоритм использует детектор. В случае детектора с «жестким» решением атака осуществляется возле границы, где детектор меняет свое решение с «присутствует» на «отсутствует».

Пример атаки на детектор с жестким решением:

1. На основе имеющегося изображения, содержащего стегоообщение, создается тестовое изображение. Тестовое изображение может быть создано разными путями, модифицируя исходное изображение до тех пор, пока детектор не покажет отсутствия ЦВЗ. Например, можно постепенно уменьшать контрастность изображения, либо пиксел за пикселом заменять действительные значения какими-то другими.

2. Атакующий увеличивает или уменьшает значение какого-либо пиксела, до тех пор, пока детектор не обнаружит ЦВЗ снова. Таким образом выясняется, увеличил или уменьшил значение данного пиксела ЦВЗ.

3. Шаг 2 повторяется для каждого пиксела в изображении.

4. Зная, насколько чувствителен детектор к модификации каждого пиксела, атакующий определяет пикселы, модификация которых не приведет к существенному ухудшению изображения, но нарушит работу детектора.

5. Данные пикселы вычитаются из исходного изображения.

Атаки против используемого протокола. Многие стегосистемы ЦВЗ чувствительны к так называемой инверсной атаке. Эта атака заключается в следующем. Нарушитель заявляет, что в защищенном изображении часть данных есть его водяной знак. После этого он создает ложный оригинал, вычитая эту часть данных. В ложном оригинале присутствует настоящий ЦВЗ. С другой стороны, в защищенном изображении присутствует провозглашенный нарушителем ложный ЦВЗ. Наступает неразрешимая ситуация. Конечно, если у детектора имеется исходное изображение, то собственник может быть выявлен. Другой известной атакой на протокол использования ЦВЗ является атака копирования. Эта атака заключается в оценивании ЦВЗ в защищенном изображении и внедрении оцененного ЦВЗ в другие изображения. Целью может являться, например, противодействие системе имитозащиты или аутентификации.

Краткий обзор стеганографических программ

Операционная среда Windows:

- **Steganos for Win** - является легкой в использовании, но все же мощной программой для шифрования файлов и скрытия их внутри BMP, DIB, VOC, WAV, ASCII, HTML — файлов. Для удобства использования программа выполнена в виде мастера. Это 32-разрядное приложение содержит собственный Shredder — программу, которая уничтожает файлы с жесткого диска. С новыми свойствами и дополнительными возможностями Steganos for Windows является серьезным конкурентом на рынке информационной безопасности для скрытия файлов.
- **Contraband** — программное обеспечение, позволяющее скрывать любые файлы в 24 битовых графических файлах формата BMP.

Операционная среда DOS:

- **Jsteg** — программа предназначена для скрытия информации в

популярном формате JPG.

- **FFEncode** — интересная программа, которая скрывает данные в текстовом файле. Программа запускается с соответствующими параметрами из командной строки.
- **StegoDos** — пакет программ, позволяющий выбирать изображение, скрывать в нем сообщение, отображать и сохранять изображение в другом графическом формате.
- **Wnstorm** — пакет программ, который позволяет шифровать сообщение и скрывать его внутри графического файла PCX формата.

Операционная среда OS/2

- **Hide4PGP v1.1** — программа позволяет прятать информацию в файлах формата BMP, WAV и VOC, при этом для скрытия можно использовать любое число самых младших битов.
- **Texto** — стеганографическая программа, преобразующая данные в английский текст. Текстовые файлы-контейнеры после преобразования не содержат какого-либо смысла, но достаточно близки к нормальному тексту, чтобы пройти примитивную проверку.
- **Wnstorm** — аналогична программе для DOS.

Для ПК Macintosh:

- **Stego** — позволяет внедрять данные в файлы формата PICT без изменения внешнего вида и размера PICT -файла.
- **Paranoid** — эта программа позволяет шифровать данные по алгоритмам IDEA и DES, а затем скрывать файл в файле звукового формата.

Основные выводы

Основная цель проведения расследования инцидентов, вирусных

заражений заключается в точном определении последствий атаки, причин и способов ее появления. Определив причины и способы возникновения атаки можно принимать корректирующие воздействия для предотвращения повторных атак и заражений.

Процесс расследования инцидентов информационной безопасности состоит из следующих стадий: оценка, сбор, анализ и отчет.

На этапе расследования инцидентов основную роль играют: ведение журналов регистрации событий, четкое разделение полномочий пользователей, ответственность за выполненные действия — важны доказательства того, кто участвовал в инциденте и какие действия он выполнял.

Основные источники информации об инциденте: Helpdesk, сообщения непосредственно от пользователей, инциденты, обнаруженные сотрудниками ИБ, журналы и оповещения систем.

При управлении инцидентами основные сложности вызывают следующие моменты: обнаружение и регистрация инцидента, устранение причин и последствий инцидента, расследование инцидента, реализация корректирующих и превентивных действий.

Расследование инцидента включает в себя определение виновных в его возникновении, сбор доказательств и улик инцидента, определение соответствующих дисциплинарных взысканий.

Прецедент и текущая ситуация представляются объектами, для которых необходимо обнаружить аналогию и благодаря переносу фактов, справедливых для прецедента, сделать некоторое заключение относительно рассматриваемого инцидента.

Стеганография - это метод организации связи, который собственно скрывает само наличие связи. В отличие от криптографии, где неприятель точно может определить является ли передаваемое сообщение

зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.

Цифровая стеганография - направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов.

Компьютерная стеганография изучает способы сокрытия информации в компьютерных данных, представляющих собой различные файлы, программы, пакеты протоколов и т. п.

Основным направлением компьютерной стеганографии является использование избыточности аудио и визуальной информации.

Стеганографическая система или стегосистема - совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

Категории атак против стегосистем: атаки против встроенного сообщения, атаки против стегодетектора, атаки против протокола использования цифровых водяных знаков (ЦВЗ), атаки против самого ЦВЗ.

Вопросы для самоконтроля

1. *Раскройте понятие «инцидент».*
2. *Процесс расследования инцидентов информационной безопасности.*
3. *Объясните основные источники информации об инциденте.*
4. *Какие моменты вызывают основные сложности при управлении инцидентами?*
5. *Объясните основные этапы расследования инцидента.*
6. *Какие существуют категории инциденты безопасности?*
7. *Приведите перечень элементов расследования компьютерных*

инцидентов.

8. *В чем базируется прецедентный анализ инцидентов информационной безопасности?*
9. *Объясните модель алгоритма прецедентного анализа.*
10. *В чем назначение стеганографии?*
11. *Как классифицируются направления стеганографии?*
12. *Какие существуют основные виды атак на стеганографическую систему?*
13. *Приведите примеры стеганографических программ.*

5. КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ СРЕДСТВ И СИСТЕМ

5.1. Криминалистическое исследование

Компьютерные преступления имеют общую криминалистическую характеристику, включающую сведения о способах преступлений и совершивших их лицах, о потерпевшей стороне и обстоятельствах, способствующих и препятствующих данным преступлениям.

Направление криминалистической техники можно считать сформировавшимся, если оно отвечает следующим критериям:

- решение специфических криминалистических задач, которые не ставятся при исследовании подобных объектов в других сферах человеческой деятельности;
- специфика объектов исследования-вещественных доказательств и, в то же время, их распространенность, частая встречаемость в уголовном и гражданском судопроизводстве;
- методологическая и методическая разработанность данного направления.

Криминалистическое исследование компьютерных средств и систем включает исследование как стационарных компьютеров, серверов, носителей данных, так и мобильных устройств сотовой связи, смартфонов, планшетных компьютеров и т.д.

Обычно компьютерные средства и системы приобщаются к материалам дела в качестве вещественных доказательств, но именно информация, содержащаяся в памяти данных устройств, является основным объектом криминалистического исследования. Информация представлена в неявном виде, и для обеспечения возможности ее восприятия необходимо

использовать специальные средства.

Проведение криминалистического исследования является важной частью расследования инцидента информационной безопасности. Это связано с тем, что носители информации содержат сведения, которые могут пролить свет на произошедший инцидент, а также помочь в идентификации лиц, причастных к его совершению. Благодаря полученной информации заключение о проведенном криминалистическом исследовании может быть использовано в качестве доказательства.

Криминалистическое исследование компьютерной информации и средств вычислительной техники основаны на выполнении следующих работ:

- восстановление хронологии каких-либо событий в информационной системе;
- поиск следов предположительно несанкционированного доступа;
- извлечение и анализ переписки (электронная почта, программы мгновенного обмена сообщениями);
- криминалистическое исследование мобильных устройств;
- исследование баз данных;
- исследование дампов сетевого трафика, дампов ОЗУ;
- поиск вредоносного программного обеспечения, присутствующего на компьютере;
- сравнение программных продуктов на предмет плагиата;
- установление целостности (неизменности) содержимого машинных носителей информации после их изъятия.

Основные принципы криминалистического исследования.

При проведении следственных действий, сопряженных с изъятием компьютерных средств и систем:

– не должна изменяться никакая информация, содержащаяся на

изымаемых носителях компьютерной информации;

- доступ к информации и исследование ее на месте допустимо только когда невозможно изъять носитель для производства судебной экспертизы;
- любые манипуляции с компьютерными средствами и системами должны осуществляться только с участием специалиста;
- все выполняемые действия должны подробно протоколироваться, чтобы обеспечить возможность использования результатов этих действий в доказывании.

В криминалистическое исследование компьютерных средств и систем должны также входить описание современных возможностей экспертного исследования, которое дается через перечни типичных задач основных родов судебных экспертиз, назначаемых при изучении указанных объектов. В первую очередь, это, безусловно, касается судебной компьютерно-технической экспертизы, представляющей в настоящее время класс судебных экспертиз, в которую входят:

- судебная аппаратно-компьютерная экспертиза - исследование аппаратных средств компьютерной системы (материальных носителей информации);
- судебная программно-компьютерная экспертиза - исследование программного обеспечения компьютерной системы;
- судебная информационно-компьютерная экспертиза (данных) - поиск, обнаружение, анализ и оценка информации, подготовленной пользователем или порожденной (созданной) программами для организации информационных процессов в компьютерной системе;
- судебная компьютерно-сетевая экспертиза, задачи которой включают практически все основные задачи рассмотренных видов экспертизы, т.е. решение аппаратных, программных и

информационных аспектов установления фактов и обстоятельств по делам. Ее объекты интегрированы из объектов описанных видов экспертиз (аппаратные, программные и информационные), но лишь с той разницей, что они все функционируют в определенной сетевой технологии.

Следующие ***общенаучные методы исследования*** применяются в цифровой криминалистике без ограничений:

1. Наблюдение.
2. Измерение.
3. Описание.
4. Сравнение.
5. Эксперимент.
6. Моделирование.
7. Объяснение.
8. Анализ и синтез.
9. Предсказание.

Представим себе, что на месте преступления обнаружен след – отпечаток обуви. Следователи фиксируют этот след в протоколе, а после готовы показать, что видели именно отпечаток обуви и у судьи не появится сомнений, что они могли видеть то, что было на самом деле.

Совсем по-другому с компьютерной информацией. Представим, что на «месте происшествия», а именно на диске сервера, в лог-файле обнаружена запись. Органами чувств человека она не воспринимается. Чтобы увидеть эту запись, потребуется посредничество следующих технических средств:

- механизм жесткого диска (НЖМД);
- контроллер НЖМД с внутренней микропрограммой (firmware);
- программное обеспечение BIOS и файловая система (драйвер);
- ПО для просмотра содержимого файла (например, вьювер «less»);

- драйвер экрана;
- аппаратные средства (клавиатура, монитор) со своими микропрограммами.

Наряду с общенаучными форензика применяет и ***специальные методы исследования,*** свойственные только ей:

1. Создание и применение специализированных криминалистических информационных систем.
2. Использование в целях обнаружения или исследования доказательств публичных поисковых систем (таких как «Google»), а также поисковых систем специального назначения (типа «Эшелон»).
3. Сбор хэш-функций известных файлов для отделения их от файлов, содержащих оригинальную пользовательскую или модифицированную информацию.
4. Архивирование полного содержимого носителей для целей последующего расследования возможных инцидентов.
5. Эмулирование сетевых сервисов для исследования поведения подозрительных программ в лабораторных условиях.

Общенаучные и специальные методы компьютерной криминалистики должны использоваться в борьбе с преступностью в следующих формах:

1. Производство компьютерно-технических экспертиз. ИТ-специалисты должны принимать участие в некоторых других видах экспертиз. Например, товароведческая (экономическая) экспертиза по определению стоимости прав на использование экземпляра ПО. Такая экспертиза совершенно необходима для доказывания нарушения авторских прав. Обычный экономист не знаком с особенностями ценообразования на программные продукты, с существующей практикой в этой области.

2. Участие специалистов в проведении следственных действий, имеющих отношение к компьютерной информации, – обыска, выемки, осмотра места происшествия и т.д. Например, такая элементарная задача, как выключение компьютера, который подлежит изъятию. Нет однозначного способа выключения. Чтобы правильно его выключить, нужно проанализировать обстоятельства дела, взвесить вероятности разных событий и, только исходя из этого, избрать способ выключения.

3. Участие специалиста в судебном заседании. Специалист в зале суда может действовать наподобие переводчика, разъясняя участникам процесса значения терминов, поясняя значение тех или иных технических деталей и так далее.

4. Снабжение оперативных работников и следователей техническими средствами, которые те могут использовать в работе самостоятельно, без участия специалиста.

5. Обучение пользователей и технических специалистов предприятий методам первичной фиксации цифровых доказательств, их предохранения от уничтожения. Значительная часть компьютерных преступлений остается нераскрытой только из-за того, что оператор информационной системы, которая стала целью злоумышленника, не позаботился о сбережении логов, электронных сообщений, использованных программ и иных потенциальных доказательств. Либо не знал, как их правильно сберечь, чтобы в дальнейшем такие доказательства имели силу, либо вообще не подозревал о существовании некоторых цифровых следов.

5.2. Восстановление данных

Утрата важной информации и ее недоступность через цифровые носители могут быть как случайностью - результатом поломки, брака,

некорректного обращения, так и преднамеренным шагом со стороны злоумышленников с целью уничтожить определенные данные, в том числе «цифровые улики» преступления.

Восстановление удаленных или поврежденных данных, записанных на различных типах носителей информации (накопители на жестких магнитных дисках, флеш-накопители, иные) осуществляются с помощью восстановление:

- удаленных файлов различного типа (документы, фотографии, видеофайлы и т. п.);
- данных после работы компьютерных вирусов;
- данных после логического повреждения файловых систем;
- данных, хранящихся на неисправных машинных носителях информации;
- файлов, поврежденных в результате программной ошибки.

Выделяются следующие категории объектов, которые могут являться носителями криминалистически значимой компьютерной информации:

- устройства для хранения информации;
- устройства для ввода/вывода информации;
- устройства обработки информации;
- устройства для передачи информации по каналам связи;
- информационные комплексы и системы.

Специфические особенности компьютерных средств и систем послужили причиной того, что в зарубежной практике выделен особый класс цифровых доказательств и описаны методы и приемы работы с ними. При этом необходимо различать оригинал цифрового доказательства, его дубликат и копию. Оригинальным цифровым доказательством являются материальные носители и такие информационные объекты, которые связаны с этими носителями на момент изъятия (получения). Дубликатом является

точная цифровая репродукция всех информационных объектов, хранящихся на оригинальном материальном носителе, в то время как копия - точная репродукция информации, содержащейся в информационных объектах, независимая от материального носителя.

Если выделять информацию, формирующуюся в процессе работы с вычислительной техникой, в особую группу материальных следов, то наиболее рациональным полагаем обозначить их как «информационно-технологические», поскольку формирование данных следов обусловлено спецификой реализации информационных технологий, а для их преобразования в доступную для восприятия форму информационные технологии также применяются. С криминалистической точки зрения такие следы близки следам орудий, инструментов и механизмов, поскольку различные информационные технологии используются в качестве инструмента, и при совершении определенных действий пользователя по известным алгоритмам и закономерностям будет формироваться доказательственная информация, представленная в цифровом виде и зафиксированная путем изменения свойств и состояния элементов носителя информации.

В настоящее время используются самые различные способы записи информации и, соответственно, самые разные запоминающие устройства и носители*:* жесткие магнитные диски, оперативная память, флеш-память, оптические и магнитооптические диски.

По принципу энергозависимости устройства для хранения информации могут быть разделены на два класса: энергозависимые (оперативная память) и энергонезависимые (жесткие магнитные диски, флеш-память, оптические и магнитооптические диски). Энергозависимая память очищается при снятии электропитания, в то время как энергонезависимые запоминающие устройства сохраняют информацию при отключении электропитания.

По устойчивости записи устройства для хранения информации делятся на постоянные запоминающие устройства (BIOS); записываемые (CD-R); многократно перезаписываемые (CD-RW, DVD-RW, жесткие магнитные диски, флеш-память); оперативные.

Запоминающие устройства могут быть классифицированы и по иным основаниям, но они определяют специфику криминалистического исследования данных объектов и применяемые технические средства. При изъятии устройств хранения информации наиболее важно определить порядок его изъятия и сохранения содержащейся в памяти информации, что, в первую очередь, определяется характером энергозависимости.

Устройства ввода информации предназначены для преобразования поступающих команд в доступную для обработки форму. К таковым относятся клавиатуры, манипуляторы, сенсорные графические планшеты (не путать с мобильными устройствами), интерактивные доски, сканеры, веб-камеры, устройства видеозахвата, звуковые карты с аудиовходом, считыватели смарт-карт, акселерометры и гироскопы, приемники спутниковой навигации, сканеры папиллярных узоров и узоров сетчатки глаз, разного рода датчики и измерительное оборудование, а также иные устройства. Ключевым элементом устройств ввода информации является аналого-цифровой преобразователь, задача которого преобразовывать сигналы различной природы (механических, электрических, акустических и др.) в цифровую форму, доступную для обработки.

Устройства вывода информации предназначены для преобразования информации цифровой формы в форму, доступную для восприятия. К ним относятся индикаторы, мониторы, проекторы, принтеры, звуковые карты, исполнительные механизмы и телемеханика (например, турникет или электронный замок) и т.д.

Устройства обработки информации предназначены для регистрации

поступающей информации и формирования управляющих команд в соответствии с алгоритмом. Среди компонентов персонального компьютера примером устройства обработки информации являются центральный процессор, графический контроллер (видеокарта), звуковой процессор (звуковая карта). В устройствах обработки информации также обычно присутствует оперативная память, используемая для хранения обрабатываемых объемов информации (кэш, буфер). Практически в каждом цифровом устройстве в том или ином виде имеется устройство обработки информации-микроконтроллер (преобразователь), осуществляющий обработку данных по алгоритму, заложенному в микропрограмме («прошивке») и хранящемуся в постоянном запоминающем устройстве (BIOS).

Устройства передачи информации по каналам связи предназначены для формирования сигналов и их трансляции и приема посредством различных каналов связи (проводных и беспроводных). По своей сути они представляют собой устройства ввода/вывода информации, которые осуществляют преобразование поступающих данных в сигнал, пригодный для передачи по каналу связи (модуляцию), и его трансляцию, а также прием сигналов и их обратное преобразование в доступную для обработки форму (демодуляцию). К устройствам передачи информации относятся модемы, bluetooth-модули, Wi-Fi роутеры и адаптеры, сетевые карты, GSM-модули, коммутаторы, маршрутизаторы, модули ИК-связи.

Современный компьютер независимо от своих конструктивных особенностей (будь то сервер, ноутбук, смартфон или планшет) включает в себя все типы перечисленных устройств и, по сути, является единым информационным комплексом. Управление данным информационным комплексом и взаимодействие компонентов осуществляется посредством программного обеспечения. Основной задачей применения данных

информационных комплексов является обработка данных и формирование результатов, необходимых пользователю. Соответственно, можно выделить три основных компонента любого информационного комплекса или системы: аппаратный, программный и информационный.

Передачу и хранение криминалистически значимой информации необходимо рассматривать не только для стационарных компьютерных средств и систем, их связи с локальными и глобальными сетями, но и для мобильных телефонов сотовой связи, смартфонов, планшетных компьютеров, которые в силу своего всеобщего распространения в настоящее время являются одними из важнейших объектов криминалистического исследования, поскольку выступают не только как носители и средства передачи криминалистически значимой информации, но и предметами, и орудиями совершения преступлений. Указанные устройства уже не могут классифицироваться как электронно-вычислительные машины, поскольку имеют постоянное соединение с сетью и являются ее частью. Они представляют собой интегрированные устройства, в которые входит персональный компьютер, устройство связи, коммутации; используют специфическое программное обеспечение; содержат носители информации (SIM-карты, карты памяти, USB-накопители); осуществляют функции глобальной системы позиционирования (GPS), оснащены фото- и видеокамерами.

Отличительными чертами доказательственной информации, хранящейся в цифровом виде, являются следующие:

- неявный вид и необходимость использования специальных средств для обеспечения ее восприятия;
- возможность уничтожения или модификации в кратчайшие сроки и удаленно;
- наличие специальных средств, ограничивающих доступ к данной

информации;

- постоянное изменение информации в ходе работы пользователя и выполнения различных операций;
- формирование взаимосвязанной информации на различных устройствах одновременно при передаче данных по каналам связи.

Перечисленные свойства цифровых данных обусловливают необходимость соблюдения определенных правил при фиксации и изъятии цифровых доказательств, а также их судебно-экспертном исследовании.

5.3. Компьютерно-техническая экспертиза

Расследование и раскрытие неправомерного доступа к компьютерной информации, когда средства компьютерной техники используются для подготовки, совершения или сокрытия рассматриваемого правонарушения, невозможно без привлечения специальных познаний в области современных информационных технологий.

Преступления, совершенные при помощи компьютерных технологий, не могут быть расследованы в полной мере и объективно без экспертов, которые обладают специальными знаниями в сфере компьютерных технологий. Основной процессуальной формой использования специальных знаний по делам совершенных с использованием компьютерных технологий является компьютерно-техническая экспертиза.

Это обусловлено тем, что только экспертное исследование обеспечивает получение результатов, имеющих наибольшее доказательственное значение при исследовании аппаратных средств, программного обеспечения и компьютерной информации.

Именно экспертные исследования придают изъятым аппаратным средствам, программному обеспечению и компьютерной информации

доказательственное значение. В таких условиях основными задачами следователя являются поиск, фиксация, изъятие и представление эксперту необходимых материальных объектов – носителей информации.

Существуют следующие разновидности объектов компьютерно-технических экспертиз:

-текстовые и графические документы (стандартные и электронные), изготовленные с использованием средств автоматизации (вычислительных систем, средств передачи данных и копирования информации);

- программы для компьютера и вспомогательная компьютерная информация, необходимая для их функционирования;

- видео- и звукозаписи, визуальная и аудиальная информация, представленная в формате мультимедиа;

- компьютерные данные и сведения, представленные в форматах, обеспечивающих их автоматизированное хранение, поиск, обработку и передачу (базы данных);

- физические носители информации различной природы (магнитные, магнитооптические, оптические и др.).

Соответственно, исходя из этого, предполагается, что с помощью компьютерно-технических экспертиз могут решаться следующие задачи:

1. Воспроизведение и распечатка всей или части информации, содержащейся на физических носителях, в том числе в нетекстовой форме.

2. Восстановление информации, ранее содержавшейся на физических носителях и впоследствии стертой или измененной по различным причинам.

3. Установление времени ввода, изменения, уничтожения либо копирования той или иной информации.

4. Расшифровка закодированной информации, подбор паролей и вскрытие систем защиты информации.

5. Установление авторства, места, средства подготовки и способа

изготовления документов (файлов, программ).

6. Выяснение технического состояния, исправности программно-аппаратных комплексов автоматизированных информационных систем, возможности их адаптации под конкретного пользователя.

Видовую классификацию компьютерно-технических экспертиз целесообразно организовать на основе обеспечивающего предназначения компьютерных средств (аппаратных (технических), программных, информационных) и использовать ее в виде, соответствующем процессам разработки и эксплуатации любых компьютерных систем. Поэтому можно выделить: **аппаратно-техническую и программно-техническую экспертизу** (данных). Кроме того, достаточно оправданным представляется выделение еще одного вида компьютерно-технической экспертизы - **компьютерно-сетевой** экспертизы для исследования фактов и обстоятельств, связанных с использованием сетевых и телекоммуникационных технологий.

Сущность ***аппаратно-технической экспертизы*** заключается в проведении исследования технических (аппаратных) средств компьютерной техники. Предметом экспертизы являются факты и обстоятельства, устанавливаемые на основе исследования закономерностей эксплуатации аппаратных средств компьютерной системы – материальных носителей информации о факте или событии неправомерного доступа к компьютерной информации.

Целью ***программно-технической экспертизы*** является изучение функционального предназначения, характеристик и реализуемых требований, алгоритма и структурных особенностей, текущего состояния представленного на исследование программного обеспечения компьютерной системы.

Объектами исследования ***компьютерно-сетевой экспертизы*** могут

быть как компьютеры пользователей, подключенных к сети Интернет, так и различные ресурсы поставщиков сетевых услуг (Интернет провайдеры), а также предоставляемые ими информационные услуги (электронная почта, служба электронных объявлений, телеконференции, WWW – сервисы и пр.)

При ***аппаратно-технической экспертизе*** целесообразно перед экспертом поставить следующие вопросы:

1. Какая модель компьютера представлена на исследование, каковы его технические характеристики, параметры периферийных устройств, вычислительной сети?
2. Имеется ли техническая документация на компьютер и его составные части? Соответствуют ли имеющиеся технические устройства документации?
3. Каковы условия сборки компьютера и его комплектующих: фирменная сборка, сборка из комплектующих в другой фирме или кустарная сборка? Имеются ли в наличии дополнительные устройства, не входящие в базовый комплект поставки (базовый комплект определяется из документации)?
4. Имеет ли место наличие неисправностей отдельных устройств, магнитных носителей информации (выявляются различными тестовыми программами)?
5. Не проводилась ли адаптация компьютера для работы с ним специфических пользователей (левша, слабовидящий и пр.)?

При ***программно-технической экспертизе*** (данных) ставится следующий круг вопросов:

1. Каков тип операционной системы, используемой в компьютере?
2. Какие программные продукты эксплуатируются на данном компьютере? Являются ли они лицензионными или «пиратскими» копиями, или собственными оригинальными разработками? Когда

производилась инсталляция (установка) данных программ?

3. Каково назначение программных продуктов? Для решения каких прикладных задач они предназначены? Какие способы ввода и вывода информации используются? Соответствуют ли результаты выполнения программ требуемым действиям?
4. Какие программные методы защиты информации используются (пароли, идентификационные коды, программы защиты и т.д.)? Не предпринимались ли попытки подбора паролей или иные попытки неправомерного доступа к компьютерной информации?
5. Какая информация содержится в скрытых файлах? Возможно ли восстановление ранее удаленных файлов и каково их содержание?
6. В каком виде хранится информация о результатах работы антивирусных программ, программ проверки контрольных сумм файлов? Каково содержание данной информации?
7. Имеет ли место наличие сбоев в работе отдельных программ? Каковы причины этих сбоев?
8. В каком состоянии находятся и что содержат файлы на магнитных носителях? Когда производилась последняя корректировка этих файлов?

Приведем пример из следственной практики:

К… со своего компьютера, осуществлял неправомерный доступ в компьютерную сеть "Интернет", используя логины и пароли скопированные и полученные с использованием вредоносной компьютерной программы типа "троянский конь".

По делу было назначено проведение программно-технической экспертизы. Перед экспертом были поставлены следующие вопросы:

1. *Какие программы содержаться на жестком диске представленного на исследование системного блока?*

2. *Имеются ли на данном системном блоке программы, с помощью которых осуществляется доступ в сеть "Интернет"?*
3. *Какие ярлыки присутствуют в системном блоке для осуществления удаленного доступа?*
4. *Какие логины, пароли и телефоны доступа (дозвона) соответствуют каждому ярлыку?*
5. *Имеются ли на жестком диске системного блока программы для осуществления несанкционированного доступа в компьютерные сети и системы (сканирующие порты, "троянские кони", "клавиатурные шпионы" и др.)?*
6. *Какая программа на системном блоке использовалась для работы с электронной почтой и новостями?*
7. *С каких электронных адресов приходила почта, и на какие электронные адреса она отправлялась?*
8. *Какие учетные записи почты содержаться на жестком диске?*
9. *Присутствуют ли в письмах, отправленных по электронной почте, файлы, содержащие вредоносные программы?*
10. *Содержаться ли в полученной почте пароли доступа в сеть "Интернет"?*

При ***компьютерно-сетевой экспертизе*** необходимо задать вопросы относительно того:

1. Какое программное обеспечение используется для функционирования компьютерной сети? Является ли оно лицензионным?
2. Каким образом осуществляется соединение компьютеров сети? Имеется ли выход на глобальные компьютерные сети?
3. Какие компьютеры являются серверами (главными компьютерами) сети? Каким образом осуществляется передача информации на

данном предприятии, учреждении, организации, фирме или компании по узлам компьютерной сети?

4. Используются ли для ограничения доступа к информации компьютерной сети пароли, идентификационные коды? В каком виде они используются?
5. Имеются ли сбои в работе отдельных программ, отдельных компьютеров при функционировании их в составе сети? Каковы причины этих сбоев?
6. Какая информация передается, обрабатывается и модифицируется с использованием компьютерной сети?

Участие экспертов в расследовании преступлений, совершенных при помощи компьютерных технологий, обусловлено тем, что успех расследования зависит от участия эксперта в осмотре, обыске, выемке и дальнейшем изучении содержимого.

Специальные знания компьютерно-технической экспертизы составляют электроника, электротехника, информационные системы и процессы, радиотехника и связь, вычислительная техника, в том числе и программирование, и автоматизация.

Востребованность экспертных услуг. Техника сегодня во многом заменила труд людей, большое количество сведений теперь хранится на различного рода носителях. Поэтому при возникновении каких-либо споров или разбирательств бывает необходима консультация эксперта в сфере компьютерного оборудования и программ.

Помимо доказательной базы уголовных дел, экспертная оценка востребована и в других областях судопроизводства. Например, в силу причин глобальной компьютеризации коммерческой сферы зачастую приходится решать гражданские споры в арбитражном суде. Помимо этого, в рамках административного кодекса в целях защиты прав потребителей

иногда возникает необходимость проведения экспертизы по факту продажи компьютерных средств и программного обеспечения. В данном случае необходимо подтвердить (или опровергнуть) их качество, безопасность для пользователя и т.д.

В досудебном споре по заявлению потребителя предоставляются результаты проверки качества компьютерных систем (обслуживание, ремонт и т.д.). Как правило, в данном случае основной задачей эксперта является анализ дефектов аппаратуры с целью определения их цены. Здесь необходимо комплексное заключение о наличии каких-либо проблем, связанных с компьютером и комплектующими, изменения их качеств, вопросы возможности дальнейшего использования и т.д. таким образом не только устанавливается истинное положение вещей, но и определяется размер выплаты ущерба (компенсации).

Объекты судебных компьютерно-технических экспертиз.

Аппаратные объекты

- персональные компьютеры (настольные, портативные);
- периферийные устройства (принтеры, модемы и т.п.);
- сетевые аппаратные средства (серверы, рабочие станции, активное оборудование, сетевые кабели и т.п.);
- интегрированные системы (органайзеры, пейджеры, мобильные телефоны и т.п.);
- любые комплектующие всех указанных компонент (аппаратные блоки, платы расширения, микросхемы памяти, магнитные и лазерные диски, магнитные ленты, карты и т.п.).

Программные объекты

- системное программное обеспечение компьютеров;
- прикладное программное обеспечение компьютеров.

Информационные объекты (данные)

- документация, изготовленная с использованием компьютерных средств;
- компьютерно-информационные данные в мультимедийных форматах;
- компьютерная Информация в базах данных и других приложений, имеющих прикладной характер и пр.

В приложении 1,2,3 даются образцы аппаратных и программных средств, применяемых в цифровой криминалистики и сведения о разработчиках.

Виды экспертиз (Рис.23):

Рис.23. Последовательность экспертиз

1. Аппаратно-компьютерная экспертиза, т.е. исследование аппаратных компонентов, магнитных носителей, документации.

2. Программно-компьютерная экспертиза, т. е. исследование ОС.
3. Информационно-компьютерная экспертиза - исследование прикладного программного обеспечения, и т. д.
4. Комплексные экспертизы проводятся на пограничных областях специальных знаний.
5. Компьютерно-сетевая экспертиза.

Аппаратно-компьютерная экспертиза заключается в выявлении и исследовании закономерностей использования аппаратных устройств и средств компьютерной технологии. В ходе проведении аппаратно-компьютерной экспертизы можно выявить марку, тип, свойства аппаратного устройства, а также выявить все их технические характеристики.

Данный подвид экспертизы предназначен для исследования компьютеров, а именно для определения модели, технический показателей устройства, тип, модель устройства. Так же при помощи аппаратно – компьютерной экспертизы можно установить параметры функционального предназначения и функциональных возможностей конкретного компьютерного устройства в сети или в системе, первоначальное техническое состояния и конфигурации аппаратного средства, а также состояния и конфигурации на момент исследования.

Предметом данного вида экспертизы являются факты и обстоятельства, устанавливаемые на основе исследования закономерностей эксплуатации компьютерной системы – материальных носителей информации о факте или событии уголовного дела.

На сегодняшний день судебная аппаратно-компьютерная экспертиза решает следующий круг задач:

– определение вида (типа, марки), свойств, аппаратного средства, а также его технических и функциональных характеристик для решения определенных функциональных задач;

- определение фактического состояния и исправности аппаратного средства, наличия физических дефектов;
- определение структуры механизма и обстоятельства события по его результатам за счет использования выявленных аппаратных средств, как по отдельности, так и в комплексе в составе компьютерной системы;
- установление причинной связи между использованием конкретных возможностей аппаратных средств и результатами их применения;
- определение условий (обстановки) применения аппаратных средств, восстановление хронологической последовательности их использования, места действия и функционирования.

Программно - компьютерная экспертиза исследует программное обеспечение компьютеров. Данная экспертиза исследует программное обеспечение с целью определения:

- общей характеристики программного обеспечения и его компонентов;
- реквизиты разработчиков и законного владельца;
- даты создания, объем программы;
- аппаратных требований, совместимости программы с программной оболочками и иными программами на конкретном компьютере, работоспособность программы;
- вносились ли исследуемую программу изменения, время, цели, состав изменений, новые свойства, которые приобрела программа после изменений;
- является ли программа вредоносной, каковы последствия ее использования.

Предметом являются закономерности разработки и использования программного обеспечения компьютерной системы, представленной на

исследование в целях установления истины по уголовному делу.

Решаемыми задачами программно-компьютерной экспертизы являются:

- индивидуальное отождествление оригинала программы и ее копии на носителях данных компьютерной системы;
- установление групповой принадлежности программного обеспечения по общим признакам;
- выявление частных признаков программы, позволяющих впоследствии идентифицировать ее авторство;
- выявление частных признаков программы, позволяющих впоследствии выявить взаимосвязь с информационным обеспечении исследуемой компьютерной системы;
- определение основных характеристик операционной системы;
- выявление и исследование функциональных свойств, а также настроек программного обеспечения, времени его инсталляции (установки на машинный носитель);
- определение фактического состояния программного объекта, состава соответствующих ему файлов, их параметров (объем, дата создания, атрибуты), способов ввода-вывода информации, наличия или отсутствия каких-либо отклонений от типовых параметров;
- диагностирование алгоритма программного продукта (представленного как в виде программного продукта, так и графического или текстового файла);
- установление видов инструментальных средств, использованных при разработке программного продукта (алгоритма);
- установление типов аппаратно-программных платформ, поддерживаемых программным продуктом;
- установление первоначального состояния программы (например, при

начальной инсталляции) и выявление возможных последующих изменений (обновлений, изменений состава);

- определение целей и условий изменения свойств и состояния программного обеспечения (преднамеренное изменение каких-либо функций, конфигурирование на конкретную аппаратную среду);
- установление способа осуществления изменений в программе (например, воздействие вредоносной программы, ошибки программной среды, несанкционированный доступ);
- определение свойств и состояния программы по ее отображению в обрабатываемых данных (по содержанию служебных, системных файлов), по обеспечивающим аппаратным средствам;
- выявление структуры механизма события по результатам работы программного обеспечения и в динамике;
- установление причинной связи между действиями пользователя компьютерной системы в отношении программного обеспечения и наступившими последствиями.

Информационно - компьютерная экспертиза является ключевым видом компьютерно- технической экспертизы. Именно данный вид экспертизы дает возможность завершить целостное построение доказательственной базы путем окончательного разрешения большинства диагностических и идентификационных вопросов, связанных с компьютерной информацией. Данный вид экспертизы исследует пользовательскую информацию и информацию, созданную программами.

Целью этого рода экспертиз является поиск, обнаружение, анализ и оценка информации, подготовленной пользователем или порожденной (созданной) программами для организации информационных процессов в компьютерной системе. В ходе информационно - компьютерной экспертизы определяются:

- вид записи данных на носителе;
- физическое и логическое размещение данных;
- свойства, характеристики, вид и параметры данных на носителе;
- доступность данных, наличие средств защиты, признаков преодоления защиты;
- содержание информации, ее первоначальное состояние, произведенные с данными операции, а именно копирование, модификация, блокирование, стирание, хронология данных операций.

Компьютерно-сетевая экспертиза в отличие от предыдущих основывается, прежде всего, на функциональном предназначении компьютерных средств, реализующих какую-либо сетевую информационную технологию. Предметом компьютерно-сетевой экспертизы являются факты и обстоятельства, связанные с использованием сетевых и телекоммуникационных технологий.

Компьютерно- сетевая экспертиза производится для решения следующих задач:

- определение свойств и характеристик аппаратного средства и программного обеспечения; установление места, роли и функционального предназначения исследуемого объекта в сети (например, для программного средства - в отношении к сетевой операционной системе; для аппаратного средства - отношение к серверу, рабочей станции, активному сетевому оборудованию и т.д.);
- выявление свойств и характеристик вычислительной сети, установление ее архитектуры, конфигурации, выявление установленных сетевых компонент, организация доступа к данным;
- принадлежности средства к серверной или клиентской части приложений;

– определение фактического состояния и исправности сетевого средства, наличия физических дефектов, состояния системного журнала, компонент управлением доступа;
– установление первоначального состояния вычислительной сети в целом и каждого сетевого средства в отдельности, возможного места покупки (приобретения), уточнение изменений, внесенных в первоначальную конфигурацию (например, добавление дополнительных сетевых устройств, устройств расширения на сервере либо рабочих станциях и пр.);
– определение причин изменения свойств вычислительной сети (например, по организации уровней управления доступом; установление факта нарушения режимов эксплуатации сети; фактов (следов) использования внешних («чужих») программ и т.п.);
– определение свойств и состояния вычислительной сети по ее отображению в информации носителей данных (например, raid-массивы, жесткие диски, флоппи-диски, CD-rom, zip-накопители и т.п.) и пр.;
– определение структуры механизма и обстоятельства события в сети по его результатам (например, сценария несанкционированного доступа, механизма распространения в сети вредоносных функций и т.д.);
– установление причинной связи между использованием конкретных аппаратно-программных средств вычислительной сети и результатами их применения.

Проанализировав судебную практику, мы пришли к выводу о том, что на сегодняшний день основными задачами программно-компьютерной экспертизы являются:

– общая диагностика и установление функций программного средства;

– диагностирование алгоритма программного продукта с целью выявления в его теле возможности выполнения действий (модификации, блокирования, копирования) без соответствующей санкции на них пользователя;
– установление признаков вредоносности программ;
– установление общего источника происхождения программного продукта.

Следует отметить, что для решения приведенных задач компьютерно-технической экспертизы необходимо обладать специальными знаниями в области программирования, алгоритмизации, построения баз данных, классификации ПО, и тому подобное.

Экспертные программы. Предназначены для исследования содержимого компьютерных носителей информации (прежде всего НЖМД) во время проведения экспертизы.

Популярные экспертные программы:

- Семейство программ ProDiscover.
- SMART (Storage Media Analysis Recovery Toolkit).
- Forensic Toolkit (FTK) фирмы «AccessData» Encase – экспертная система
- SATAN (System Administrator Tools for Analyzing Networks) – средство для снятия полной информации с компьютеров для ОС Unix.
- Helix – экспертный комплект на загрузочном компакт-диске на основе ОС Linux.

5.4. Типы и категории исследования

1. **Аппаратная экспертиза технических систем** своей целью ставит

исследование правильной работы материальных носителей информации о факте преступления. Ее основные задачи на данном этапе:

- определение технических и функциональных характеристик аппаратуры;
- проверка технического состояния;
- установление схемы и обстоятельств события по результатам использования средств аппаратных;
- нахождение связи между использованием оборудования и результатом его применения;
- установление хронологии;
- конкретизация аппаратных средств по найденным признакам.

2. **Программная компьютерно-техническая экспертиза (КТЭ)** исследует закономерности разработки и применения компьютерного софта, который предназначен для установления истины в расследовании по уголовным или гражданским делам. А данном этапе необходимо изучить характеристики и функциональное предназначение реализуемого алгоритма, структурные особенности и текущее состояние программного обеспечения компьютерной системы.

3. **Исследование данных** - ключевая оценка в экспертном комплексе, поскольку позволяет представить целостную картину базы доказательств. Достигается это за счет завершения большей части вопросов диагностики и идентификации, связанных с компьютерной информацией. В задачи данного этапа входит поиск, обнаружение, анализ и оценка сведений, подготовленных пользователем или порожденных (созданных) программами для организации информационных процессов в компьютерной системе.

Методы исследования. Необходимо заметить, что на сегодняшний день методология компьютерной экспертизы проходит стадию становления. Но уже можно разделить методы исследования аппаратных, программных

средств и баз данных.

Средства проверки функциональности аппаратуры:

- математические методы переключательных функций;
- методы синтеза и построения БИС и БИС памяти;
- архитектурные методы микропроцессоров;
- методы синтеза цифровых узлов;
- способы обработки сигналов аудио-и видеоносителей;
- оптические методы и т.д.

Исследовательские процедуры софта можно классифицировать в зависимости от вида объекта, представленного на экспертную оценку:

- методы изучения загрузочных модулей и алгоритмов программ;
- исследование исходных текстов.

Для проверки значимой информации (данных) методы могут представлять собой следующий комплекс:

- методы доступа и поиска данных;
- методы восстановления и архивации;
- способы информационных манипуляций (редактирование, перемещение, копирование).

К специальным методам судебной компьютерно-технической экспертизы можно отнести распределение обработки данных; иерархизацию; топологию; маршрутизацию, коммутацию и т.д. В тех случаях, когда проверку проходят всевозможные средства связи (мобильной, спутниковой, транковой, беспроводной и т.д.) на первый план выходят методы телекоммуникаций:

1. Протоколирования.
2. Цифровые и аналоговые способы передачи информации.
3. Методы сжатия и защиты сведений.
4. Кодирование и декодирование.

5. Модуляции и демодуляции сигналов и пр.

В числе наиболее достоверных методов исследования можно назвать эксперимент в среде вычислительной сети. Проводится в рамках изучения программных интернет-закладок. Создается сегмент модели интернет-сети, состоящий, как правило, из нескольких компьютеров, призванных имитировать участников взаимодействия в сети.

Первый из них представляет объект, подключенный через определенного провайдера, второй – сервер этого провайдера. Вот с его помощью и можно обнаружить интернет-данный о других компьютерах в Сети, к которым обращается программная закладка.

Второй компьютер имитирует домен сервера, а третий - получателя. Вот по его адресу и передаются данные с программы-закладки. Таким способом можно определить, поступает ли информация о пользователе или другие сведения с его компьютера на посторонние носители. Все вышеперечисленные методы никогда не используются поодиночке. Получить достоверный и компетентный результат можно только путем реализации комплексного подхода.

Какие вопросы должен решать компьютерный эксперт. Судебная компьютерно-техническая экспертиза (СКТЭ) может быть инициирована следователем (или судом), а проводит ее назначенный эксперт или экспертная организация. Доказательством по делу будет служить протокол исследования. В гражданском правовом поле назначить экспертизу может суд, одна сторона или нотариус по ее просьбе.

Вопросы, стоящие перед специалистом-экспертом, следующие:

1. Присутствие на исследуемых объектах информации, которая может быть использована в суде (скрытой или явной).
2. Возможность использования объектов экспертизы для определенных целей (например, для подключения к сети).

3. Вероятность совершения с объектом исследования каких-либо действий.
4. Свойства компьютерных программ, в том числе их принадлежность к вредоносным.
5. Идентифицировать найденные программы, документы, компьютерных пользователей.

В то же самое время есть ряд пунктов, которые не входят в компетенцию эксперта в данном случае, поэтому их присутствие в протоколе будет признано ошибочным. К ним относятся:

1) Оригинальность (лицензионность) программного софта.
2) Правоправность действий, которые были произведены при помощи объектов исследования.
3) Стоимость аппаратуры, носителей и программ.
4) Перевод найденных текстов, документов и т.д.

Для того чтобы экспертная оценка была признана в суде, необходимо ее составить по всем правилам. Ошибки в данном случае должны быть исключены.

Чаще всего встречающие вопросы экспертной оценки. Для того чтобы установить все обстоятельства дела, наиболее часто сегодня специалистом приходится искать ответ на следующие вопросы:

- ✓ Есть ли доказательства работы данного компьютерного средства в Интернет?
- ✓ При помощи чего осуществлялось подключение к Всемирной Сети?
- ✓ Наличие заготовленных соединений с Интернет, их свойства (даты создания, имена пользователей, пароли, координаты провайдера и пр.).
- ✓ Содержание установок программ удаленного доступа и протоколов соединения.

- ✓ Какие сайты посещал пользователь данного компьютера?
- ✓ Наличие информации об электронных платежах или перечислений с кредитных карт.
- ✓ Сообщения электронной почты (как полученные, так и отправленные).
- ✓ Сообщения, отправленные через специальные программы связи, их содержание.

5.5. Процесс расследования

В ходе расследования специалисты выполняют следующие действия:

1. Оценивают ситуацию - проводят анализ области расследования и предпринимаемых действий.

2. Накапливают данные - собирают, защищают и сохраняют доказательства.

3. Анализируют данные - исследуют и сопоставляют цифровые доказательства с теми событиями, которые представляют реальный интерес, что в дальнейшем позволит понять ход атаки.

4. Подготавливают отчет о проведенном расследовании - собирают и упорядочивают информацию и составляют окончательный отчет.

Детально стадии проведения расследования рассмотрим ниже.

Прежде чем начинать свое расследование, необходимо инициировать процесс расследования. Для начала следует решить, будете ли вы привлекать юристов для проведения административного (уголовного) преследования злоумышленника. Если да, то следует привлечь правоохранительные органы. Но стоит иметь в виду, что это можно сделать и на более поздних стадиях проведения расследования. Однако нужно понимать, что в первую очередь необходимо предотвратить дальнейшее нанесение ущерба

злоумышленниками. Ведь важнее всего защитить организацию от возможного ущерба, если, конечно, не затронуты интересы государственной безопасности.

Уведомление руководства. Для проведения внутреннего расследования компьютерного инцидента следует получить соответствующее разрешение руководства компании, если политика безопасности не предусматривает инцидентное разрешение. В таком случае требуется провести полную оценку ситуации и определить дальнейшие шаги. Для этого необходимо сделать следующее.

a) Если в организации не существует определенной политики реагирования на инциденты, то необходимо письменно уведомить руководство и получить письменное же разрешение от уполномоченного лица о проведении компьютерного расследования.
b) В ходе расследования необходимо документировать все связанные с ним действия. У вас должно быть точное и законченное описание событий и решений, имевших место в ходе инцидента и ответа на инцидент. В дальнейшем эта документация может использоваться в суде для описания действий, проводимых в ходе расследования.
c) В зависимости от контекста инцидента и при отсутствии угрозы государственной безопасности главной задачей является защита организации от нанесения дальнейшего ущерба. После того как безопасность организации будет обеспечена, необходимо восстановить работу и расследовать инцидент.

Вместе с тем, следует учитывать, что ваши решения и доказательства могут быть оспорены в суде, поскольку компьютерное доказательство - процесс весьма сложный и различные исследования могут дать разные результаты и заключения.

Обзор политик и процедур. Приступая к компьютерному расследованию, крайне важно понимать политики и процедуры, принятые в компании, к которым вы можете обратиться в ходе расследования. Обратите внимание на следующие важные соображения.

1. Имеете ли вы законные полномочия для проведения расследования?
2. Существуют ли принятые в организации политики и процедуры, в которых описаны правила обращения с конфиденциальной информацией?
3. Описаны ли в этих политиках и процедурах правила проведения внутреннего расследования в случае инцидента? Ведь не секрет, что во многих компаниях соответствующие политики и процедуры отсутствуют или не рассмотрены и не согласованы с юристами. Кроме того, не все сотрудники и посетители уведомлены об их существовании. Если вы не уверены в своих полномочиях, проконсультируйтесь с руководством и юристами.

Проконсультируйтесь с юристами во избежание потенциальных проблем, связанных с неправильной обработкой результатов проведенного расследования. В число факторов, провоцирующих такие проблемы, могут входить:

- персональные данные скомпрометированных клиентов;
- нарушение любых государственных законов;
- несение уголовной или административной ответственности за перехват электронных сообщений;
- просмотр закрытой информации. Данные, которые могут поставить под угрозу конфиденциальность информации клиента, должны быть доступны как часть связанной с расследованием документации, если это непосредственно использовалось в проведении расследования.

В дальнейшем необходимо гарантировать конфиденциальность

клиентских данных:

- все данные должны надежно храниться, при этом контроль доступа к ним должен быть ужесточен;
- по окончании расследования все данные, включая документацию, в течение периода времени, согласованного с юристами или в соответствии с законодательством, должны находиться под пристальным вниманием. Если данные - потенциальная часть уголовного дела, то необходимо проконсультироваться с правоохранительными органами.

В случае судебного иска требуется поддерживать и тщательно хранить все цифровые копии доказательств. Если вы не обеспечите безопасное хранение доказательств, вы не обеспечите доверие собранным в ходе расследования доказательствам. Сохранность доказательств достигается при наличии документации, поддающейся проверке.

Создание группы проведения расследований. Для успешного проведения внутреннего компьютерного расследования следует сформировать группу реагирования на инциденты. Лучше всего создать группу заранее, до того, как реально потребуется проводить расследование. Важно, чтобы члены группы имели навыки проведения подобных расследований. При этом необходимо учесть следующее.

- ✓ Определите компетентных сотрудников, которые понимают, как нужно проводить расследование. Идеальным будет обучение на соответствующих курсах. Помните, что в случае проведения слушаний в суде навыки и умения сотрудника, проводившего расследование, будут тщательно проверяться.
- ✓ Назначьте членов группы расследования и определите их обязанности.
- ✓ Назначьте одного из членов группы как технического

руководителя.

Как правило, технический руководитель должен иметь опыт участия в проведении расследований и достаточные технические знания. Не забывайте, что члены группы проведения расследования должны иметь более высокую квалификацию, чем подозреваемые.

1. Для обеспечения защиты информации и личной безопасности членов группы расследования состав группы должен держаться в секрете.
2. В случае отсутствия в организации должным образом подготовленного персонала к расследованию может привлекаться доверенная внешняя группа, обладающая необходимыми знаниями.
3. В случае проведения расследования необходимы гарантии, что каждый член группы обладает полномочиями для решения поставленной задачи. Данный пункт особенно важен в случае привлечения специалистов со стороны для проведения расследований.

Полная оценка ситуации. Для определения приоритета соответствующих действий и распределения ресурсов группы расследования необходима тщательная оценка ситуации. Данная оценка определяет текущее и потенциальное воздействие инцидента на работу организации, позволяет идентифицировать затронутую инфраструктуру и как можно полнее оценить ситуацию. Вместе с тем эта информация позволит быстрее определить соответствующее направление работы.

Для получения полной оценки ситуации необходимы следующие действия.

- Исследовать все потенциальные опасности, потенциально затрагиваемые стороны и, если возможно, информацию о подозреваемой стороне.
- Изучить возможное воздействие на организацию. Оценить, затрагивает ли инцидент данные клиентов, финансовые данные или

конфиденциальные данные компании. Данная оценка, вполне вероятно, будет находиться за пределами полномочий служб информационных технологий и информационной безопасности и, возможно, должна быть сделана при поддержке руководства и юристов компании.

- В течение расследования проанализировать воздействие инцидента на работу организации и перечислить ресурсы, необходимые для полной ликвидации последствий инцидента, время простоя, стоимость поврежденного оборудования, оцените возможную потерю доходов и стоимость разглашенной конфиденциальной информации.
- Проанализировать возможные нематериальные потери — влияние на репутацию организации т. д. Данная оценка потерь будет находиться вне компетенции служб информационных технологий и информационной безопасности и будет выполняться руководством вместе с юристами и сотрудниками других подразделений.

Для проведения идентификации, анализа и документирования сетевой инфраструктуры и компьютеров, затронутых инцидентом, необходимо сделать следующее.

1. Идентифицировать сеть, вовлеченную в инцидент, количество, типы и роли затронутых инцидентом компьютеров.
2. Изучить топологию сети, включая детальную информацию о серверах, сетевых аппаратных средствах, системах сетевой защиты, подключениях к Internet.
3. Идентифицировать внешние запоминающие устройства.
4. Определить удаленные компьютеры, подключаемые к компьютерной сети.

5. В случае необходимости фиксировать сетевой трафик. Данный тип анализа необходим в том случае, если в сети по-прежнему наблюдается подозрительный трафик.
6. Для исследования состояния приложений и операционных систем на компьютерах, которые затрагивает расследование, используйте инструментальные средства. В этом случае будут полезны файлы журналов Windows, Windows Sysinternals PsTools.
7. Для исследования и документирования затронутых файлов и серверов приложений используйте инструментальные средства Windows Sysinternals: PsTools, PsFile, ShareEnum и файлы журналов Windows.

Для получения завершенного понимания ситуации необходимо сделать следующее:

- Составить временной график. Это особенно важно для глобальных инцидентов. Данный документ должен содержать возможные несоответствия между датой и временем рабочих станций и службой времени Windows Server.
- Определить круг вовлеченных в инцидент лиц и побеседуйте с ними. Это чрезвычайно важно для понимания ситуации.
- Документировать все результаты интервью. Они потребуются позже для полного понимания ситуации.
- Восстановить и сохранить информацию (файлы журналов) внешних и внутренних устройств сети, таких как системы сетевой защиты и маршрутизаторы, которые могли находиться на пути атаки.
- Общедоступную информацию, типа IP-адреса и имени домена, для возможной идентификации атакующего можно получить с помощью Windows Sysinternals Whois.

Сбор доказательств. Сбор цифровых доказательств выполняется

локально или по сети. Однако локальный сбор данных не всегда возможен. В случае сбора данных по сети следует учитывать тип собираемых данных и те усилия, которые для этого потребуются.

Рекомендуемый процесс сбора данных:

1. Создать точную документацию, которая позволит подтвердить подлинность собранных доказательств. Важно обращать внимание на любые потенциально интересные элементы и регистрировать любые действия, которые могут быть позже признаны важными в процессе расследования. Ключом к успешному расследованию является надлежащая документация, в том числе такая информация:

1) Кто выполнил действие и почему?
2) Чего таким образом пытались добиться?
3) Как именно выполнено действие?
4) Какие использовались инструменты и процедуры?
5) Когда (дата и время) выполнено действие?
6) Какие результаты достигнуты?

2. Определить необходимые методы проведения расследования. Как правило, используется комбинация автономных и интерактивных методов.

- ✓ При проведении автономных расследований дополнительный анализ выполняется на поразрядной копии оригинального доказательства. Автономный метод расследования применяется всегда, когда это возможно, так как это уменьшает риск повреждения оригинального доказательства. Однако стоит учесть, что данный метод может использоваться только в тех случаях, когда может быть создана соответствующая копия, и не может применяться для сбора некоторых энергозависимых данных.
- ✓ При проведении интерактивного расследования анализ выполняется на оригинальном оперативном доказательстве. Сотрудники,

участвующие в проведении расследования, должны быть особенно осторожны ввиду риска модификации доказательств.

3. Идентифицировать и задокументировать потенциальные источники данных, включая:

- серверы; информация включает роль сервера, файлы логов, файлы данных, приложения;
- файлы журналов внутренних и внешних сетевых устройств;
- внутренние аппаратные компоненты (например, сетевые адаптеры);
- внешние порты — Firewire, USB и PCMCIA;
- запоминающие устройства, включая жесткие диски, сетевые запоминающие устройства, сменные носители;
- переносные мобильные устройства — Pocket PC, Smartphone и MP3-плееры.

4. При фиксировании энергозависимых данных следует тщательно рассматривать порядок сбора данных. Необходимо учесть, что энергозависимое доказательство может быть легко разрушено при выключении питания.

5. Необходимо использовать следующие методы сбора данных:

- ✓ Если необходимо извлечь какие-либо устройства внутренней памяти, требуется проверить, все ли энергозависимые данные зафиксированы, а затем выключить компьютер.
- ✓ Решите, удалить запоминающее устройство или использовать собственную систему для фиксирования данных. Учтите, что возможна ситуация, когда вы не сможете удалить запоминающее устройство из-за аппаратной несовместимости.
- ✓ Создайте поразрядную копию доказательства на резервном носителе, защитив оригинальное доказательство от записи. Весь последующий анализ данных должен выполняться на этой копии,

а не на оригинальном доказательстве.

- ✓ Документируя запоминающие устройства, гарантируйте включение информации об их конфигурации. Обратите внимание на изготовителя и модель оборудования, параметры настройки перемычки, объем устройства, тип интерфейса и состояние диска.

6. Проверить собранные данные. Если есть возможность, создайте контрольные суммы и цифровые подписи, чтобы гарантировать, что скопированные данные идентичны оригиналу. Учтите, что в некоторых случаях (например, при наличии сбойных секторов на носителе данных) вы не сможете создать абсолютную копию. Однако следует гарантировать, что вы получили наилучшую копию, которую можно было создать с помощью имеющихся инструментальных средств.

Хранение и архив. После того как доказательства собраны и готовы к анализу, чрезвычайно важно архивировать и хранить их таким образом, чтобы гарантировать целостность.

Перечислим наиболее надежные способы хранения и архивации данных.

1. Хранение данных в физически безопасном месте.
2. Документирование физического и сетевого доступа к информации.
3. Гарантия того, что неуполномоченные лица по сети или иным способом не могут получить доступ к доказательствам.
4. Защита комнат и оборудования, в которых хранятся носители, содержащие доказательства, от воздействия электромагнитных полей и статического электричества.
5. Изготовление не менее двух копий доказательств, собранных в ходе расследования. При этом одна из копий должна храниться в безопасном месте вне основного здания.
6. Гарантия того, что доказательство защищено как физически

(например, помещено в сейф), так и в цифровой форме (например, назначен пароль на носители данных).

7. Документирование всего процесса хранения информации доказательства.
8. Создание журнала контроля, который включает следующую информацию:

– имя человека, исследующего доказательство;
– дату и время начала работы с доказательством;
– дату и время его возврата в хранилище.

5.6. Цифровая судебно-медицинская экспертиза Forensic Toolkit (FTK)

Forensic Toolkit (Судебный Инструментарий), ***FTK*** - является программным обеспечением для компьютерной экспертизы, разработчиком которой является AccessData. Это программа позволяет сканировать жесткий диск, облегчая поиск различной информации. Например, определить местоположение удаленных электронных писем или найти диск для текстовых строк, чтобы использовать их в качестве словаря пароля.

Инструментарий также включает автономную программу создания образа диска под названием «The FTK Imager» (Формирователь изображения FTK) - простой, но убобный в использовании инструмент, позволяющий сохранить образ жесткого диска в одном файле или в сегментах, которые могут быть позже восстановлены. Также вычисляет значения хеша и подтверждает целостность данных прежде, чем закрыть файлы. Результат - файлы образа, которые можно сохранить в нескольких форматах, включая сырые данные DD.

Судебный Набор инструментов (FTK), признанный во всем мире стандартом программного обеспечения, используемым в цифровой

криминалистике, является единственным процитированным судом цифровым решением для исследований, созданным для быстрого, стабильного и непринужденного использования. Известный своим интуитивным интерфейсом, почтовым анализом, настраиваемыми представлениями данных и стабильностью, FTK позволяет расширить свою структуру.

Forensic Toolkit *(FTK)* является признанным мировым стандартом в области компьютерной экспертизы. Одобренная судами программная платформа для проведения расследования осуществляет расширенный анализ информации с криминалистической точностью, дешифрует и взламывает пароли. Обладает интуитивно понятным интерфейсом с возможностью индивидуальных настроек. Программа FTK создана для проведения быстрого анализа данных с возможностью масштабирования для использования в больших компаниях. Известная своим дружелюбным интерфейсом, мощным анализом электронной почты, возможностью настраивать форматы отображения исследуемых данных и стабильностью в работе, FTK позволяет в дальнейшем наращивать масштаб проведения компьютерной экспертизы при возникновения потребностей в вашей организации. Forensic Toolkit в настоящее время является самой передовой программой для проведения компьютерно-технической экспертизы. Раньше, как правило, только богатые компании могли позволить себе программные решения, обладающие таким функционалом, тем не менее, мы полны решимости сделать нашу технологию доступной для всех исследователей и аналитиков, работают ли они в правоохранительных органах, в учреждениях образования, в государственных структурах, в корпорациях из списка Fortune 500 или в качестве поставщика услуг по проведению компьютерной экспертизы.

AccessData Forensic Toolkit - программное обеспечение для проведения компьютерных экспертиз, обеспечивает анализ дампа оперативной памяти, использует мощный инструмент поиска, осуществляет

архивацию данных и проводит полное исследование компьютера в рамках судебной экспертизы. FTK интегрируется с программным продуктом фирмы AccessData, предназначенным для восстановления паролей и дешифрования файлов (Password Recovery Toolkit).

Функциональные возможности FTK:

1) Удобство в работе:

a) Предварительный просмотр файлов более 270 форматов и кодировок, благодаря технологии Stellent's Outside In Viewer Technology.

b) Сохраняет результаты всех действий и операций, выполненных в ходе экспертизы.

c) Генерирует соответствующие отчеты.

d) Полная индексация текстовой информации на исследуемом носителе позволяет мгновенно выводить результаты контекстного поиска.

e) Режим расширенного поиска для графических файлов формата JPEGи файлов – текстовых элементов Web-страниц.

f) Поиск информации по заданным параметрам.

g) Построение библиотек файлов (hashsets), типичных для экспертной практики, с целью их применения при автоматизированном анализе информации.

2) Работа с файловыми системами и копиями носителей:

a) Поддерживает работу в файловых системах: NTFS, сжатую NTFS, FAT 12/16/32 и Linux ext2 и ext3.

b) Поддерживает базы программ - почтовых клиентов: Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail и MSN.

c) Позволяет просматривать, производить поиск, распечатывать и

экспортировать из почтовых баз электронные письма или вложения.

d) Восстанавливает электронные письма, помещенные в папку «Черновики», или удаленные электронные письма.
e) Автоматически извлекает файлы из архивов, созданных программами: PKZIP, WinZip, WinRAR, GZIP и TAR.Known File Filter (KFF):
f) Поддерживает работу баз Hash Sets, созданные NIST и Hashkeeper.
g) Создает собственные базы.

Registry Viewer осуществляет:

- ✓ Прямой доступ к информации и дешифрование зашифрованной информации на носителе
- ✓ Просмотр файлов системного реестра.
- ✓ Генерацию отчетов.
- ✓ Данная программа совместима с другими программными продуктами AccessData.

Особенности Forensic Toolkit (FTK):

Комплексное решение для проведения компьютерно-технической экспертизы. Создание образов, проведение анализа реестра, проведение расследований, дешифровка файлов, взлом паролей, распознавание стеганографии и создание отчетов. Восстановление паролей более чем к 100 приложениям, использование вычислительной мощности процессоров во время простоя в сети для расшифровки паролей и выполнения атак по словарю. Библиотека хэшей, состоящая из 45 миллионов хэшей.

Архитектура масштаба предприятия. Поддержка очень больших, самых сложных наборов данных. Так как модули программы независимы друг от друга, то в случае сбоя не будут потеряны результаты работы программы. Предусмотрена возможность резервного копирования и архивирования дел. Каждая версия FTK включает 4 агента для выполнения

распределенной обработки -1 стоит на машине эксперта, оставшиеся 3 на других ПК (опционально можно получить большее количество экспертов). Распределенная обработка требует мощных аппаратных средств и сетевых технологий. Для обработки информации требуется быстрый диск, потому что операции I/O происходят очень интенсивно. Кроме того, машина, на которой работает Processing Manager, должна иметь самую быструю скорость (CPU) в группе. Программное решение легко расширяется путем добавления лабораторных возможностей. Это имеет значение для правительственных структур и правоохранительных органов.

Мощные и быстрые средства обработки.

1. Быстро реагирующий на действия графический интерфейс.
2. Распределенная обработка позволяет использовать до 3-х дополнительных компьютеров, чтобы значительно сократить время обработки и анализа массивных объемов данных.
3. Поддержка многопроцессорности и многопоточности.
4. Опция «Отменить процесс/поставить на паузу/возобновить».
5. Отображение текущего статуса обработки.
6. Распределение нагрузки на CPU.
7. Возможность уведомления по email об окончания обработки.
8. Продвинутый движок по выборке данных позволяет выбирать информацию из размеченного/неразмеченного пространства, удовлетворяющую определенным критериям: размер файла, тип данных и т.д., для того, чтобы отбросить ненужную информацию.
9. Улучшенная интеграция с dt Search позволяет быстро индексировать и получать быстрые результаты поиска.

Предварительный просмотр, сбор и анализ оперативных данных. Выполняет безопасное получение информации с криминалистической точностью с физических устройств, логических томов и RAM. Программный

агент легко устанавливается. Не требует громоздкой инсталляции и процесса аутентификации. Безопасное монтирование удаленных устройств

Интуитивно понятный интерфейс с богатой функциональностью. Простой для понимания и простой в использовании графический интерфейс с настраиванием форматов представления данных, продвинутой фильтрацией, перемещаемыми окнами и автоматизированной классификацией данных.

Программное средство Forensic Toolkit (FTK) представляет собой незаменимый инструмент для судебных экспертов, занимающихся производством компьютерно-технических экспертиз. Forensic Toolkit своего рода признанным мировым стандартом в области компьютерной экспертизы, широко используемым криминалистами всего мира. Программа позволяет осуществляет расширенный анализ информации с криминалистической точностью, дешифрует и взламывает пароли, путем подбора, является незаменимым средством при проведении цифровых криминалистических экспертиз. Программа обладает интуитивно понятным интерфейсом с возможностью индивидуальных настроек, что облегчает работу в программе, за счет экономии времени во время работы в программной среде Forensic Toolkit.

Благодаря тому, что программа позволяет проводить быстрый анализ данных с возможностью масштабирования для использования в крупных компаниях, она дает возможность в дальнейшем также наращивать масштаб проведения компьютерной экспертизы при возникновении определенных потребностей в той или иной организации. Forensic Toolkit в настоящее время является самой передовой программой для проведения компьютерно-технической экспертизы. Раньше, как правило, только богатые компании могли позволить себе подобные программные решения, обладающие свойством доступности для всех исследователей и аналитиков, работают ли они в правоохранительных органах, в учреждениях образования, в

государственных структурах, в корпорациях, или в качестве поставщика услуг по проведению компьютерной экспертизы. Сегодня же даже небольшие фирмы могут использовать подобное программное обеспечение. Что является еще одним достоинством данного программного обеспечения.

5.7. Компьютерная экспертиза данных и носителей данных с помощью технологии EnCase Forensic

Guidance Software, на данный момент, и уже продолжительное время, входит в ряд ведущих разработчиков инструментария для работы компьютерной экспертизы. Значительная, заметная часть разработок – это программные средства и программы для обучения компьютерных экспертных специалистов.

С помощью программных инструментов и технологий EnCaseForensic есть возможность и проводить исследования разного типа на любой стадии, и выдавать научно точные, различного типа, экспертные заключения.

С помощью программных комплексов компании Guidance Software и специальных технологий EnCaseForensic можно обучать специалистов компьютерной экспертизы. И проводить аттестации специалистов через специальные сертификационные экзамены. Любые сертифицированные эксперты и вообще любые специалисты могут получить сертификат эксперта от работающей во всем мире компании Guidance Software в области компьютерной экспертизы и информационных технологий.

Что же такое EnCase – технология и программы для проведения всех этапов компьютерной экспертизы.

EnCase Forensic это локальное программное обеспечение для проведения компьютерно-технической экспертизы, являющееся по сути международным стандартом поиска цифровых улик и предоставления

данных в суд. EnCase Forensic позволяет экспертам получать данные с помощью широкого спектра готовых фильтров и модулей, выявлять потенциальные доказательства путем криминалистического анализа информации, содержащейся на жестком диске, и подготавливать полные отчеты о полученных результатах, сохраняя при этом надежность и целостность полученных доказательств.

Гарантированная правомерность в поиске доказательств при помощи проверенного временем продукта, являющегося не просто лидером рынка, а стандартом проведения компьютерно-технической экспертизы.

- позволяет найти улики при помощи широкого спектра поисковых механизмов.
- ускоряет проведения расследования при помощи автоматизации типовых задач.
- сохраняет улики в едином контейнере доказательной базы EnCase.

EnCase Forensic сохраняет все найденные данные в единый файл улик с соблюдением всех принципов проведения криминалистической экспертизы и возможностью использования в суде.

Мощные и эффективные возможности криминалистического поиска информации и расследования компьютерных инцидентов сделали EnCase Forensic стандартным инструментом для проведения корпоративных расследований и аудита данных. Без ложной скромности можно констатировать тот факт, что в мире не существует иных решений, имеющих такие же возможности.

Это и программные, и аппаратные средства – помимо специальных программ предусмотрена собственная технология доступа к источникам и носителям данных с помощью устройства FastBloc. Как и программные инструменты EnCase, FastBloc работает в среде MSWindows, в ней отображает полученные результаты. И дает возможность полностью

корректно – с экспертной и юридической точки зрения – обеспечить доступ к носителям информации и к информации, которая на них находится, провести исследование и копирование не нарушая состояние первоначальных носителей данных и находящейся на них информации.

Копирование информации с первоначальных носителей, согласно правилам компьютерных экспертиз, производится определенным образом, с фиксацией всех шагов, при сохранении первоначальной информации и носителей именно в том виде, в каком они были изъяты или получены для проведения экспертизы. Технологические средства EnCaseосновываются в работе на так называемой Case-методологии, которая отвечает за сохранность первоначального состояния носителя и информации – объектов исследования – в процессе и после проведения экспертизы.

Технологические возможности программных комплексов Encase и Case-методологии. Системы EnCase и их методология – это возможность подходить к компьютерной экспертизе и ее проведению творчески, и более разнообразно, чем при работе с другими инструментами для подобных исследований. Многие зарубежные эксперты имеют опыт работы с уже давно выпущенными версиями комплексов EnCase, которые отлично справляются со своими задачами на новых информационных носителях, в работе с новыми операционными системами, новыми типами файлов и новыми типами ситуаций, которые сегодня приходится рассматривать компьютерной экспертизе.

Для более точного понимания возможностей этой технологии, рассмотрим задачи, которые она предлагает решать:

– возможность глубокой настройки и создания собственных инструментов на базе EnCase. Собственный макроязык программирования, встроенный в системы EnCase, так называемый ESCRIPT, приспособлен для написания программ и фильтров,

настраивающих работу EnCaseи расширяющих ее возможности. Таким образом, создаются пути для применения в работе на EnCasecамых современных методов и работы в современных условиях;

- конечно, анализ и поиск информации на различно форматированных носителях, старых и новых форматов, на разных аппаратных платформах, в разных средах с точки зрения операционных систем, на разных типах стационарных и сменных носителей. Различного типа жесткие и сменные диски и прочие типы носителей;
- при работе с графическими изображениями дает большие возможности распознавать графические файлы, автоматически отмечать их, производить их автоматическое копирование;
- корректные технологии точного зеркального копирования содержания носителей на специально предназначенные для экспертных исследований стендовые диски;
- различные гибкие операции по работе с зеркальными копиями жестких дисков и их содержания, с копиями логических томов и разделов;
- RAID-массивы и работа с ними в разном направлении – поддерживается;
- для криминалистов и экспертного исследования бывает очень важно без внесения изменений в носители и данные предварительно и быстро просмотреть информацию, содержащуюся на носителе. Для этого в EnCase существуют специальные технологии. Материалы останутся неприкосновенны, в то же время вы сможете быстро проверить носители на присутствие каких-то значимых данных;
- с помощью собственных аппаратных инструментов марки FastBloc к жестким дискам любого типа можно настроить безопасный и

корректный во всех отношениях доступ.

Это сфера вопросов и решаемых задач, относящаяся к работе с носителями, доступу к ним, их анализу, к настройке всей системы EnCase для более продуктивной работы, и к использованию EnCase в современных компьютерных экспертизах. Отдельный, обязательно интересующий специалистов по компьютерной экспертизе, раздел работы любого комплекса такого рода – это его возможности по работе с файлами и файловыми системами.

Самая разнообразная работа с файлами с помощью программ EnCase, и компьютерная экспертиза. Возможности компьютерной экспертизы, разного направления, судебной или внесудебной, часто зависят от возможностей используемых программных комплексов в отношении работы с файлами и файловыми системами. Насколько гибкой может быть настройка и работа с файлами, насколько быстро может вестись анализ файловой структуры, типов и содержания файлов – от всего этого зависит, будут ли связаны или наоборот свободны руки экспертов в решении поставленных перед ними задач.

В отношении работы с файлами инструменты EnCase от Guidance Software обладают следующими возможностями, все из которых реализуются без нарушения состояния носителей и первоначально полученной нами информации:

- выяснение содержимого любых файлов, определение дат их создания и изменения и других атрибутов;
- быстрый поиск ключевых и искомых слов, текста, алфавитно-цифровых данных в содержимом файлов, без запуска файлов, и без риска и возможности изменить структуру файловой системы, привести в действие механизмы защиты и другие программы;
- быстрый поиск, копирование, выделение, исследование таких

файлов, как сжатые, скрытые, архивированные, файлы, зарегистрированные в реестре ОС, системных файлов разных типов и других файлов по специальным или распространенным признакам;

– при работе с электронной почтой и сообщениями, передаваемыми другими способами – нахождение и анализ присоединенных файлов разного типа, формата;

– возможность в графическом виде отображать для изучения расположение на копии носителя всей информации и всех файлов.

Отображение структуры секторов и кластеров. С графическим и информационным отображением местоположения любых файлов:

– отметка, выделение, копирование, перенос и экспорт файлов, частей файловой структуры и дерева папок, отдельных фрагментов файлов;

– исследовательская работа с сигнатурами различных файлов, возможность расширять и модифицировать библиотеку сигнатур файлов, содержащуюся в EnCase;

– специальное построение библиотек и структур файлов и их форматов и типов для удобства экспертной работы и автоматического распознавания информации;

– возможность изучения содержания файлов, которые создает операционная система, таких как spooler-файлы, slack-файлы, swap-файлы, и другие. А также удаленные, помещенные в корзину и другие;

– в системе EnCase предусмотрены удобные средства, помогающие по окончании работы создать отчет о проведенных операциях, подробный, с датами и временем, что очень хорошо помогает в создании юридически и экспертно правильных заключений и представлении информации судебным и другим специальным инстанциям.

Интерфейс. Важные и удобные для эксперта особенности программных инструментов EnCase. Для экспертов, не близко знакомых с работой в этой области и разнообразными ее нюансами, может быть полезно на примерах объяснить, о каких возможностях в различных пунктах этого списка шла речь. Но для этого нужно было бы создавать специальные подробные технические материалы, что не является нашей целью на этом сайте. Определим одно из главных преимуществ этой программы. Нам кажется, что удобство EnCase во многом объясняется удобством ее графических интерфейсов – видов отображения содержимого копий носителей и содержимого любых файлов, и других данных.

Когда мы говорим о возможности «творчески» вести исследования с помощью пакета EnCase, то имеется в виду возможность настраивать программу изнутри с помощью макроязыка, и возможность настраивать работу с программой и данными, в том числе – получаемыми данными – снаружи, сточки зрения оперативного интерфейса для разных операций и случаев. К тому же для современных экспертов это более удобно, если информация показывается в удобном и комфортном для глаз виде «пользовательского интерфейса». Например, в интерфейсе EnCase есть следующие возможности: с помощью опции CaseTab вы можете представить изучаемые файлы почти так же, как это делается в стандартном проводнике Windows Explorer. Если слева вы получите дерево папок и файлов, то справа – информацию о закладках типа Report, Timeline, Gallery, Table. С помощью команды ViewFileStructure очень просто «не прикасаясь к информации» просматривать содержание архивных и сжатых файлов.

На основании самых разных признаков и атрибутов можно систематизировать файлы и отображать их таблицы в виде удобного графического интерфейса в верхней части окна программы с помощью функции TableView. Она же подразумевает в нижней части окна

отображение физического диска с точки зрения его содержания.

С помощью KeywordsTab можно очень удобно работать с интересующими вас ключевыми словами, их категориями и поиском. С возможностью выбора кодировок искомой информации, формирования в новых вкладках новых категорий ключевых слов для дальнейшей работы.

Таблица закладок BookmarksTab предлагает собрать в виде таблицы закладок ссылки на все найденные совпадения. Ссылки можно распределять в разные папки, закладки (таблицу закладок) можно организовывать по-разному, и назначать разный вид представления закладок: Report, Timeline, Gallery, и Table. Эти режимы предназначены для отображения разных типов файлов, просматривания их временных отметок по действиям с файлами – с возможностью настройки интересующих вас временных периодов.

Основные выводы

Проведение криминалистического исследования, благодаря полученной информации, может быть использовано в качестве доказательства.

Восстановление удаленных или поврежденных данных, записанных на различных типах носителей информации осуществляются с помощью восстановление: удаленных файлов различного типа; данных после работы компьютерных вирусов; данных после логического повреждения файловых систем; данных, хранящихся на неисправных машинных носителях информации; файлов, поврежденных в результате программной ошибки.

Передачу и хранение криминалистически значимой информации необходимо рассматривать не только для стационарных компьютерных средств и систем, но и для мобильных телефонов сотовой связи, смартфонов, планшетных компьютеров, поскольку выступают не только как носители и

средства передачи криминалистически значимой информации, но и предметами, и орудиями совершения преступлений.

Существуют следующие виды экспертиз:

- аппаратно-компьютерная экспертиза;
- программно-компьютерная экспертиза;
- информационно-компьютерная экспертиза;
- компьютерно-сетевая экспертиза;
- комплексные экспертизы.

Аппаратная экспертиза технических систем своей целью ставит исследование правильной работы материальных носителей информации о факте преступления.

Программно - компьютерная экспертиза исследует закономерности разработки и применения компьютерного софта, который предназначен для установления истины в расследовании по уголовным или гражданским делам.

Информационно - компьютерная экспертиза дает возможность завершить целостное построение доказательственной базы путем окончательного разрешения большинства диагностических и идентификационных вопросов, связанных с компьютерной информацией.

Компьютерно-сетевая экспертиза основывается на функциональном предназначении компьютерных средств, реализующих какую-либо сетевую информационную технологию.

Для успешного проведения внутреннего компьютерного расследования следует сформировать группу реагирования на инциденты.

Судебный набор инструментов (FTK), признанный во всем мире стандартом программного обеспечения, используемым в цифровой криминалистике, является единственным процитированным судом цифровым решением для исследований, созданным для быстрого, стабильного и

непринужденного использования, осуществляет расширенный анализ информации с криминалистической точностью, дешифрует и взламывает пароли.

Технология и программы для проведения всех этапов компьютерной экспертизы (EnCase Forensic) позволяет экспертам получать данные с помощью широкого спектра готовых фильтров и модулей, выявлять потенциальные доказательства путем криминалистического анализа информации, содержащейся на жестком диске, и подготавливать полные отчеты о полученных результатах, сохраняя при этом надежность и целостность полученных доказательств.

Вопросы для самоконтроля

1. *В чем основаны криминалистическое исследование компьютерной*
2. *информации и средств вычислительной техники?*
3. *Каким образом восстанавливается данные?*
4. *Основные принципы криминалистического исследования.*
5. *Перечислите отличительные черты доказательственной информации, хранящейся в цифровом виде.*
6. *Сущность компьютерно-технической экспертизы.*
7. *Основные задачи аппаратной экспертизы технических систем.*
8. *Какие вопросы должен решать компьютерный эксперт?*
9. *Какие виды инструментов для судебных экспертов существуют?*
10. *Перечислите типы и категории исследования, и их задачи.*
11. *Какие этапы включает процесса расследования.*
12. *Как осуществляется процесс сбора цифровых доказательств.*
13. *Какие задачи решает Цифровая судебно-медицинская экспертиза Forensic Toolkit?*

14. *Что позволяет технология и программы для проведения компьютерной экспертизы EnCase Forensic?*

6. ПРОБЛЕМЫ КИБЕРПРЕСТУПНОСТИ

6.1. Современная киберпреступность

В 2015 году 2,5 миллиарда человек или более трети от общей численности населения планеты имели доступ к Интернету. Более 60 процентов всех пользователей Интернета находятся в развивающихся странах, причем 45 процентов всех пользователей Интернета составляют лица в возрасте до 25 лет. По оценкам, к 2018 году доступ к мобильному широкополосному Интернету получат до 70 процентов от общей численности населения мира. К 2020 году количество сетевых устройств («Интернет вещей») будет в шесть раз превосходить численность населения, что полностью изменит нынешнее представление об Интернете.

В сверх подключенном к сети мире будущего будет трудно представить себе какое-либо «компьютерное преступление», а, возможно, и вообще любое преступление, которое не сопровождалось бы электронными доказательствами, связанными с подключением к интернет-протоколу (IP).

Определения киберпреступности преимущественно зависят от цели использования этого термина.

Киберпреступность в узком смысле (компьютерная преступность) — это любое противозаконное поведение в форме электронных операций, направленное против безопасности компьютерных систем и обрабатываемых ими данных. **Киберпреступность в более широком смысле** (преступления, связанные с применением компьютеров) — это любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети.

Основу киберпреступности составляет ограниченный круг деяний, направленных против конфиденциальности, целостности и доступности компьютерных данных или систем. Однако, если этим не ограничиваться, то в отношении деяний, предполагающих использование компьютера в целях извлечения личной или финансовой прибыли или причинения личного или финансового вреда, включая формы преступлений, связанных с использованием персональных данных, и деяния, связанные с содержанием компьютерных данных (все они входят в более широкое понятие «киберпреступности»), найти всеобъемлющее правовое определение не так легко. В отношении преступлений, составляющих основу киберпреступности, некоторые определения необходимы. Однако наличие «определения» киберпреступности не столь важно для других целей, таких как определение диапазона специальных следственных полномочий и возможностей в области международного сотрудничества, которые в большей степени касаются обнаружения электронных доказательств совершения любого преступления, а не нахождения широкого, искусственного определения концепции «киберпреступности». Поэтому понятие «киберпреступность» лучше рассматривать как *совокупность* деяний или действий.

Помимо социально-экономических выгод, компьютерные технологии и Интернет, как и любые другие средства, расширяющие возможности взаимодействия между людьми, безусловно, могут применяться для совершения преступных деяний. Хотя преступления, совершаемые с применением компьютера, или компьютерные преступления представляют собой относительно давно устоявшийся феномен, рост подключения к глобальной сети неразрывно связан с развитием современной киберпреступности.

Основу современной киберпреступности составляет именно та идея,

что сближение глобальных информационно-коммуникационных технологий может использоваться для совершения уголовно-наказуемых правонарушений в транснациональных масштабах.

К таким правонарушениям могут относиться все приведенные выше компьютерные преступления, а также и многие другие правонарушения, например, связанные с компьютерным или интернет-контентом или предполагающие использование компьютера в целях извлечения личной или финансовой прибыли.

Тем не менее, подключение к глобальной сети должно рассматриваться как центральный элемент современной киберпреступности и в особенности киберпреступности завтрашнего дня. По мере расширения киберпространства и IP-трафика, а также по мере опережения объема трафика беспроводных устройств объемов трафика проводных устройств и роста интернет-трафика, генерируемого некомпьютерными устройствами, возможно, сложно будет представить себе «компьютерное» преступление при отсутствии IP-подключения к глобальной сети. Особый персонализированный характера мобильных устройств и появление подключенных к интернет-проколу бытовых приборов или личных вещей ведут к тому, что электронные данные и их передача могут генерироваться или стать неотъемлемой частью практически каждого, будь то законного или незаконного, действия человека.

Основные причины роста киберпреступности. С точки зрения криминологии вполне вероятно, что расширение использования информационно-коммуникационных систем и Интернета создает новые возможности для преступников и стимулирует рост преступности (Рис.24).

Хотя в данном случае можно применить ряд криминологических теорий, тот факт, что киберпреступность представляет собой «новый и отличный от других вид преступлений», создает проблемы в

прогнозировании изменения ситуации и предупреждении таких преступлений путем применения общих теории преступности.

Рис.24. Возможные причины роста киберпреступности

Одно из ключевых предположений состоит в том, что развитие «киберпространства» ведет к формированию новых феноменов, которые связаны явно не с существованием самих компьютерных систем, и непосредственных возможностей для преступной деятельности, которые дают компьютеры. Человек может демонстрировать разницу между незаконопослушным и законопослушным поведением в рамках киберпространства по сравнению с физическим миром. Например, в киберпространстве люди могут совершать преступления, которые они не совершали бы в физическом мире в силу своего статуса и положения. Кроме того, гибкость идентичности, диссоциативная анонимность и отсутствие

сдерживающих факторов могут стимулировать преступное поведение в киберпространстве

Концепция привычной деятельности также может помочь выявить основные движущие силы киберпреступности. Концепция повседневной деятельности предполагает, что риск преступления возрастает при взаимодействии: заинтересованного преступника, подходящей жертвы и отсутствия действенного защитника. В случае киберпреступлений большое число подходящих жертв может появляться в связи с увеличением времени, которое люди проводят в глобальной сети, и использованием онлайн-услуг, таких как банковские услуги, покупки и обмен файлами, что создает для пользователей риск стать жертвой фишинга или мошенничества.

Развитие социальных сетей, включая «Twitter» и «Facebook», также ведет к формированию миллионов потенциальных жертв афер или мошенничества. Если пользователи не задействуют настройки, чтобы ограничить общение только кругом своих «друзей», такие социальные сети позволяют получить доступ сразу к большому числу потенциальных жертв. Кроме того, люди обычно организуют свои профили в социальных сетях с учетом своих интересов и месторасположения, что позволяет преступникам атаковать жертв, объединенных определенным стилем поведения или биографическими данными. Те «защитные» меры, которые существуют, например, антивирусные программы и (сравнительно небольшой) риск правоприменительных мер, могут оказаться недостаточными, чтобы остановить правонарушителя, заинтересованного в получении значительной прибыли.

Подключение к глобальной сети и обмен опытом с себе подобными могут являться основными причинами киберпреступлений, совершаемых организованными преступными группами. Одним из таких примеров являются онлайн форумы «кардинга» или мошенников, ворующих данные о

кредитных картах, которые используются для обмена украденными данными. Форумы мошенников, ворующих данные о кредитных картах, нередко зарождаются в форме «роевой» структуры при отсутствии цепочки управления, когда преступники ищут друг друга и «встречаются» в глобальной сети, чтобы обмениваться знаниями и предоставлять преступные услуги. Впоследствии форумы трансформируются в более контролируемые преступные группировки, работающие как «хабы» с более высокой степенью организованности. Сайты социальных сетей также могут использоваться для социальной «пропаганды» и связи между отдельными преступниками и преступными группами.

Социально-экономические факторы также могут играть важную роль в стимулировании роста киберпреступности. Ситуация, когда предприятия частного сектора вынуждены сокращать расходы и численность работников, может привести, например, к снижению безопасности и возможности использовать слабые места в информационно-коммуникационных системах. В связи с тем, что компаниям приходится нанимать сторонних или временных подрядчиков, или же среди работников компаний возникает недовольство в связи со снижением заработной платы и страхом потерять работу, может возрасти риск преступных деяний, совершаемых отдельными «инсайдерами» компаний, или влияния организованных преступных групп на таких «инсайдеров». Некоторые компании, занимающиеся вопросами кибербезопасности, выражают озабоченность в связи с тем, что бывшие работники, попавшие под сокращение штатов, представляют собой одну из возможных угроз в период экономического спада. Также отмечается, что растет число безработных или занятых на неполный рабочий день студентов, получающих постдипломное образование и обладающих компьютерными навыками, которые могут стать новым ресурсом для организованной преступности.

6.2. Классификация киберпреступлений

Международный союз электросвязи (МСЭ) предлагает следующую развернутую классификацию киберпреступлений:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных или систем

- незаконный доступ к компьютерной системе (хакерство, взлом шифра);
- незаконный доступ, перехват или получение компьютерных данных (информационный шпионаж);
- незаконное вмешательство в данные или вмешательство в систему;
- производство, распространение или хранение средств неправомерного использования компьютеров;
- нарушение конфиденциальности или мер защиты данных.

2. Преступления, связанные с применением компьютеров

- компьютерное мошенничество или подлог;
- компьютерные преступления, связанные с использованием персональных данных;
- компьютерные преступления, касающиеся авторских прав или товарных знаков;
- распространение или контроль распространения спама;
- деяния, предполагающие использование компьютера в целях причинения личного вреда;
- деяния, предполагающие использование компьютера в целях завлечения детей и груминга.

3. Преступления, связанные с контентом

- компьютерные преступления, связанные с пропагандой ненависти;
- использование компьютеров с целью производства, распространения

или хранения детской порнографии;

- деяния, предполагающие использование компьютера в целях содействия;
- религиозные преступления;
- клевета и фальшивая информация;
- спам и связанные с ним угрозы.

В приложении 4 дается более детальное описание каждого из этих деяний. Цель перечня состоит в том, чтобы установить примерный круг деяний, которые могут входить в термин «киберпреступность».

При этом следует отметить, что повсеместное распространение Интернета и персональных компьютерных устройств означает, что компьютерные системы или компьютерные данные могут использоваться для совершения практически любого уголовного преступления. Поэтому сфера электронных доказательств неразрывно связана с киберпреступностью, хотя и отличается от нее в концептуальном плане. Сбор и представление электронных доказательств являются неотъемлемой частью расследования и судебного преследования киберпреступлений. Кроме того, это все чаще касается традиционных преступлений, таких как грабеж, кража или кража с взломом, а также различных форм организованной преступности. Компьютерные записи телефонных разговоров, электронная почта, журналы-соединений, SMS-сообщения, адресные книги мобильных телефонов и компьютерные файлы могут содержать доказательства местонахождения, мотива, нахождения на месте преступления или вовлеченности подозреваемого в преступление в случае практически любого вида преступлений.

Перечень из 14 киберпреступлений не является исчерпывающим. Другие деяния, которые могут являться киберпреступлениями: «предполагающие использование компьютера средства для совершения

неправомерных деяний, связанных с финансовыми инструментами и средствами платежа», «азартные игры в режиме онлайн», «использование устройств информационных технологий для целей торговли людьми», «незаконный оборот наркотиков с использованием компьютера», «вымогательство с использованием компьютера», «незаконное распространение паролей» и «доступ к секретной информации».

В некоторых из этих случаев деяния могут рассматриваться как специализированные формы или варианты одного из уже перечисленных киберпреступлений. Например, использование или владение предполагающими использование компьютера средствами для совершения финансовых правонарушений может быть отнесено к широкой категории компьютерного мошенничества или подлога. Доступ к секретной информации может считаться одним из подвидов незаконного доступа к компьютерным данным в целом. Незаконное распространение паролей охвачено некоторыми положениями о средствах неправомерного использования компьютеров.

По мере создания условий для повсеместного доступа к интернету в мире может возникнуть потребность в использовании понятия киберпреступности на разных уровнях: в случае определения отдельных киберпреступлений потребуется конкретное и детальное описание понятия, при этом для обеспечения применения прав проведения расследований и механизмов международного сотрудничества в отношении преступлений, непрерывно перемещающихся из реального мира в глобальную сеть, может потребоваться достаточно широкий подход при наличии действенных защитных механизмов.

Криминализация. Согласно информации об уголовном законодательстве в области киберпреступности, собранной при помощи вопросника, подготовленного для целей проведения исследования, а также

посредством анализа основных источников с использованием имеющейся информации о законодательстве стран, были выделены 14 деяний, которые обычно включаются в понятие киберпреступности. Страны-респонденты сообщили о том, что эти 14 деяний широко криминализованы, за явным исключением преступлений, связанных со спамом, и в некоторой степени — преступлений, связанных со средствами неправомерного использования компьютеров, преступлений, связанных с расизмом и ксенофобией, а также использования Интернета с целью завлечения или ***«груминга»*** детей. Страны сообщили о нескольких дополнительных преступлениях, не упомянутых в вопроснике. Они главным образом касались данных, хранящихся в компьютере, включая криминализацию непристойных материалов, азартных игр в режиме онлайн и онлайновых незаконных рынков, таких как рынки торговли наркотиками и людьми. В том, что касается указанных 14 деяний, страны сообщили, что в отношении основных киберпреступлений против конфиденциальности, целостности данных и доступности компьютерных систем применяются специальные преступления в области киберпреступности. В отношении других форм киберпреступности чаще использовались правонарушения общего характера, непосредственно не связанные с киберпреступностью. В то же время применительно к деяниям, связанным с использованием компьютера в целях вторжения в частную жизнь, мошенничества или подлога, а также преступлениям, касающимся персональных данных, как сообщается, применяются оба подхода.

Преступления, связанные с незаконным *доступом* к компьютерным системам и данным различаются в зависимости от объекта преступления (данные, система или информация) и в зависимости от криминализации «просто» доступа как такового или наличия дополнительного умысла, такого как причинение убытков или повреждения. Различаются подходы к наличию умысла в составе преступления при криминализации вмешательстве в

функционирование компьютерных систем или данные. В большинстве стран вмешательство должно быть преднамеренным, в то время как в других странах предусматривается и вмешательство по неосторожности. В том, что касается вмешательства в компьютерные данные, деяния, представляющие собой вмешательство, охватывают деяния от повреждения или удаления до изменения, блокировки, ввода или передачи данных. Криминализация незаконного перехвата данных различается в зависимости от того, ограничивается ли правонарушение перехватом не предназначенных для общего пользования данных или не ограничивается им, а также в зависимости от того, ограничивается ли преступление перехватом при помощи «технических средств». Не во всех странах криминализированы средства неправомерного использования компьютеров. В тех странах, где они криминализированы, имеются различия в зависимости от того, связано ли преступление с хранением, распространением или использованием программного обеспечения и компьютерных кодов доступа. С точки зрения международного сотрудничества такие различия могут влиять на двойную уголовную ответственность.

В ряде стран приняты положения в отношении специальных киберпреступлений: компьютерного мошенничества, подлога и использования персональных данных. В других странах используются общие положения в отношении мошенничества или хищения либо за основу берутся преступления, отражающие составные элементы деяния, такие как незаконный доступ, вмешательство в данные и подлог в случае преступлений, связанных с использованием персональных данных. Весьма широкое распространение получила криминализация правонарушений, связанных с содержанием данных, особенно преступлений, касающихся детской порнографии. Однако существуют расхождения в определении термина «ребенок», ограничениях, касающихся «визуальных» материалов

или исключения имитируемых материалов, а также в отношении охватываемых деяний. Хотя в подавляющем большинстве стран криминализация охватывает изготовление и распространение детской порнографии, в области криминализации хранения и доступа наблюдаются более широкие вариации. Что касается компьютерных правонарушений, связанных с авторскими правами и товарными знаками, страны чаще всего сообщают, что в случае деяний, совершенных умышленно и в коммерческих масштабах, они применяют общие уголовные преступления.

Рост популярности социальных сетей и интернет-контента, генерируемого пользователями, заставил многие страны принять меры нормативного характера, в том числе в области уголовного права, что стало причиной призывов к уважению прав на свободу выражения мнения. Представившие ответы страны сообщают о различной степени ограничения свободы выражения мнения, в том числе в отношении диффамации, неуважения, угроз, подстрекательства к ненависти, оскорбления религиозных чувств, непристойных материалов и подрыва государственных устоев. Социально-культурный элемент некоторых ограничений находит отражение не только в национальном законодательстве, но и в многосторонних документах. Так, в некоторых региональных документах по противодействию киберпреступности предусмотрены правонарушения общего характера в отношении нарушения общественной морали, порнографических материалов и религиозных или семейных принципов или ценностей.

6.3. Предупреждение киберпреступности

Термин **«предупреждение преступности»** охватывает стратегии и меры, направленные на снижение уровня риска совершения преступлений и

потенциальных вредных последствий от них для отдельных граждан и общества в целом с помощью мер по устранению многочисленных причин преступлений. Руководящие принципы для предупреждения преступности подчеркивают, что важную роль в предупреждении преступности играет руководящая функция правительственных органов в сочетании с сотрудничеством и партнерством на уровне министерств и ведомств, а также между властями и общественными организациями, неправительственными организациями, деловыми кругами и отдельными гражданами (Рис.25).

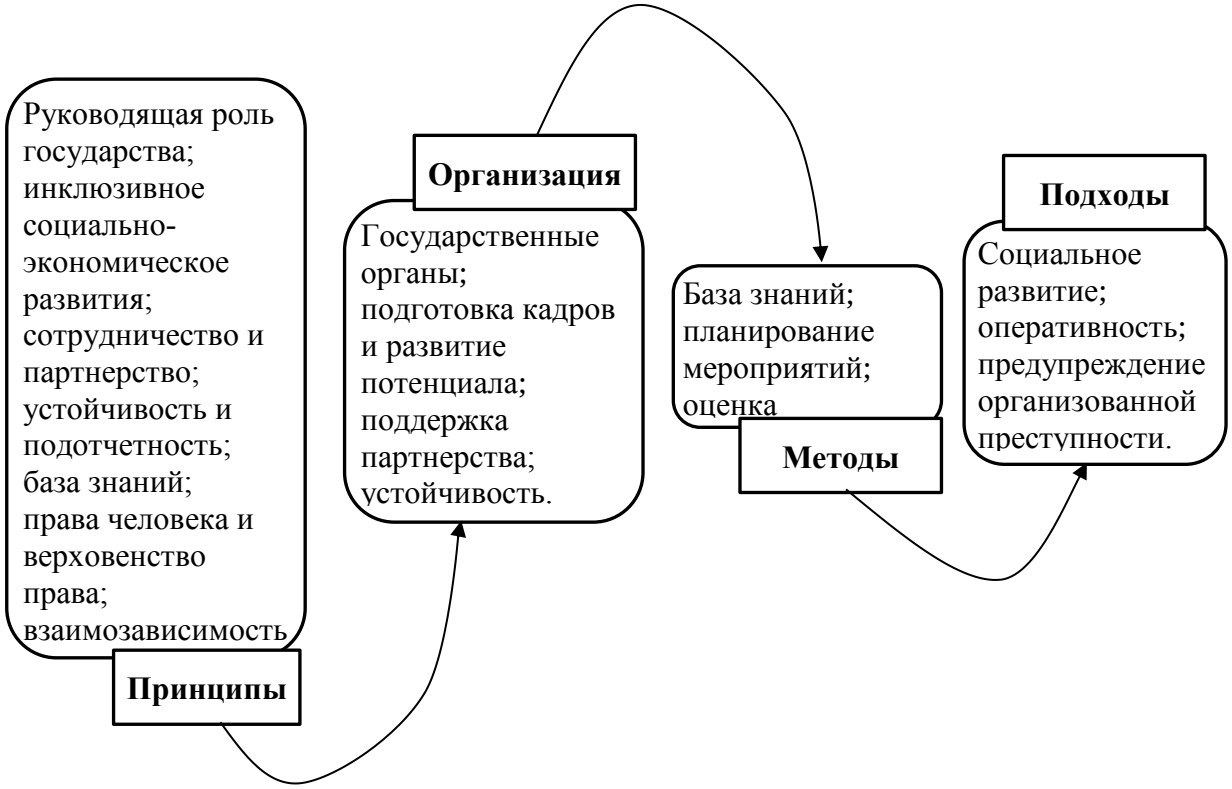


Рис.25. Принципы, организация, методы и подходы в области предупреждения преступности

Оптимальная практика предупреждения преступности опирается на базовые принципы (такие как руководство, сотрудничество и верховенство права), предлагает формы организации (такие как планы мероприятий по предупреждению преступности), и подводит к реализации методов (такие как

создание прочной базы знаний) и подходов (включая сокращение возможностей для совершения преступлений и усиление защищенности жертв преступлений).

Существует ряд проблем в области предупреждения киберпреступности. К ним относятся повсеместное распространение и доступность интернет-устройств, что обеспечивает большое число потенциальных жертв; относительно высокая степень готовности лиц «рискованно» вести себя в глобальной сети; возможность анонимности и запутывания со стороны правонарушителей; транснациональный характер многих киберпреступлений; и высокие темпы инноваций в области преступлений. Каждая из этих проблем влияет на *организацию, методы* и *подходы* в области предупреждения киберпреступности. Так, *организационные* структуры должны отражать потребность в сотрудничестве на международном и региональном уровне в области предупреждения киберпреступности. *Методы* должны обеспечивать постоянную актуализацию картины угроз в киберпространстве, а *подходы* должны предполагать участие ряда заинтересованных сторон, особенно организаций частного сектора, которые владеют интернет-инфраструктурой и службами и эксплуатируют их.

К двум ключевым технологическим изменениям последнего времени, которые влияют на риски в сфере информационной безопасности, относятся быстрый рост использования услуг облачных вычислений и использование работниками их собственных цифровых устройств (особенно смартфонов и планшетов) для доступа к корпоративным системам.

В последние время отмечено усиление влияния услуг облачных вычислений на вопросы безопасности. Например, одна компания-консультант по вопросам технологий указала: «Для более мелких компаний пользоваться облачными технологиями, наверное, безопаснее с точки зрения

киберпреступности, чем пытаться сделать это своими силами с помощью сервера в подсобке. Экспертов по кибербезопасности недостаточно, чтобы обеспечить ими каждую компанию, и очевидно, что стоить это будет слишком дорого. Поэтому с точки зрения защиты и реагирования на угрозы будет, вероятно, вполне обоснованно сконцентрировать такие ресурсы в «Amazon». Очевидно, однако, что это ведет к появлению возможных жертв нападения, поскольку гораздо интереснее взломать защиту крупного поставщика услуг, чем защиту мелкого местного магазинчика».

Другая проблема использования работниками личных устройств. Компания-консультант по вопросам технологий заметила: «Я полагаю, что риск накапливается в результате использования собственных устройств. Все приносят на работу устройства с широким кругом функций, которые подключаются к беспроводным сетям, обеспечивают взаимосвязь между социальными сетями и электронной почтой на работе и в частной жизни. Поэтому я думаю, что основная угроза связана с отсутствием культуры понимания проблемы».

В последнее время рассматриваются возможности использования информации, собираемой компаниями, для реагирования на атаки. Ряд организаций помогают компаниям составлять профили правонарушителей и причин их атак. Эта информация позволяет повысить качество технической защиты и судебных исков, использовать прием размещения ложной информации в собственных сетях компаний для обмана правонарушителей и сделать атаки более ресурсоемкими мероприятиями. Некоторые компании рассматривают возможности «обратных хакерских атак», направленных против хакеров, но пока неясно, насколько это будет законно или технически возможно.

В целом картина предупреждения киберпреступности носит смешанный характер. Более крупные компании, особенно в секторе

финансовых услуг, придерживаются более сложных стратегий предупреждения киберпреступности, в том числе используя специальные технологии в области безопасности, такие как аппаратные ключи безопасности для авторизации пользователей. Компании, занимающиеся вопросами безопасности, осуществляют активный мониторинг и регулярно публикуют отчеты о формировании новых угроз, а ряд крупных технологических компаний активно обращаются в суды с исками о ликвидации бот-сетей, преследовании спамеров и мошенников. Тем не менее, более мелкие компании не столь хорошо защищены, причем некоторые из них не предпринимают даже базовые меры предосторожности или не имеют реалистичного представления о рисках, связанных с вопросами безопасности.

Предупреждение киберпреступности со стороны поставщиков услуг Интернета и хостинга. Поставщики услуг Интернета занимают уникальное положение в рамках интернет-инфраструктуры.). Они приобретают в собственность или арендуют емкие оптоволоконные каналы и другие ключевые элементы интернет-инфраструктуры, такие как серверы, сетевые коммутаторы и маршрутизаторы, а также (в случае операторов мобильных сетей) *радиосоты*, что позволяет размещать и доставлять контент, подключать к Интернету настольные и карманные устройства. С одной стороны, «очевидно», что поставщики услуг должны играть некоторую роль в предупреждении киберпреступности, но с другой стороны, с этим связано много нюансов и сложностей, включая проблемы обязанностей и ответственности поставщиков услуг за интернет-контент. Для дальнейшего рассмотрения возможностей поставщиков услуг в деле предупреждения киберпреступности, прежде всего, необходимо кратко проанализировать ряд технических аспектов.

Поставщики услуг Интернета обеспечивают подключение пользователей к Интернету и передачу данных между пользователями и

устройствами, такими как глобальная сеть, электронная почта и серверы для передачи речи по IP-протоколу (VOIP). Поставщики услуг Интернета потенциально могут анализировать некоторую часть этого трафика, если пользователь не шифрует данные с использованием виртуальной частной сети, прокси-сервера или функций, встроенных в используемое для информационного обмена программное обеспечение. К данным абонента, которые могут быть доступны поставщикам услуг Интернета, относится содержание информационного обмена, т.е. незашифрованные тексты и изображения на веб-сайтах и в электронной почте, и контекстуальные данные, например, какие серверы абонент посещает, источник и назначение сообщений электронной почты, время и продолжительность использования различных услуг абонентом, причем эта информация доступна поставщику услуг даже при условии использования шифрования. В целом, содержание может быть доступно только в момент отправки данных, а затем — только при условии конкретного мониторинга подключений пользователя и сохранения данных с применением специального оборудования. Примечательным исключением являются случаи, когда поставщик услуг Интернета управляет таким сервисом, как сервер электронной почты, на котором сообщения хранятся более длительный период времени.

Одно лицо нередко обслуживается несколькими поставщиками услуг Интернета, поскольку доступ осуществляется из разных мест. Часто услуги Интернета для дома предоставляет один поставщик, а услуги Интернета для мобильных устройств — другой. Для доступа в Интернет на рабочем месте может использоваться третий провайдер, а при подключении к беспроводной сети в местном кафе задействуется еще один поставщик услуг Интернета, обеспечивающий такое подключение. Поэтому информацией об активности одного лица могут владеть разные поставщики услуг.

Поставщики интернет-хостинга контролируют системы, которые

используются для работы веб-сайтов и других сервисов. Как и в случае отношений между поставщиками услуг Интернета и их абонентами, компании-поставщики услуг хостинга имеют уникальную возможность наблюдать весь входящий и исходящий трафик сервисов их клиентов. Поэтому у них имеются технические возможности отключить или заблокировать незаконное использование таких сервисов. В своих соглашениях об обслуживании компании, предоставляющие хостинг, как правило, устанавливают ограничения на характер сервисов, которые могут размещаться на их серверах, обычно охватывающие широко известные виды ненадлежащего поведения, такие как рассылка большого количества спама или оскорбительных почтовых сообщений, размещение незаконного контента или нарушение авторских прав.

Поставщики услуг могут играть определенную роль в предупреждении киберпреступности в рамках двух основных направлений:

- хранение данных пользователей, к которым впоследствии могут получить доступ правоохранительные органы, чтобы использовать эти данные в расследовании киберпреступлений;
- активная «фильтрация» информационного обмена в Интернете или содержания данных, прежде всего, в целях предупреждения киберпреступлений.

Хранение данных. Учитывая объем трафика, проходящего через сети поставщиков услуг Интернета, они не в состоянии вести полный учет всего трафика. Некоторые страны внедрили сложные системы наблюдения за Интернетом, однако в связи с технологическими ограничениями могут возникать сложности со сбором и анализом огромных объемов данных. Регистрация менее детальной информации (такой как IP-адреса, присваиваемые отдельным пользователям в определенные моменты времени) может охватывать длительные периоды времени. Поставщики услуг

Интернета, как правило, в состоянии осуществлять адресный мониторинг данных «в режиме реального времени», а правила «законного перехвата» многих стран предполагают, что поставщики услуг Интернета должны иметь возможность осуществлять целевой мониторинг подключений лица или помещения в режиме реального времени.

Защита данных. Хранение и обработка данных поставщиками услуг Интернета во многих странах регулируются законодательством о защите данных, которое устанавливает требования в области защиты и использования данных личного характера. Принцип безопасности гласит, что картотеки должны быть защищены «от связанных с деятельностью человека рисков, таких как несанкционированный доступ, противозаконное использование данных или заражение компьютерным вирусом».

Однако предусмотренная в рамках защиты данных обязанность удалять данные личного характера, когда они более не нужны для целей, для которых они собирались, может влиять на процесс расследования киберпреступлений органами полиции. Например, ряд правоохранительных органов сообщили о проблемах, связанных с коротким периодом хранения данных поставщиками услуг Интернета, что в некоторых случаях может быть связано с положениями законодательства о защите данных. Кроме того, законодательство о защите данных, действующее в отношении всех организаций и отдельных лиц, которые обрабатывают данные личного характера, способствует предупреждению киберпреступности со стороны поставщиков услуг Интернета, поскольку оно определяет стандарты обработки данных, позволяющие обеспечить безопасность и целостность данных о пользователях.

Сохранение данных. Учитывая требования положений законодательства о защите данных в сочетании с финансовыми последствиями хранения больших объемов данных, поставщики услуг

Интернета не хранят данные неограниченно долгий период времени. В целях оказания помощи правоохранительным органам в проведении расследований некоторые страны приняли исключения к положениям законодательства о защите данных, в соответствии с которыми поставщики услуг Интернета обязаны хранить определенные виды данных об онлайновой активности абонентов на протяжении некоторого периода времени (например, одного года), в течение которого следственные органы могут получить доступ к этим данным при наличии разрешения судебных или административных органов.

Уведомление о повреждении систем безопасности данных. Наконец, требования об «обязательном уведомлении о повреждении систем безопасности данных» также могут оказывать влияние на хранение данных абонентов поставщиками услуг Интернета. Обязательное уведомление пострадавших сторон и регулирующих органов о повреждении систем безопасности данных, особенно в случае раскрытия данных личного характера, нашло широкую поддержку в ряде стран. Уведомление призвано дать стороне, пострадавшей от такого повреждения, возможность предпринять меры по снижению последствий такого инцидента с точки зрения безопасности (например, посредством смены паролей или персонального кода пользователя или обращения за перевыпуском платежных карточек), усилить конкурентное давление на компании с тем, чтобы они совершенствовали свои системы безопасности и поддержать усилия регулирующих органов, отвечающих за вопросы защиты данных и жизненно важной инфраструктуры.

В то время как уведомления о повреждении систем безопасности данных могут представлять собой важный элемент системы информационной безопасности, в том числе в отношении поставщиков услуг Интернета, такие законы должны обеспечивать осторожный подход к определению термина

«повреждение систем безопасности» и применяться в сочетании с рядом других мер, включая действенные законы о защите данных.

Фильтрация интернет-контента. Помимо содействия предупреждению преступности за счет возможностей, связанных с хранением данных, поставщики услуг Интернета также могут принимать участие в деле предупреждения киберпреступности за счет активного анализа информационного обмена в Интернете и передаваемых при этом данных. В этой связи одной из основополагающих концепций является «фильтрация» интернет-контента поставщиками услуг Интернета. Фильтрация интернет-соединений имеет место на определенном уровне практически в любой сети. Самый базовый уровень фильтрации, используемый для повышения эффективности работы и безопасности сети, состоит в блокировании неверных или иным образом поврежденных данных. Поставщики услуг Интернета также могут иметь технические возможности для фильтрации данных на предмет определенного вредоносного или незаконного контента. Например, многие поставщики услуг Интернета могут применять базовые спам-фильтры для фильтрации сообщений в электронной почте их абонентов и обеспечивать защиту от хорошо известного вредоносного трафика, связанного с вирусами или хакерскими атаками, отказываясь передавать далее трафик, отнесенный к этой категории.

Спам и бот-сети. Фильтрация спама является серьезной проблемой всех поставщиков услуг электронной почты, учитывая большие объемы содержащих спам сообщений, которые отправляются и поступают ежедневно. Средства фильтрации спама разнообразны и сложны. К ним относятся анализ отправителя почтовых сообщений для определения известных источников спама, а также анализ текстов для выявления стандартных фраз и структуры содержания в сообщениях. Сообщения, которые классифицируются как спам, иногда полностью блокируются или

доставляются в «папку спама» пользователя.

Когда поставщики услуг Интернета получают уведомление или определяют, исходя из структуры интернет-трафика, что устройство в их сети, по-видимому, стало частью бот-сети или иным образом заражено вредоносными программами, один из возможных вариантов действий включает в себя блокирование части или всего трафика, идущего с этого адреса при одновременном уведомлении абонента о шагах, которые он может предпринять для удаления вредоносных программ. Такие уведомления могут поступать от отвечающих за безопасность компаний, которые осуществляют мониторинг в целях выявления бот-сетей с использованием таких приемов, как устройства-«ловушки», которые преднамеренно привлекают вредоносные программы. Поставщики услуг Интернета также могут предпринимать шаги по активному выявлению взломанных устройств, осуществляя мониторинг трафика на предмет известных сигнатур, однако для эффективности таких действий необходима определенная степень адресности.

Фильтрация содержания данных. Как говорится ниже, когда речь идет об ответственности поставщиков услуг Интернета, в законодательстве некоторых стран содержится требование о том, чтобы поставщики услуг Интернета блокировали доступ к незаконному контенту, такому как детская порнография. Существуют различные способы, с помощью которых поставщики услуг Интернета могут это делать, причем разные методы предполагают разные варианты компромиссного выбора с точки зрения сочетания скорости, стоимости, действенности и точности. Применение *фильтров DNS* позволяет поставщикам услуг Интернета контролировать ответы, которые DNS серверы направляют их абонентам и ограничивать доступ к домену, такому как «google.com», но не к конкретной странице или набору результатов поиска. Такие ограничения легко обойти, поскольку

пользователи могут просто использовать альтернативные серверы DNS, которые дадут подлинные результаты.

Фильтрация по заголовкам IP может использоваться для блокирования отдельных компьютеров в зависимости от их адресов или даже для частичного блокирования определенных сервисов, таких как Интернет или электронная почта. Поскольку на одном интернет-сервере может размещаться большое количество веб-сайтов, это может повлиять на не связанные с проблемой веб-сайты, причем иногда их число может быть очень велико. *Углубленная проверка пакетов* может применяться для анализа основного содержания интернет-трафика. Это позволяет очень гибко подходить к фильтрации, но требует дорогостоящего оборудования, которое приходится устанавливать на высокоскоростных каналах ISP и которое может замедлять соединения всех абонентов. На практике многие режимы фильтрации предполагают некое сочетание этих подходов с образованием гибридного фильтра. Более простые фильтры, например, на основе DNS, часто используются для выявления трафика, который следует направить для проверки более сложными фильтрами. Такой гибридный подход обеспечивает сложную фильтрацию при значительном сокращении необходимых ресурсов.

В целом, учитывая, что поставщики услуг Интернета и хостинга обеспечивают подключение отдельных лиц и организаций к Интернету, они могут играть ключевую роль в предупреждении киберпреступности. Они могут вести журналы, которые могут использоваться при расследовании уголовных преступлений; помогать клиентам выявлять взломанные компьютеры; блокировать некоторые виды незаконного контента, такого как спам; и оказывать общую помощь в создании безопасной среды информационного общения для своих клиентов. Во многих странах положения законодательства о защите данных требуют, чтобы поставщики

услуг Интернета обеспечивали защиту данных клиентов, а следственные полномочия были пропорциональными с точки зрения обеспечения доступа полиции к этим данным. Принцип свободы выражения мнений также должен учитываться в законодательстве, определяющем ограничения свободного потока информации в Интернете. Защита поставщиков услуг Интернета и других посредников от ответственности стала ключевым фактором быстрого роста услуг в режиме онлайн, но при этом на поставщиков услуг Интернета возлагаются некоторые обязанности, такие как принятие мер в случае получения уведомления о нарушении авторских прав и других нарушениях.

Участие научного сообщества в предупреждении киберпреступности. Научные учреждения и межправительственные организации играют важную роль в деле предупреждения и борьбы с киберпреступностью. Такие учреждения могут, в частности, внести свой вклад в области развития базы знаний и обмена знаниями, разработки законодательства и политики, разработки технологий и технических стандартов, оказания технической помощи и сотрудничества с правоохранительными органами.

Развитие базы знаний и обмен знаниями: В ответ на спрос со стороны государственных учреждений и частных предприятий на квалифицированные кадры и повышение квалификации сотрудников в области кибербезопасности научные учреждения создали специальные образовательные программы, учебные планы и центры подготовки кадров, чтобы консолидировать знания и результаты исследований и усилить синергетический эффект межотраслевого и междисциплинарного подхода. Растет число вузов, которые предлагают дипломы, сертификаты и курсы профессиональной подготовки в области кибербезопасности и киберпреступности, чтобы обеспечить «образование и профессиональную подготовку молодых специалистов и будущих профессионалов по вопросам

безопасных компьютерных практик и по техническим аспектам». Посредством организации семинаров и конференций вузы также поощряют практическое обучение и развитие социальных сетей для борьбы с киберпреступностью. Такие мероприятия служат площадкой для обмена информацией и рекомендациями по вопросам предупреждения преступности и ответных мер, что содействует развитию неформального сотрудничества, а иногда и механизмов информирования соответствующих органов о конкретных преступлениях, и выработке технических решений.

Разработка законодательства и политики: Специалисты вузов вносят значительный вклад в разработку проектов и внесение изменений в законодательство и политику. На национальном, региональном и международном уровне ученые предоставляют консультативную помощь и принимают участие в подготовке проектов законодательства по ряду тем, включая вопросы криминализации, конфиденциальности и права на частную жизнь, конституционной и правовой защиты. Такая консультативная помощь оказывается с применением ряда механизмов, в том числе в рамках консультативных и специальных рабочих групп, контактов на уровне учреждений и отдельных специалистов, а также программ технической помощи. Один респондент из состава представителей научных учреждений отметил, например, что специальные научные центры, занимающиеся вопросами киберсреды, часто выступают в роли координаторов «деятельности исследователей в ряде узких специальных областей, связанных с проблемами киберпреступности (правовая, криминалистическая, техническая экспертиза)».

Технологии и технические стандарты: Вузы ведут фундаментальные и прикладные научные исследования в области компьютерных технологий либо в контексте сотрудничества с организациями частного сектора и (или) государственными учреждениями при финансовой поддержке отечественных

или внешних спонсоров, либо в рамках обеспечения безопасности вузовской сети. Вузы также могут вносить вклад по таким направлениям, как компьютерная криминалистика, анализ доказательств и анализ данных учреждений. Помимо исследований на уровне вузов и отдельных специалистов, вузы также являются важными партнерами и организаторами сотрудничества в рамках участия в профессиональных организациях и организациях, отвечающих за утверждение стандартов, а также в технических рабочих группах.

Сотрудничество с правоохранительными органами: Руководство правоохранительных органов может быть заинтересовано в сотрудничестве с вузами, учитывая накопленный в вузах экспертный опыт в области киберпреступности и кибербезопасности. Респонденты из числа представителей вузов сотрудничают с правоохранительными органами в области развития базы знаний, технических стандартов и технической помощи, хотя многие респонденты из числа представителей научных кругов также отмечали отсутствие прямого взаимодействия с правоохранительными органами. Представители научных кругов часто подчеркивали, что озабоченность вызывает проблема наличия ресурсов для расширения таких образовательных программ и информационного взаимодействия. Один респондент отметил, например: «Отсутствуют общие официально оформленные основания для сотрудничества – у государственных ведомств отсутствуют какие-либо стандарты или бюджет для сотрудничества с вузами. Поэтому все имеющиеся контакты и информационное взаимодействие носят неформальный характер». «Финансирование, численность персонала и наличие научных сотрудников узкой специализации» для оказания поддержки в работе по обеспечению общественной безопасности представляются теми факторами, которые необходимы для повышения результативности, это особенно касается «увеличения финансирования

исследований по вопросам инструментария судебной экспертизы и криминалистического анализа, подготовки и квалифицированных кадров». Несмотря на потребность в «дополнительных ресурсах, готовности к взаимодействию со стороны правоохранительных органов и развитии прикладных исследований в научных учреждениях», присутствует значительный потенциал для расширения сотрудничества с государственными учреждениями и правоохранительными органами.

Киберпреступники и кибертеррористы постоянно берут на вооружение все новые практики, программные решения и технологические новации. Все это происходит на фоне революции в финансовом секторе, связанной с проникновением в финансовые технологии новых способов шифрования, транзакций и т. и. В этих условиях стратегии кибербезопасности и соответствующие им нормативы, процедуры и программные средства, а также системы стресс-тестирования и подготовки кадров требуют периодического пересмотра и обновления. Только при постоянном изменении программные, аппаратные, организационные, управленческие и кадровые решения в сфере кибербезопасности будут опережающим образом адаптированы к множащимся рискам, возрастающим угрозам и стремительному изменению киберсреды. Проблемы в иных, нефинансовых секторах экономики, и особенно в энергетике и телекоммуникациях, могут оказать заметное позитивное или негативное влияние на ситуацию с кибербезопасностью в финансовом секторе. Поэтому руководители и акционеры финансовых институтов, первые лица государственных органов должны рассматривать вопросы кибербезопасности как ключевые вопросы не просто развития, а выживания общества, бизнеса и государства. Вопросы кибербезопасности должны найти свое место в рамках любых управленческих процессов в сфере бизнеса, национальной безопасности и государственной службы.

Использование новейших технологий в предупреждении преступлений.

В настоящее время во Великобритании не менее 70% хранилищ данных о криминале занимают видео- и фотофайлы. С переходом городов Великобритании с населением свыше 100 тыс. человек и всех транспортных коммуникаций страны на 100%-ный охват видеонаблюдением (не позднее 2018 г.) именно видеофайлы станут основным элементом данных и материалом для профилактики преступности и проведения расследований. В настоящее время перед системой криминальной юстиции и обеспечения правопорядка в Великобритании стоит задача не только технически ответить на этот вызов, но и оснаститься средствами и инструментами, позволяющими максимально полно использовать видеоинформацию совместно с текстовой и аудиоинформацией. Британская полиция использует большие данные и технологии, причем не только программные, но и физические технологии . В отличие от ряда других стран британский криминал уступает полиции по своей оснащенности. Это дает определенные преимущества в ведении правоохранительной деятельности.

Анализ больших данных. Электронные устройства генерируют новые данные с невероятной скоростью. Значительная часть данных может быть использована для профилактики преступности. Если раньше общественность интересовали прежде всего процедуры доступа к персональным и корпоративным данным, то в ближайшие годы необходимо четко регламентировать доступ правоохранительных структур к потоковым видеоданным, протоколам платежных систем и конечно же протоколам «Интернета вещей». Уже сегодня данные, в том числе геолокация, получаемые со смартфонов, позволяют раскрыть и предотвратить многие серьезные преступления.

Благодаря расширенному использованию информационных технологий

в борьбе с преступностью и с чрезвычайными обстоятельствами, стало возможным:

– реализовать автоматический анализ видеоинформации для предотвращения преступлений;

– ускорить расследование преступлений в 10—30 раз;

– использовать автоматизированные предсказания, поиск ассоциативных связей и техники кластеризации данных для ускорения принятия решений;

– автоматизировать процесс построения регламентов ответа на чрезвычайные ситуации;

– обеспечить сопровождение событий и отображение местонахождения сил и средств в реальном времени.

Искусственный интеллект. В ряде штатов США использование полицией методов и алгоритмов кластеризации и классификации технологии Text Mining (интеллектуальный анализ текста) для выделения криминально значимой информации совместно с технологией Visual Mining (визуальный анализ) в режиме реального времени обеспечивает возможность выполнения аналитической работы по профилактике и расследованию преступлений в автоматизированном режиме на качественно новом уровне. Эта возможность реализована в интеллектуальной системе криминального анализа в реальном времени RICAS (Real-time Intelligence Crime Analytics System), которая позволяет связать географическое пространство, время, лица и события в одном визуальном пространстве отображения.

RICAS – это интеллектуальная система криминального анализа данных, которая объединила в едином пространстве отображения основные и наиболее передовые методы и методики криминального анализа и аналитического поиска в реальном времени, что позволяет значительно повысить эффективность и результативность раскрытия преступлений по горячим следам и не раскрытых ранее преступлений, а также предотвращать

готовящиеся преступления.

Глобальная навигационная система – это совокупность методов, программных и технических средств, позволяющих организовать фиксацию пространственно-временной информации и получение ее правоохранительными органами. Целью создания данной системы является повышение уровня информационно-аналитического обеспечения деятельности правоохранительных органов при осуществлении расследования и предупреждение преступлений.

Глобальная навигационная система представляет собой совокупность средств получения, а также программно-аппаратных комплексов обработки и передачи пространственно-временной информации. Комплекс средств получения пространственно-временной информации включает в себя следующие подсистемы: ГЛОНАСС, подсистему стационарной связи, подсистему мобильной связи, подсистему радиочастотной идентификации, подсистему видеофиксации, подсистемы фиксации фактов обращения и персонализации.

Распознавание лиц преступников на базе нейронных сетей. В 2014 г. ФБР США объявило об успешном запуске в эксплуатацию ***системы распознавания нового поколения (NGI)***. Ее целью является расширение возможностей ведомства по идентификации граждан. Основной особенностью NGI является то, что она получает и обрабатывает биометрические данные автоматически. Система работает за счет информации, получаемой с камер видеонаблюдения по всей стране. Она выявляет уникальные черты лица того или иного человека и сохраняет их в базе данных. Затем при расследовании преступления она сможет провести быстрый анализ снимков и обнаружить злоумышленников. Для идентификации человека достаточно обнаружить, например, характерный шрам на его лице или татуировку на теле.

Помимо распознавания лиц NGI способна идентифицировать человека по его зрачку. В последнее время фотографии зрачков заключенных активно собирают в американских тюрьмах. Теоретически они могут использоваться для идентификации злоумышленников на месте преступления.

Новые технологии прогнозирования преступного поведения. Ученые из Шанхайского университета транспорта использовали различные алгоритмы машинного зрения, чтобы изучить лица преступников и законопослушных граждан, а затем проверили, может ли машина выявить разницу.

В отличие от человека компьютерный алгоритм классификации изображений совершенно не отягощен багажом субъективности, не имеет эмоций и неточностей, связанных с прошлым опытом, расовыми, религиозными или политическими предпочтениями, полом, возрастом и т.д., он не утомляется и не страдает от последствий недостатка сна или пищи, пишут китайские ученые, предлагая свою автоматизированную систему предсказания преступных наклонностей на основе снимков лиц.

Компания Cloud Walk (КНР), проводит машинное обучение систем лицевого распознавания, а также анализа и оценки больших массивов данных для отслеживания уровня риска потенциальных преступников. Те, кто является завсегдатаями магазинов по продаже оружия или часто посещает различные транспортные узлы, вероятнее всего, будут отмечены системой. Под «подозрение» могут попасть даже посетители хозяйственных магазинов, потому как эти места рассматриваются властями зонами «повышенного риска».

«Конечно, если кто-то покупает кухонный нож, то здесь нет ничего криминального. Но если этот же человек вдогонку покупает мешок и молоток, то для системы он станет подозрительным», – отметил представитель компании Cloud Walk.

Как утверждают эксперты, подобное исследование требует дальнейших изысканий, и в случае успеха подобное исследование сможет дать новый инструмент для раскрытия и предупреждения преступлений.

Основные выводы

Киберпреступность в узком смысле (компьютерная преступность) — это любое противозаконное поведение в форме электронных операций, направленное против безопасности компьютерных систем и обрабатываемых ими данных.

Киберпреступность в более широком смысле (преступления, связанные с применением компьютеров) – это любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети.

Основу современной киберпреступности составляет именно та идея, что сближение глобальных информационно-коммуникационных технологий может использоваться для совершения уголовно-наказуемых правонарушений в транснациональных масштабах.

Деяния, направленные против конфиденциальности, целостности и доступности компьютерных данных или систем, предполагающие использование компьютера в целях извлечения личной или финансовой прибыли или причинения личного или финансового вреда и связанные с содержанием компьютерных данных могут являться киберпреступлениями.

Расширение использования информационно-коммуникационных систем и Интернета создает новые возможности для преступников и стимулирует рост преступности.

Риск накапливается в результате использования собственных устройств. Основная угроза связана с отсутствием культуры понимания проблемы.

К числу оптимальных видов практики в области предупреждения киберпреступности относятся принятие законов, эффективное руководство, развитие потенциала органов уголовного правосудия и правоохранительных органов, информационно-просветительская деятельность, создание прочной базы знаний и сотрудничество между органами государственного управления, общинами, частным сектором, а также на международном уровне.

Поставщики услуг Интернета и хостинга могут сыграть ключевую роль в деле предупреждения киберпреступности. Они могут сохранять журналы соединений, которые потребуются при расследовании преступной деятельности; оказывать абонентам помощь в выявлении взломанных компьютеров; блокировать некоторые виды незаконного контента, например, спам; и, в целом, обеспечивать безопасную среду связи для своих клиентов.

Научные организации являются важным партнером в деле предупреждения киберпреступности, в том числе посредством развития базы знаний и обмена ими, разработки законодательной базы и политики, разработки технологий и подготовки технических стандартов, оказания технической помощи и сотрудничества с правоохранительными органами.

Новейшие технологии в предупреждении преступлений: анализ больших данных, интеллектуальная система, глобальная навигационная система, нейронные сети.

Вопросы для самоконтроля

1. *Что составляет основу киберпреступности?*

2. *Как влияет подключение к глобальной сети к вопросу киберпреступности?*
3. *Основные причины роста киберпреступности.*
4. *Приведите деяния, направленные против конфиденциальности, целостности и доступности компьютерных данных или систем.*
5. *Приведите деяния, предполагающие использование компьютера в целях извлечения личной или финансовой прибыли или причинения личного или финансового вреда.*
6. *Приведите деяния, связанные с содержанием компьютерных данных.*
7. *В чем состоит криминализация киберпреступности?*
8. *Что охватывает термин «предупреждение преступности» и на чем он опирается?*
9. *Поясните перечень предупреждений киберпреступности со стороны поставщиков услуг Интернета и хостинга.*
10. *Поясните участие научного сообщества в предупреждении киберпреступности.*

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента Республики Узбекистан от 7 февраля 2017 года № УП-4947 «О Стратегии действий по дальнейшему развитию Республики Узбекистан».
2. Постановление Президента Республики Узбекистан Шавката Мирзиёева “О мерах по коренному совершенствованию системы распространения актов законодательства” от 8 февраля 2017 года №ПП-2761.
3. Мирзиёев Шавкат Миромонович. Критический анализ, жесткая дисциплина и персональная ответственность должны стать повседневной нормой в деятельности каждого руководителя. Доклад на расширенном заседании Кабинета Министров, посвященном итогам социально-экономического развития страны в 2016 году и важнейшем приоритетным направлениям экономической программы на 2017 год. / Ш.М. Мирзиёев. – Ташкент: Узбекистон, 2017. - 104 с.
4. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе / В. Ю. Агибалов. - М.: Юрлитинформ, 2012.-152 с.
5. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А., Стеганография, цифровые водяные знаки и стеганоанализ, Монография, 2009 г.
6. Андреев Б.В. Расследование преступлений в сфере компьютерной информации. М.: Юр- литинформ, 2001. 250 с.
7. Бегларян М.Е. Судебная компьютерно-техническая экспертиза: научно-практическое пособие -М.: Юнити-Дана, 2014. 71 с.
8. Белкин А.Р. Криминалистические классификации. -М., 2000.
9. Быстряков Е.Н., Иванов А.Н., Климов В.А. Расследование компьютерных преступлений. Учебное пособие / Саратов: СГАП, 2000.-112 с.
10. Волеводз А.Г. Следы преступлений, совершенных в компьютерных

сетях // Российский следователь. 2002. № 1.С. 4–12.

11. Всестороннее исследование проблемы киберпреступности. Доклад управления организации объединенных наций по наркотикам и преступности. Организация Объединенных Наций, февраль 2013 г.
12. Гаврилов М.В., Иванов А.Н. Осмотр места происшествия при расследовании преступлений в сфере компьютерной информации. – Саратов, СГАП, – 2006, 2008 г. 136 с.
13. Гатин Р.Б. Расследование преступлений связанных с внедрением новейших технологий / Науки и жизнь. 2001 - 45 с.
14. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. - К.: МК-Пресс, 2006. - 288 с.
15. Криминалистика. Учебник / под ред. Ищенко Е.П., Филиппов А.Г. – М.: изд-во «Проспект», 2007.
16. Криминалистическая видеозапись: Учебное пособие (курс лекций) / под ред. Трубицина Р.Ю. – М.: изд-во «Щит и меч», 2004.
17. Криминалистика: учебник для вузов / Т. В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская. - 4-е изд., перераб. и доп. - М.: Норма: Инфра-М, 2014. - 928 с.
18. Криминалистика: информационные технологии доказывания: учебник под ред. В.Я. Колдина. М.: Зерцало, 2007. 752 с.
19. Кэрриэ Б. Криминалистический анализ файловых систем. СПб.: Питер, 2006. 480 с.
20. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. Воронеж: ВГУ, 2001. 255 с.
21. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: ВГУ, 2002. 408 с.
22. Нехорошев А.Б. Компьютерные преступления: квалификация, расследование, экспертиза: в 2 ч. / А.Б. Нехорошев; под ред.

В.Н. Черкасова. Саратов: СЮИ МВД России, 2004. Ч. 2. Расследование и экспертиза. 372 с.

23. Нехорошев А.Б., Шухнин М.Н., Яковлев А.Н., Юрин И.Ю. Практические основы компьютерно-технической экспертизы (учебно-методическое пособие). Саратов: Издательство «Научная книга», 2007. – 266 с.
24. Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. - М. : Норма : ИНФРА-М, 2018. - 352 с.
25. Протасевич А.А. Борьба с киберпреступностью как актуальная задача современной науки / А.А. Протасевич, Л.П. Зверянская // Криминологический журнал Байкальского государственного университета экономики и права. 2011. № 3. С. 28–33.
26. Россинская Е. Р. Судебная компьютерно-техническая экспертиза / Е. Р. Россинская, А. И. Усов. -М.: Право и закон, 2001. -416 с.
27. Савельева М.В., Смушкин А.Б. Криминалистика. Учебник. М,: Издательство Издательский дом «Дашков и К». - 2009 г. – 608.
28. Семикаленова А. И. Мобильные телефоны сотовой связи - новые объекты судебной компьютерно-технической экспертизы / А.И. Семикаленова, К.А. Сергеева // Законы России, опыт, анализ, практика. 2011. № 12. С. 89–94.
29. Федотов Н.Н. Форензика. Компьютерная криминалистика. М.: Юридический Мир, 2007. - 432 с.
30. Чернышов В.Н., Сысоев Э.В., Селезнев А.В., Терехов А.В. Технико-криминалистическое обеспечение следствия: Учебное пособие. Тамбов: Изд-во Тамб. гос. техн. ун-та, 2005.
31. Caloyannides M.A. Privacy Protection and Computer Forensics (Second Education). – «Artech House Publishers», 2004.
32. C.Altheide & H. Carvey. Digital Forensics with Open Source Tools,

Syngress, 2011. ISBN: 9781597495868. (Required textbook).

33. Carvey H. Windows Forensics and Incident Recovery. O'Reilly, 2004.
34. Computer Forensics: Principles And Practices, 1st Edition By Linda Volonino, Reynaldo Anzaldua, Jana Godwin. 2012.
35. Gottschalk L, Liu J, Dathan B, Fitzgerald S, Stein M. Computer forensics programs in higher education: a preliminary study, SIGCSE Technical Symposium on Computer Science Education, 2005. 203–231.
36. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response – Recommendations of the National Institute of Standards and Technology (NIST), Publ. 800_86. 2006.
37. Keith John Jones, Richard Bejtlich, Curtis W. Rose. Real Digital Forensics. Mit DVD: Computer Security and Incident Response. Addison Wesley Professional, 2006 - Computers - 650 pages.
38. Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis. Digital Crime and Forensic Science in Cyberspace. 2013.
39. Spivey M.D. Practical Hacking Techniques and Countermeasures. – "Auerbach", 2008.

ПРИЛОЖЕНИЯ

Приложение 1. Образцы аппаратных средств цифровой криминалистики

Защищённый паролем жёсткий диск iStorage diskAshur

Защищенные флешки кнопочным ПИН-кодом, это самый надежный способ защитить конфиденциальные данные от несанкционированного доступа. Даже в случае утери или кражи диска с аппаратным шифрованием, можно быть уверенным, что все данные на диске не будут прочитаны посторонними лицами, даже если диск будет извлечен из корпуса.

Особенности, защищенная флешка iStorage diskAshur:

- встроенная цифровая клавиатура для ввода PIN кода (6-16 знаков);
- аппаратное шифрование данных в реальном времени;
- защита от кейлоггеров и brute-force атак;
- невозможность восстановления данных после их уничтожения;
- водонепроницаемый ударостойкий алюминиевый корпус;
- не требует установки драйверов;
- возможность работы со всеми видами ОС;
- небольшие габариты и вес.

Флеши-накопитель EPOS eFlash

Специализированный флеш-накопитель с функцией гарантированного уничтожения данных EPOS eFlash обеспечивает быстрое стирание данных во

всех ячейках флеш-памяти, включая скрытые и служебные области. EPOS eFlash не требует специальных драйверов и программного обеспечения. Для работы с накопителем нужно просто подключить его к USB порту ПК с помощью входящего в комплект поставки кабеля. Для уничтожения данных достаточно нажать скрытую кнопку на корпусе флешки, накопитель при этом должен быть подключен к ПК.

Основные особенности EPOS eFlash:

1. Гарантированное уничтожение данных с восстановлением работоспособности Flash носителя.
2. Не требуется установка специальных драйверов.
3. Высокая скорость стирания данных.
4. Возможно автономное питание для экстренного уничтожения данных в процессе транспортировки.
5. Небольшие размеры и вес.

Устройство для уничтожения данных Лавина (LAVINA)

В «Лавине» применяется физический метод уничтожения данных, основанный на воздействии на накопитель мощного электромагнитного импульса. В результате все магнитные домены носителя однородно намагничиваются до состояния насыщения. Это приводит к исчезновению магнитных переходов, в которых кодируется записанная на носителе информация. Таким образом, полное разрушение исходной магнитной структуры носителя приводит к гарантированному уничтожению всех данных, когда-либо сохраненных на нем. «Лавина» также может использоваться для уничтожения данных с других носителей, использующих магнитный принцип записи: стримерных лент, дискет, ZIP, Jazz-дисков, кассет и др.

Основные особенности:

1. Мгновенное (0,1 сек) уничтожение данных мощным

электромагнитным импульсом.

2. Гарантированное уничтожение данных на физическом уровне без возможности их восстановления.
3. Возможность уничтожения информации как на исправных, так и на неисправных накопителях.
4. Возможность массового уничтожения данных – до 100 накопителей/час
5. Простота в эксплуатации.
6. Компактные размеры и небольшой вес.

EPOS DiskMaster Portable

EPOS DiskMaster Portable разработан как универсальное средство для специалистов сервисных центров, ИТ служб и служб безопасности предприятий, обеспечивающее выполнение полного комплекса работ при эксплуатации и обслуживании жестких дисков. Прибор позволяет работать со всеми жесткими дисками с интерфейсами PATA, SATA, eSATA независимо от производителя, модели и емкости.

В отличие от программных средств с аналогичной функциональностью, прибор обеспечивает копирование и уничтожение данных в скрытой области жестких дисков HPA (Host Protected Area), а также на жестких дисках с дефектами на поверхностях.

Возможности EPOS DiskMaster Portable обеспечивают ему широкий спектр применений:

- для обеспечения безопасного хранения и предотвращения утечки информации – для уничтожения данных на жестких дисках;
- для расследования ИТ инцидентов (computer forensics) – для съема

данных с жестких дисков с защитой от записи на источник, в том числе и с защищенных областей HDD;

- для восстановления информации и ремонта HDD – для копирования данных с поврежденных жестких дисков в щадящем режиме, а также скрытия дефектных секторов.

Лаборатория для съема данных IM Solo-4 Forensic Super Kit

IM Solo-4 Forensic дает возможность предварительного просмотра данных и содержимого файлов на исследуемом HDD до его копирования и осуществляет съем и анализ данных с телефонов, смартфонов, КПК и др. мобильных устройств.

Основные функции и особенности IM Solo-4 Forensic Super Kit:

- *Непревзойденная скорость*

IM Solo-4 Forensic позволяет копировать данные, уничтожать информацию, выполнять хеш-верификацию с максимальной скоростью до 18 ГБ/мин.

- *Широкий перечень поддерживаемых накопителей*

IM Solo-4 Forensic поддерживает работу с SAS, SATA, eSATA, USB 2.0, SCSI, USB 3.0, FireWire 400/800 накопителями.

- *Способы копирования*

- Single Copy. Копирование одного исследуемого накопителя на один приемник, одновременно можно выполнять три такие задачи.
- Multi Copy. Копирование одного исследуемого накопителя на два или три приемника.
- Parallel Copy. Копирование двух исследуемых накопителей на два приемника, например, при съеме данных на RAID массивах.
- Drive Spanning. Копирование источника большого объема на несколько приемников меньшей емкости.

Криминалистическая лаборатория RoadMASSter-3 X2

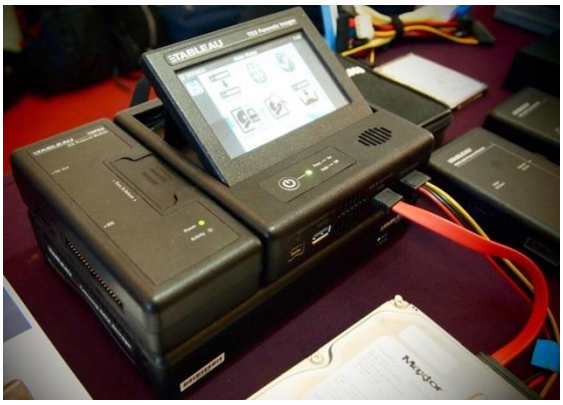
Лаборатория RoadMASSter-3X2 представляет собой многофункциональную систему на базе специализированного портативного персонального компьютера, оборудования, программного обеспечения, смонтированную в прочный корпус с защитой от электромагнитных излучений.

Основные функции и особенности RoadMASSter-3 X2 Forensic:

- *Копирование данных.* RoadMASSter-3 X2 Forensic обеспечивает съем данных практически со всех типов HDD (SAS, SATA, PATA, SCSI, USB, FireWire), SSD, флеш накопителей,CD/DVD дисков, RAID массивов (RAID 0, 1, JBOD), а также с ПК и ноутбуков без вскрытия их корпуса.
- *Анализ данных.* Лаборатория поддерживает любое специальное программное обеспечение для просмотра и анализа информации, такое как EnCase, FTK, X-Ways Forensics и др. Во время копирования информации с одного носителя исследователь может одновременно анализировать данные на других накопителях и копиях с помощью установленного на RoadMASSter-3 специального программного обеспечения.
- *Уничтожение (стирание) данных.* Стирание данных с HDD может проводится по спецификации DoD 5220-22M или в быстром однопроходном режиме.

Аппаратный комплекс UltraKit III

Набор UltraKit III от компании Digital Intelligence, США, представляет собой переносной комплект, содержащий полный набор аппаратных блокаторов записи UltraBlock производства Tableau, дополненный адаптерами и разъемами для использования в создании криминалистически значимых образов физических носителей информации - жестких дисков, разного рода накопителей, или других устройств хранения информации. Для этого достаточно выбрать из набора блокиратор с подходящим входным интерфейсом, после чего вы можете, используя функцию аппаратной защиты от записи,создать на своем компьютере образ исходного носителя.



Блокиратор записи Tableau TD3 Forensic Imager

Tableau TD3 Forensic Imager представляет собой портативное устройство с поддержкой сети. Благодаря поддержке расширенных сетевых параметров, таких как съем информации по сети, дистанционную сортировку и сетевую блокировку записи можно обеспечить удаленный доступ к устройству с помощью безопасного веб-интерфейса. Гибкая архитектура продукта имеет широкий спектр судебных случаев использования, а интуитивно понятный пользовательский интерфейс с поддержкой английского, португальского (бразильский), испанского (Испания), французского, немецкого и русского языков обеспечивает легкую работу с минимальным обучением. Цветной сенсорный экран упрощает ввод данных, просмотр журналов, подключение к сетям и завершение настройки/работы. Поддержка внешней USB-клавиатуры для еще более простого управления.

Устройство выполняет такие стандартные операции:

- дублирование данных с диска на диск (клонирование);
- создание образа диска с использованием форматов DD, .E01, .EX01 или .DMG;
- форматирование;
- стирание данных;

- хеширование (одновременный MD5 и SHA-1);
- обнаружение и удаление скрытых областей диска HPA / DCO;
- диагностика диска.

Блокиратор записиEPOS BadDrive Adapter

EPOS BadDrive Adapter – это компактный прибор, который включается в разрыв между ПК и HDD и перехватывает все передаваемые по интерфейсу команды. Если на жестком диске нет ошибок, EPOS BadDrive Adapter работает в режиме традиционного блокиратора записи.

Возможности EPOS BadDrive Adapter обеспечивают ему широкий спектр применений. Он может использоваться:

- *при расследовании ИТ инцидентов.* Обеспечивает безопасный (с защитой от записи) съем и анализ данных на жестких дисках, техническое состояние которых неизвестно.
- *при восстановлении информации.* Скрытие дефектов от системы устраняет необходимость в создании промежуточных копий поврежденных HDD.
- *при обслуживании компьютерной техники*. Прибор позволяет быстро получить доступ и скопировать данные с «посыпавшегося» жесткого диска.

Планшет для экспертов-криминалистов
XRY Tablet

XRY Tablet- портативный и удобный мобильный терминал, с высокой скоростью извлечения данных и упрощенным интерфейсом

пользователя.Предоставляет оперативным службам возможность получать данные и аналитическую информацию в реальном времени. Помогает ускорить процесс предварительной оценки, предоставляя следователям и оперативникам быстрый доступ к данным, в то время как более сложным оборудованием могут воспользоваться только высококвалифицированные сотрудники.

Планшет поддерживает логическое и физическое извлечение данных из мобильных устройств через кабельное соединение и Bluetooth. При помощи простого в использовании Мастера пользователи могут легко выполнять извлечение данных, используя интуитивно понятный сенсорный интерфейс. Извлеченные данные можно просматривать и исследовать в специальном средстве просмотра XRY Viewer. Эффективная функция поиска и простая в использовании графика позволяют отобразить определенные выбранные значения извлеченных данных. В процессе извлечения создается криминалистически безопасный файл XRY, в котором всегда содержатся все извлеченные из устройства данные.

Комплекс UFED TK

Данное комплексное решение от компании **Cellebrite**, представляет собой мобильные приложения для криминалистических исследований, предварительно установленные на разные модели компьютеров повышенной прочности. UFED TK является переносным комплексом в специальном корпусе с полным комплектом необходимых периферийных устройств и принадлежностей.

Возможности Cellebrite UFED TK:

- Извлечение на физическом уровне и декодирование полученных данных с обходом блокировки вводом графического ключа / пароля / PIN-

кода с устройств Android, включая семейство Samsung Galaxy S, LG, HTC, Motorola и другие.

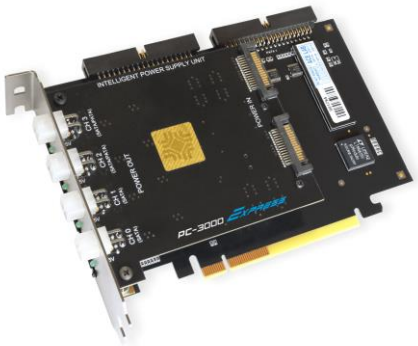
- Извлечение на физическом уровне и на уровне файловой системы, а также декодирование из устройств на базе Android.
- Извлечение на физическом уровне и декодирование из заблокированных устройств Nokia BB5 – извлечение пароля из выбранных устройств.
- Простой и быстрый доступ к заблокированным устройствам путем обхода, открытия или отключения пользовательского кода блокировки.
- Извлечение на уровне файловой системы из любых устройств Windows Phone, HTC, Samsung, Huawei и ZTE.
- Богатый выбор вариантов декодирования: Данные приложений, пароли, электронная почта, журнал вызовов, SMS, контакты, календарь, мультимедийные файлы, информация о расположении и т.п.
- Возможность комплексного анализа через UFED Physical Analyzer, включая хронологию, аналитику проекта, обнаружение вредоносного ПО и списки отслеживания.
- Удобный генератор отчетов в разных форматах с помощью UFED Physical Analyzer.

Продукт XRY Physical

XRY Physical отличается тем, что позволяет специалистам по криминалистической экспертизе расширить рамки расследования благодаря извлечению физических данных - процессу, создающему хеш-дампы из памяти телефона, обычно в обход операционной системы устройства. Часто это позволяет восстановить удаленную информацию.

XRY Physical позволяет получить данные из внутренней памяти и со съемных носителей. Кроме того, XRY Physical поддерживает создание хеш-значения копии содержимого памяти, а также отдельно расшифрованных

файлов. Благодаря обширным знаниям команды разработчиков компания MSAB целиком и полностью понимает каждую уникальную структуру памяти каждого телефона.



Программно-аппаратный комплекс PC-3000 Express

Программно-аппаратный комплекс PC-3000 Express предназначен для диагностики и ремонта (восстановления работоспособности) HDD с интерфейсом SATA (Serial ATA) и PATA (IDE).

Все специализированные утилиты входящие в комплект PC-3000 позволяют выполнить следующие действия:

- диагностировать HDD в технологическом режиме;
- проверять и восстанавливать служебную информацию HDD;
- читать и записывать содержимое Flash ПЗУ HDD;
- загружать программу доступа к служебной информации — LRD;
- просматривать таблицы скрытых дефектов P-лист, G-лист, T-лист и др;
- скрывать найденные дефекты на поверхностях магнитных дисков;
- изменять конфигурационные и идентификационные параметры;
- сбрасывать логи и S.M.A.R.T. параметры;
- подсматривать и сбрасывать пароль установленный на HDD;
- работать совместно с Data Extractor-ом.

Приложение 2. Образцы программных средств цифровой криминалистики

X-Ways Forensics

X-Ways Forensics – это интегрированный комплекс, позволяющий оперативно решать практически весь спектр задач компьютерной экспертизы и расследования ИТ инцидентов, от съема данных до составления отчетов. Благодаря этому повышается эффективность работы экспертов, существенно сокращаются сроки проведения исследований.

Основные функции и возможности X-Ways Forensics:

1. Съем и восстановление данных

- защита от записи на исследуемые носители;
- создание и восстановление образов носителей информации;
- восстановление данных на аппаратных и программных RAID массивах уровней JBOD, RAID 0, RAID 5, RAID 6 различных модификаций;
- возможность открытия файлов образов и модификации их содержимого на уровне внутренней файловой системы;
- просмотр и создание образов оперативной памяти (RAM) и виртуальной памяти запущенных процессов;
- непрерывно пополняемая база сигнатур для восстановления файлов по их внутренней структуре;
- стирание данных на различных типах носителей.

2. Просмотр и анализ данных

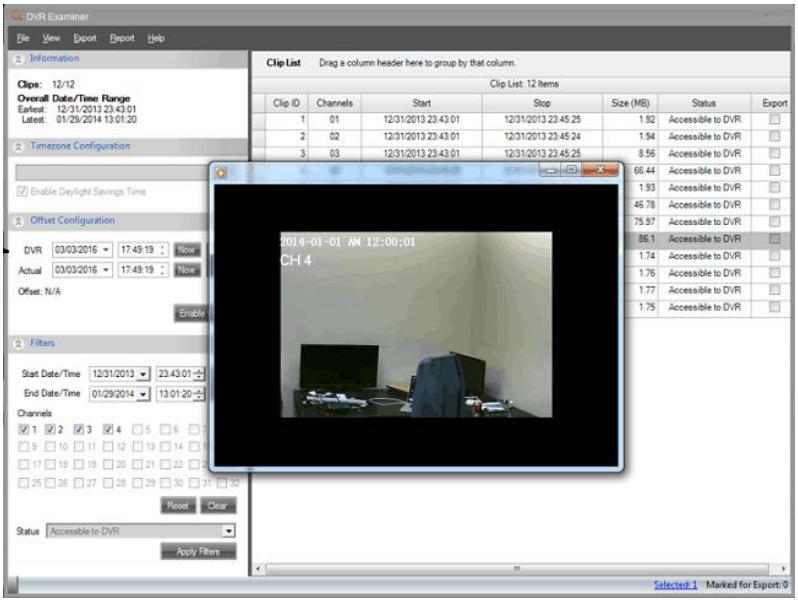
1. Анализ и редактирование логических структур данных на основе встроенных шаблонов.
2. Отображение содержимого архивов (ZIP, RAR, ARJ, GZ, TAR, 7Zip, BZIP) непосредственно в окне просмотра.
3. Возможность создания из видеозаписи набора статических кадров через заданные интервалы.
4. Автоматический поиск и извлечение изображений в других документах

(например, изображений jpeg в документах MS Office, PDF и т.п.).

5. Автоматическая идентификация сжатых и шифрованных файлов (архивов, документов MS Office, PDF).
6. Возможность создания словаря для подбора паролей на шифрованные и закрытые паролем файлы.

3. Интерфейс и совместимость

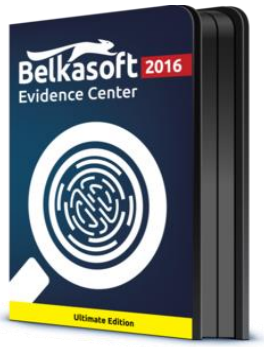
- Удобная система управления задачами и расследованиями.
- Поддержка специальных файлов-контейнеров, предназначенных для хранения и передачи релевантных файлов с сохранением всех метаданных для анализа другими участниками следствия.
- Просмотр изображений в виде галереи.
- Просмотр файлов в виде календаря по датам создания, модификации, последнего доступа.
- Автоматическое протоколирование всех операций с возможностью создания отчета в формате HTML.
- Выявление скрытых областей (HPA) жесткого диска.
- Возможность запуска с загрузочного диска или флеш на основе WinFE.



DVR Examiner - криминалистический съём и восстановление данных с видеорегистраторов.

Программа DVR Examiner от DME Forensics является решением для извлечения видео и других метаданных из видеорегистраторов, систем видеонаблюдения с криминалистической точностью. DVR Examiner позволяет экспертам обойти пароль, установленный на видеорегистраторе, и быстро извлечь данные напрямую с жесткого диска DVR устройства.

Продукт является ведущим в работе с CCTV DVR устройствами и полезен именно для экспертов-криминалистов.



Belkasoft Evidence Center (Россия)

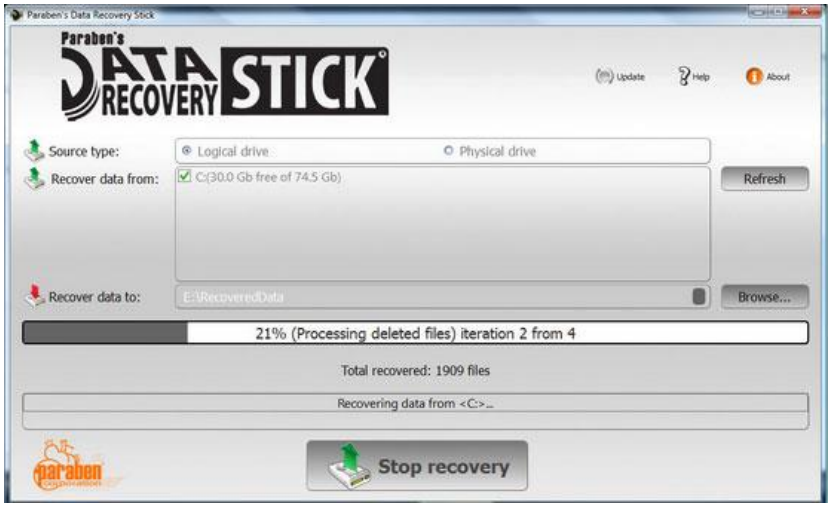
Belkasoft Evidence Center помогает экспертам-криминалистам обнаруживать скрытые и уничтоженные улики в считанные минуты. Поддерживая сотни различных артефактов, инструмент может детектировать и извлекать данные из документов в офисных форматах, интернет-чатов, социальных сетей, общение через веб-почту и многопользовательские онлайн-игры, историю работы в интернет-браузере и обмена файлами в пиринговых сетях, обеспечивает широкие возможности по поиску и анализу криминалистически значимой информации: исследование существующих файлов, восстановление файлов по их внутренней структуре, анализ дампов оперативной памяти, файлов гибернации и подкачки, исследование перехваченного трафика в виде PCAP-файлов и т.д.

Применение Belkasoft Evidence Center существенно ускоряет процесс расследования компьютерных преступлений, автоматизируя значительную часть трудоемких действий по исследованию различных типов файлов – истории сообщений мессенджеров, посещенных сайтов, почты, активности в социальных сетях или переписки в online играх.

Особенности Belkasoft Evidence Center:

- Защита от записи на исследуемые носители.
- Поддержка более 230 видов артефактов, включая все основные браузеры, почтовые клиенты, социальные сети и системы передачи файлов.
- Анализ файлов видео и изображений на наличие порнографии, лиц и текста.
- Поиск и анализ скрытых данных и файлов нераспространенных форматов.

- Восстановление удаленных файлов.
- Возможность одновременной работы нескольких пользователей.
- Создание отчетов, которые могут быть представлены в суд в качестве доказательств.



Paraben Phone Recovery Stick

Phone Recovery Stick может восстанавливать удаленные данные, такие как текстовые сообщения (SMS), переписку IM-мессенджеров, контакты, историю звонков, историю посещений Интернет, и записи календаря. Phone Recovery Stick прост в использовании, достаточно следовать простым инструкциям, и вы будете извлекать данные из устройства в кратчайшие сроки (от 10 минут до 2 часов, в зависимости от объема памяти, доступных данных, и скорости компьютера).

Особенности:

1. Восстановление удаленных данных - восстанавливает удаленные данные непосредственно с телефона и SD-карты. Он может не только восстановить текстовые сообщения, но и удаленные данные из приложений, таких как Facebook, Chrome, TextFree и многих других.

2. Получение всех пользовательских данных - загружает данные пользователя и отображает их в удобном для чтения формате, проверить все, от интернет-истории, до друзей в Facebook, Skype-переписки, закладок.

3. Безопасность источника. Первым правилом криминалистики является сохранение исходных данных. Так как Phone Recovery Stick построен на базе инструмента мобильной криминалистики, пользователь может быть уверен, что данные исследуемого телефона – в безопасности. Нет необходимости получать ROOT-права на телефоне.

Приложение 3. Сведения о разработчиках аппаратных и программных средств цифровой криминалистики

	ACE Laboratory (ООО НПП «АСЕ», Россия) – специализированное оборудование и программное обеспечение для ремонта HDD, восстановления данных с поврежденных HDD, копирования информации на HDD.
	Intelligent Computer Solutions, Inc.(США) – оборудование для высокоскоростного криминалистического сбора данных с жестких дисков. Продукты компании разрабатываются в сотрудничестве с правоохранительными органами США и других стран.
	Decision Group (Тайвань) – широкий спектр программно-аппаратных средств, мониторинга использования ресурсов Интернет, предотвращения утечки информации, анализа и восстановления утраченных данных и расследования компьютерных преступлений и инцидентов.
	Guidance Software Inc. (США) – разработчик всемирно известного ПО для расследования компьютерных происшествий «EnCase» – серии программных средств для предприятий, государственных и правоохранительных организаций.
	Cellebrite Mobile Synchronization Ltd. (Израиль) – высокопроизводительные решения в области судебно-криминалистических устройств для извлечения, декодирования и анализа данных с телефонов, смартфонов, планшетных и других портативных устройств.

	Tableau (США) – средства расследования компьютерных происшествий: устройства копирования, аппаратные блокираторы, аппаратные ускорители и программное обеспечение.
	eDEC Digital Forensics (США) – устройства и программы для компьютерной криминалистики, следующие за новейшими веяниями в отрасли. Компания известна своими средствами снятия данных со смартфонов китайского производства.
	iStorage Limited (Великобритания) – защищенные накопители с прямым вводом пароля и аппаратным шифрованием хранимой информации.
	Barracuda Networks, Inc. (США) – широкий спектр сетевых устройств и облачных услуг по обеспечению безопасности электронной почты и прочих сетевых приложений для организаций всевозможных размеров.
	**X-Ways Software Technology AG (Германия)** – криминалистическое ПО. Продукты компании предназначены для расследования компьютерных происшествий, восстановления и глубокого анализа данных, гарантированного удаления информации.
	NRTeam (NAND Recovery Team, Россия) – программные и аппаратные средства восстановления данных с Flash-накопителей. Самый известный проект лаборатории – ПО «Dumppicker» для логического восстановления информации с Flash-накопителей.

	**Rapid7 (США)** – продукты анализа и обработки рисков информационной безопасности, обладающие широким набором функциональных возможностей для выявления и уменьшения рисков, а также проверки соответствия различным стандартам информационной безопасности.
	**Secusmart GmbH (Германия)** – аппаратно-программные средства шифрования мобильной связи: звонков, сообщений SMS и электронной почты. Разрабатывает свои продукты совместно с Федеральным ведомством безопасности Германии (BSI) и производителями мобильных телефонов.
	**BelkaSoft (Россия)** – программное обеспечение для компьютерных экспертиз, обеспечивающее поиск и анализ цифровых доказательств в историях мгновенных сообщений, интернет-браузеров, ящиках почтовых клиентов, следах посещения социальных сетей, файлах видео и изображений.
	**Addonics (США)** – защищенные модульные системы хранения данных, средства шифрования информации на накопителях, дубликаторы и преобразователи интерфейсов. Разрабатываемые компанией технологии рассчитаны на обеспечение максимальной совместимости со всевозможным оборудованием и ОС.
	**Amped Software (Италия)** – программное обеспечение для криминалистического исследования цифрового фото- и видеоматериала. Продукты компании применяются экспертами-криминалистами государственных и частных организаций всего мира.

Приложение 4. Виды деяний

Деяния, направленные против конфиденциальности, целостности и доступности компьютерных данных и систем	
Незаконный доступ к компьютерной системе	Представляет собой деяния, связанные с неправомерным или необоснованным доступом к компьютерной системе в целом или ее части. Например, сюда относятся случаи, когда правонарушитель обходит брандмауэр и получает доступ к компьютерной системе банка. Сюда также могут относиться случаи, когда пользователь остается подключенным к компьютерной системе сверх отведенного ему времени, например, когда правонарушитель резервирует мощности сервера на определенный период времени, но продолжает ими пользоваться после истечения этого периода. В законодательстве некоторых стран содержится норма о том, что правонарушитель должен обойти при этом меры защиты или действовать преднамеренно.
Незаконный доступ, перехват или получение компьютерных данных	Представляют собой деяния, связанные с неправомерным или необоснованным получением доступа к компьютерным данным, включая получение не предназначенных для широкой общественности данных в процессе передачи, а также несанкционированное получение компьютерных данных. Например, сюда относятся случаи, когда правонарушитель получает незаконный доступ к компьютерной базе данных, неправомерно записывает передаваемые данные в беспроводной сети или когда правонарушитель, работающий на определенную компанию, производит несанкционированное копирование файлов, чтобы унести их с собой.
Незаконное вмешательство в данные или вмешательство в систему	Представляют собой деяния, препятствующие функционированию компьютерной системы, а также деяния, связанные с неправомерным или необоснованным повреждением, удалением, ухудшением качества, изменением или блокированием компьютерных данных. Например, сюда относятся случаи, когда правонарушитель отправляет так много запросов к компьютерной системе, что она более не может реагировать на правомерные запросы (так называемая атака типа «отказ в обслуживании»), удаляет файлы компьютерных программ, необходимые для функционирования интернет-сервера, или вносит изменения в записи в компьютерной базе данных. В законодательстве некоторых стран содержатся только нормы, касающиеся деяний, связанных с данными, в то время как в других странах установлены нормы, касающиеся и действий в отношении аппаратной части. Незаконное вмешательство в компьютерные системы, связанные с жизненно важной инфраструктурой (такие как системы водо- или

	электроснабжения) может привести к незаконному вмешательству в данные или повреждению систем.
Производство, распространение или хранение средств неправомерного использования компьютеров	Представляют собой деяния, связанные с разработкой или распространением аппаратных средств или программного обеспечения, которые могут использоваться для совершения компьютерных преступлений или преступлений, связанных с Интернетом. Например, сюда относятся случаи, когда правонарушитель разрабатывает программу для автоматизации атак типа «отказ в обслуживании». Чтобы избежать вмешательства в правомерное использование таких средств (например, специалистами по безопасности), в законодательстве некоторых стран содержится норма о том, что такие средства должны быть предназначены исключительно для неправомерных целей или что правонарушитель действует с намерением использовать эти средства для совершения преступления.
Нарушение конфиденциальности или мер защиты данных	Представляет собой деяния, связанные с использованием компьютерной системы для обработки, распространения, получения или доступа к данным личного характера в нарушение положений о защите данных. Например, сюда относятся случаи, когда правонарушитель занимается торговлей по Интернету и раскрывает данные личного характера из своей базы данных о клиентах, которую он был обязан не разглашать.
Компьютерное мошенничество или подлог	Представляет собой деяния, связанные с вмешательством или неправомерным доступом к компьютерной системе или данным с целью получения обманным или нечестным путем денег, других экономических выгод или уклонения от обязательства, а также деяния, связанные с вмешательством в компьютерную систему или данные, которое привело к созданию недостоверных компьютерных данных. Например, сюда относятся случаи, когда правонарушитель вносит изменения в программу, используемую банком, чтобы перенаправить денежные переводы на свой счет, или когда правонарушитель вносит изменения в подлинную электронную почту от финансового института преднамеренно с целью присвоить денежные средства обманным путем. Рассылка большого числа таких сообщений в целях получения данных личного характера или присвоения денежных средств обманным путем также называют «фишингом». Что касается компьютерного подлога, в законодательстве некоторых стран содержится норма о том, что исходные компьютерные данные должны касаться документации, предназначенной для формирования имеющих юридическую силу обязательств. В других странах закреплена только норма о том, что правонарушитель должен действовать с умыслом, чтобы полученная

Компьютерные преступления, связанные с использованием персональных данных	Представляют собой деяния, связанные с неправомерной передачей, хранением или использованием средств идентификации другого лица, хранящихся в компьютерных данных, с целью совершить, способствовать совершению или содействовать совершению любых неправомерных деяний. Например, сюда относятся случаи, когда правонарушитель неправомерно получает из компьютерной системы данные водительских прав и либо продает эти данные, либо использует их для сокрытия своей подлинной личности при совершении преступления. В законодательстве некоторых стран применение таких норм ограничивается определенными документами, удостоверяющими личность.
Компьютерные преступления, касающиеся авторских прав или товарных знаков	Представляют собой деяния, связанные с копированием материалов, хранящихся в компьютерных данных, или генерированием компьютерных данных в нарушение авторских прав и товарных знаков. Например, сюда могут относиться случаи, когда правонарушитель распространяет в системе обмена файлами песню, защищенную авторским правом, при отсутствии лицензии, выданной обладателем авторского права.
Распространение или контроль распространения спама	Представляют собой деяния, связанные с использованием компьютерной системы для рассылки несанкционированных или не запрошенных сообщений большому числу получателей. Во избежание вмешательства в процесс обычного общения субъектов хозяйствования со своими клиентами в законодательстве некоторых стран присутствует требование о том, что для классификации сообщения как спама в его заголовке преступник должен указать недостоверную информацию.
Деяния, предполагающие использование компьютера в целях причинения личного вреда	Представляют собой деяния, связанные с использованием компьютерной системы в целях домогательства, преследования, запугивания или угроз человеку. Например, сюда относятся случаи, когда правонарушитель отправляет обидные, угрожающие, оскорбительные или агрессивные сообщения или изображения (что также называют «троллингом») или использует компьютерную систему для отслеживания, преследования или других видов контроля или вмешательства в эмоциональное или физическое состояние человека. Деяния, заключающиеся исключительно в диффамации, к данной категории не относятся.
Компьютерные преступления, связанные с расизмом или ксенофобией	Представляют собой деяния, связанные с использованием компьютерной системы для распространения или предоставления материалов расистского или ксенофобского содержания или угроз или оскорблений группы лиц из расистских или ксенофобских побуждений. Под материалами расистского или ксенофобского содержания подразумеваются любые письменные материалы,

	изображения или отображение идей или теорий, которые поддерживают, продвигают или разжигают ненависть, дискриминацию или насилие по отношению к любым лицам или группе лиц по расовому признаку, цвету кожи, происхождению, национальной или этнической принадлежности, а также по религиозному признаку, если они используются в качестве предлога для любых из указанных факторов.
Деяния, предполагающие использование компьютера в целях завлечения детей или груминга	Представляют собой деяния, связанные с использованием компьютерной системы, чтобы предложить ребенку, не достигшему возраста согласия на вступление в половые отношения, встретиться с целью совершения сексуального преступления. Например, сюда относятся случаи, когда правонарушитель входит в интернет-чат для общения с ребенком, притворяясь тоже ребенком и предлагая ребенку встретиться с целью насилия над ребенком. Такое деяние также называют «грумингом». В законодательстве некоторых стран такие нормы ограничиваются деянием завлечения детей, за которым следуют практические действия, ведущие к встрече.
Деяния, предполагающие использование компьютера в целях содействия террористическим преступлениям	Представляют собой деяния, связанные с использованием компьютерной системы в целях содействия террористическим преступлениям. Сюда относится использование компьютерной системы для доведения до широкой общественности сообщения с целью подстрекательства к совершению террористического преступления или преступлений, если вне зависимости от наличия прямой пропаганды террористических преступлений такое деяние представляет собой угрозу возможного совершения одного или более террористических преступлений. Сюда также относится использование компьютерной системы для предоставления или сбора средств с целью их использования, или зная, что они предназначены для использования в целом или частично для совершения террористического преступления или преступлений («финансирование терроризма», связанное с использованием компьютерных систем). Сюда также относится использование компьютерной системы в целях планирования, изучения, подготовки или организации террористического преступления или преступлений («планирование террористического преступления», связанное с использованием компьютерных систем). Под террористическим преступлением понимается любое деяние, установленное в соответствии с универсальными правовыми документами по вопросам борьбы с терроризмом, или иным образом направленное на причинение смерти или серьезных телесных повреждений гражданскому лицу или любому другому лицу, не принимающему активного участия в боевых действиях в случае вооруженного конфликта.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ACL - Access Control List
CBR - Case-based reasoning
DAS - Directly Attached Storage
DNS - Domain Name System
DOS - Denial of Service
FTK - Forensic Toolkit
FTP - File Transfer Protocol
IP - Internet Protocol Address
PIN - Personal Identification Number
RAID - Redundant Array of Inexpensive Disks
TLS - Transport Layer Security
TCP - Transmission Control Protocol

АРМ – Автоматизированные рабочие места
БИС – Большая интегральная схема
ИКТ – Информационно-коммуникационная технология
ИС – Информационная система
ИТ – Информационные технологии
КТЭ - Компьютерно-техническая экспертиза
НСД - Несанкционированный доступ
ОРМ - Оперативно-розыскные мероприятия
ПК – Персональный компьютер
ПО – Программное обеспечение
СКТЭ - Судебная компьютерно-техническая экспертиза
ЦВЗ – Цифровые водяные знаки

ТЕРМИНОЛОГИЧЕСКИЙ СЛОВАРЬ

ACL (Access Control List) – список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей).

CBR (Case-Based Reasonin) – Рассуждения на основе прецедентов - в широком смысле являются методом решения новых проблем на основе уже известных решений.

DAS (Directly Attached Storage) – системы хранения данных, подключенные непосредственно к серверам.

DNS (Domain Name System), *ДНС*, служба доменных имён – система доменных имен, а также система серверов, осуществляющих разрешение доменных имен (DNS_серверов).

DoS (Denial of Service) атака – атака типа «отказ в обслуживании» на компьютерную сеть, отдельный компьютер или информационную систему.

EnCase – технология и программы для проведения всех этапов компьютерной экспертизы**.**

IP_адрес (Internet Protocol Address) – уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP.

FTK (Forensic Toolkit) – стандарт в области компьютерной экспертизы.

FTP (File Transfer Protocol) – протокол передачи файлов) - стандартный протокол, предназначенный для передачи файлов по TCP-сетям.

Proxy server – сервер посредник (брандмауэр), в котором для преобразования IP-адреса, ассоциированные с брандмауэром, используется процесс, называемый трансляцией адресов.

RAID (Redundant Array of Inexpensive Disks) – решение типичной инженерной задачи – сделать надежное устройство из ненадежных компонент.

Rootkit (руткит) – программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

TCP (Transmission Control Protocol) – протокол управления передачей, один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных. Сети и подсети, в которых совместно используются протоколы TCP и IP, называются сетями TCP/IP.

TLS (Transport Layer Security) – протокол защиты транспортного уровня, обеспечивающие защищённую передачу данных между узлами в сети Интернет.

Wireshark – анализатор сетевого трафика.

Whois – протокол, через который сервер может передать информацию клиенту о том, на кого зарегистрирован домен или его IP-адрес.

Антисоциальный тип – психопатоподобное поведение, характеризуемое импульсивностью, нарушением общепринятых норм.

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

Аутентификация (*Authentication*) – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности; в качестве указанного идентификатора чаще всего выступают **логин** и пароль **банковская (платежная) карта**, карта, карточка – средство для составления расчетных и иных документов, подлежащих оплате за счет клиента.

Аутсорс услуги (*outsourcing, outer-source-using* – использование внешнего источника и/или ресурса) - передача стороннему подрядчику ряда внутренних услуг и (или) внутренних сервисов компании-заказчика, в том числе на основе использования (например, аренды) его программных продуктов, приложений, технических средств и фрагментов инфраструктуры.

Билинговые системы – автоматизированные системы расчетов.

Бот (*Boot*) – специальная программа, выполняющая автоматически и/или по заданному расписанию какие-либо действия через те же интерфейсы, что и обычный пользователь.

Брандмауэр *(Firewall)* – метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами.

Браузер (*Browser*), веб_браузер, интернет_браузер, броузер, обозреватель, веб_клиент – программа для просмотра веб_страниц и иных сетевых информационных ресурсов; установлена на персональном компьютере пользователя, взаимодействует по сети с веб_сервером, запрашивает и принимает от него данные (обычно на языке HTML), обрабатывает и показывает их в виде веб_страницы.

Вирмейкер – программист по производству компьютерных вирусов.

Виртуальная реальность (*Virtual reality, VR, искусственная реальность*) – созданный техническими средствами мир (объекты и субъекты), передаваемый человеку через его ощущения: зрение, слух, обоняние, осязание и другие. Виртуальная реальность имитирует как воздействие, так и реакции на воздействие.

Веб_сервер – программа, установленная на сервере и осуществляющая взаимодействие браузера пользователя с **веб_сайтом** по протоколу HTTP или HTTPS.

Веб_страница – результат представления в браузере информации (обычно на языке HTML), передаваемой пользователю **веб_сервером.**

Веб_сайт - «паутина, сеть» и *site* – «место», буквально «место, сегмент, часть в сети» – совокупность логически связанных между собой **веб_страниц**; также место расположения контента сервера.

Вредоносная программа, вирус, malware – программа для компьютера, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; типы вредоносных программ: вирус, червь, троянская программа, логическая бомба, эксплоит, руткит.

Глобальная навигационная система – совокупность методов, программных и технических средств, позволяющих организовать фиксацию пространственно-временной информации и получение ее правоохранительными органами.

Дефейс – (deface – уродовать, искажать) – тип хакерской атаки, при которой главная (или другая важная) страница веб-сайта заменяется на другую – как правило, вызывающего вида (реклама, предупреждение, угроза, интернет). Зачастую доступ ко всему остальному сайту блокируется, или же прежнее содержимое сайта вовсе удаляется.

Домен – область (ветвь) иерархического пространства доменных имен сети Интернет, которая обозначается уникальным доменным именем.

Журнал восстановления – журнал, обеспечивающий возможность восстановления базы данных или файла. Содержит информацию о всех изменениях в базе данных или файле с того момента, когда было установлено, что данные достоверны и была сделана последняя резервная копия.

Звонилки (dialers) – одним из видов мошенничества является недобросовестное использование платных телефонных линий.

Зомби_сеть, ***ботнет*** (botnet) – группа компьютеров, зараженных вредоносной программой типа «троянский конь», управляемых из единого центра; как правило, такая сеть структурированная, с резервными управляющими связями; используется для рассылки спама, организации атак, сокрытия истинных источников трафика и других задач; может насчитывать от единиц до десятков тысяч компьютеров.

ИС (Информационная система) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств; информационной системой часто можно с полным основанием назвать «ЭВМ, систему ЭВМ, их сеть».

Искусственный интеллект – наука и технология создания интеллектуальных машин, особенно интеллектуальных компьютерных программ; свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека.

Инсайдер (англ. insider) – член какой-либо группы людей, имеющей доступ к информации, недоступной широкой публике. Термин используется в контексте, связанном с секретной, скрытой или какой-либо другой закрытой информацией или знаниями: инсайдер – это член группы, обладающий информацией, имеющейся только у этой группы.

Инцидент – зафиксированный случай попытки получения несанкционированного доступа или проведения атаки на компьютерную систему.

ИТ (Информационные технологии) – отрасль знаний и отрасль экономики, связанная с компьютерами, программами для ЭВМ, компьютерными сетями; тесно связана с отраслью связи.

Кардер – преступник, занимающийся мошенничеством с банковскими (платежными) картами, а именно неправомерным получением данных таких карт, их применением для приобретения товаров и услуг, изготовлением копий таких карт, их использованием в магазинах и банкоматах.

Кардинг – мошенничество с банковскими (платежными) картами каталог.

Киберпреступление – любое преступление в электронной сфере, совершенное при помощи компьютерной системы или сети, или против них.

Киберпреступность – это любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение

или распространение информации посредством компьютерной системы или сети.

Компьютерный вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия, при этом копии сохраняют способность дальнейшего распространения.

Киберсквоттинг, cybersquotting, *сквоттинг*, захват доменов – приобретение доменных имен с целью их последующей перепродажи или недобросовестного использования

Компьютерный абордаж (хакинг - hacking) - доступ в компьютер или сеть без права на то.

Компьютерно-техническая экспертиза (КТЭ) – одна из разновидностей судебных экспертиз, объектом которой является компьютерная техника и (или) компьютерные носители информации, а целью поиск и закрепление доказательств.

Контрафактный экземпляр, нелицензионная копия, *пиратский экземпляр* – экземпляр произведения (программы, фонограммы), изготовление или распространение которого влечет за собой нарушение авторских и смежных прав.

Концентратор, сетевой концентратор, hub, *хаб* – сетевое коммуникационное устройство, осуществляющее распространение (повторение) фреймов, работает на 2-м уровне, используется для соединения компьютеров в рамках одного сегмента компьютерной сети; в отличие от коммутатора, каждый полученный фрейм посылает не в один, а во все порты; как правило, не конфигурируется и не управляется.

Латентность – принято считать преступления, скрытые от органов, которым по закону представлено право расследовать или рассматривать дела о совершенных преступлениях, не выявленные этими органами и не нашедшие отражения в учете уголовно наказуемых деяний, т. е. незарегистрированные.

Лог, лог_файл – компьютерный журнал регистрации событий; файл или база данных с записями о событиях, относящихся к определенной информационной системе или программе.

Логин (login), учетное имя пользователя – символьный идентификатор учетной записи пользователя; часто используется вместе с паролем для аутентификации.

Логическая бомба – вид программы (иногда признается вредоносной), цель которой уничтожить на компьютере, где она установлена, наиболее чувствительные данные; срабатывает при выполнении или при невыполнении заранее определенных условий.

Маршрутизатор, роутер (router), *рутер* – сетевое коммуникационное устройство, осуществляющее маршрутизацию пакетов (чаще всего по протоколу IP), работает на 3-м уровне, используется для соединения различных сегментов компьютерной сети.

Несанкционированный доступ (НСД) – доступ к информационной системе или к компьютерной информации в нарушение установленного порядка; этот термин является техническим, в отличие от юридического термина «неправомерный доступ», хотя означает почти то же самое.

Обновление, *патч* (patch) – программа или набор данных с инструкцией по установке, предназначенный для модернизации отдельной программы для ЭВМ или целой информационной системы с целью увеличения ее функциональности или исправления ошибок; не имеет самостоятельной ценности, используется только вместе с обновляемой программой; обычно обновления выпускает тот же производитель, который выпустил обновляемую программу, но иногда встречаются и обновления, выпущенные иными лицами.

Оперативно-розыскные мероприятия (ОРМ) – составной структурный элемент оперативно-розыскной деятельности, состоящий из системы взаимосвязанных действий, направленных на решение определенных тактических задач.

Объектный код, исполняемый код – откомпилированный код программы для ЭВМ в машинных командах; не предназначен для восприятия человеком; получается из исходного текста методом компиляции.

Пин-код – (англ. Personal Identification Number – персональный идентификационный номер) – аналог пароля. В ходе авторизации операции используется одновременно как пароль доступа держателя карты к терминалу (банкомату) и как секретный ключ для цифровой подписи запроса. ПИН-код предусматривается для кредитных и подобных карт; с его помощью производится авторизация держателя карты.

Программное обеспечение, ПО, software, *софт, софтвер* – обобщающее название для программ для ЭВМ; термин применяется в основном при сопоставлении программной и аппаратной части (*софт* и *хард*).

Протокол коммуникационный, протокол, протокол обмена – свод правил обмена данными между различными программами, устройствами, информационными системами; обычно определяется техническим стандартом; соблюдение двумя программами единого протокола является необходимым условием их совместимости

Регистраторы - организации, занимающиеся выделением и регистрацией IP-адресов в Интернете (IP Registry).

Реферер (to refer – посылать, направлять) – человек, привлекающий пользователей на определенные интернет-ресурсы с целью заработка в рамках реферальной программы.

Сетевая карта, сетевая плата, NIC (network interface card) – плата (устройство) компьютера, выполняющая функции взаимодействия с сетью по определенному интерфейсу; как правило, вставляется в слот расширения, иногда бывает интегрирована в материнскую плату; имеет один или несколько внешних разъемов для подключения сетевого кабеля либо антенну.

Скимминг (skimming) – кража данных карты при помощи специального считывающего устройства, скиммера. Злоумышленники копируют всю информацию с магнитной полосы карты. Скиминг дает возможность узнать ПИН-код с помощью мини-камеры или накладок на клавиатуру банкомата.

Сниффер или анализатор трафика (to sniff – нюхать) – программа или устройство для перехвата и анализа сетевого трафика (своего и/или чужого).

Социальная инженерия – обход системы информационной безопасности с помощью информации, получаемой из контактов с обслуживающим персоналом и пользователям путем введения их в заблуждение различными уловками, обмана и т.д.

Спам (spam) – непрошенная массовая рекламная рассылка по электронной почте, реже по ICQ, SMS и др. системам электросвязи.

Спамер – человек, профессионально занимающийся рассылкой **спама** или сопутствующей деятельностью (сбор адресов, создание программ для рассылки, поддержание рекламируемых спамом ресурсов и т.п.).

Стеганография – отрасль науки, изучающая математические методы сокрытия конфиденциальной информации в открытых информационных массивах.

Трафик, сетевой трафик – количество информации, переданное по цифровой линии связи, измеряется в битах или байтах; реже термин

используется в значении поток информации, т.е. количество информации, переданное в единицу времени, бит/с или байт/с; содержимое передаваемых по сети фреймов, пакетов, датаграмм.

Троянская программа, *троян*, троянец – вид вредоносной программы, которая, скрытно или маскируясь под безобидную программу, несанкционированно внедряется на компьютер пользователя для выполнения действий не в интересах и помимо воли пользователя (оператора) установка программного обеспечения.

Учетная запись пользователя, аккаунт – регистрационная запись в компьютерной системе аутентификации, содержащая сведения о пользователе или ином субъекте информационного обмена, его аутентификационные данные (**логин** и пароль или хэш пароля), перечень полномочий и др.

Файл (file) – именованная область диска или иного носителя компьютерной информации; имеет отдельно заголовок с именем и иными атрибутами и отдельно тело файла; является единицей хранения информации в файловой системе.

Фишинг (phishing) – вид сетевого мошенничества, основанный на выманивании у жертвы конфиденциальных персональных данных (данных банковской карты, паролей, личных идентификационных данных) с использованием подложных писем и/или подложных вебсайтов, якобы исходящих от заслуживающих доверия инстанций (банков, провайдеров, государственных органов).

Фрикер – специалист по преодолению защиты аппаратных электронных устройств.

Хакер – компьютерный специалист очень высокой квалификации; злоумышленник, осуществляющий несанкционированный доступ к компьютерной информации, обычно через сеть.

Хэш, хэш-сумма или однонаправленная хэш-функция – представляет собой длинное число, вычисляемое из содержимого файла по особому алгоритму. Хэш-сумма похожа на контрольную сумму, но имеет одно существенное отличие: это однонаправленная функция. То есть по файлу легко вычислить его хэш-функцию, но под заданную хэш-функцию подобрать соответствующий ей файл невозможно.

Цифровой водяной знак (ЦВЗ) – технология, созданная для защиты авторских прав мультимедийных файлов. Обычно цифровые водяные знаки невидимы. Однако ЦВЗ могут быть видимыми на изображении или видео.

Обычно это информация представляет собой текст или логотип, который идентифицирует автора.

Широкополосный доступ – доступ в Интернет со скоростью передачи данных, превышающей максимально возможную при использовании.

Эквайрер – кредитная организация, осуществляющая эквайринг.

Эквайринг – деятельность кредитной организации, включающая в себя осуществление расчетов с предприятиями торговли (услуг) по операциям, совершаемым с использованием банковских карт, и осуществление операций по выдаче наличных денежных средств держателям банковских карт, не являющимся клиентами данной кредитной организации.

Эксперт-криминалист – специалист по сбору и исследованию улик с места преступления.

Эксплойт – компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на компьютерную систему.

Эскапизм – стремление бежать от реальности может возникать в виде ответной реакции на постоянный и сильный стресс, вызываемый психологическими травмами, напряжённой работой, небезопасной средой обитания или небезопасным окружением, неспособностью создать адекватные мнимому цензу отношения с окружающими субъектами представления, не занятыми «напряжённой работой».