

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания
по выполнению практических работ
по дисциплине «ЭКСПЕРТИЗА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И
КОМПЬЮТЕРНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ»
для студентов специальности 10.05.01 Компьютерная безопасность
специализация «Информационно-аналитическая и техническая экспертиза
компьютерных систем»

Ставрополь
2026

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ	2
Методические указания к лабораторным работам	4
Практическая работа № 1 Экспертиза по гражданским и уголовным делам	4
1. Нормативно-правовые акты, регламентирующие деятельность эксперта	4
2. Наказания за преступления в области компьютерной криминалистики	4
Практическая работа № 2. Компьютерная криминалистика	10
1. Двойное назначение компьютерной криминалистики.	10
2. Неотложные действия после инцидента	14
Практическая работа № 3 Компьютерная криминалистика	17
1. Цели расследования инцидента	17
2. Формирование круга подозреваемых	17
Практическая работа № 4 Компьютерная криминалистика	24
1. Основные субъекты для производства расследования	24
2. Последовательность действий при расследовании	24
Практическая работа № 5 Компьютерная криминалистика	30
1. Основные принципы изъятия компьютерной техники	30
2. Мероприятия при исследовании компьютерной техники	30
Практическая работа № 6 Компьютерная криминалистика	33
1. Правила осмотра компьютерной техники	33
2. Правила оформления документации при осмотре техники	36
Практическое занятие № 7 Компьютерная криминалистика	39
1. Оперативность	39
2. Приоритетность расследования	39
Практическое занятие № 8. Компьютерная криминалистика	45
1. Онлайн-мошенничество.	45
2. Клевета, оскорбления и экстремистские действия в Сети	49
Практическое занятие № 9 Компьютерная криминалистика	52
1. DoS-атаки	52
2. Вредоносные программы	52
Практическое занятие № 10 Компьютерная криминалистика	53
1. Кардерство	53
Использования компьютера при совершении преступлений	54
2. Посреднические онлайн-сервисы. Почему мошенничество?	56
Практическое занятие № 11 Компьютерная криминалистика	59
1. Мошенничество с трафиком	59
2. Нарушение авторских прав в офлайне	59
Практическое занятие № 12. Компьютерная криминалистика	65
1. Нарушение авторских прав в Сети	65

2. Фишинг	65
Практическое занятие № 13 Компьютерная криминалистика	68
1. Оперативно-розыскные мероприятия	68
2. Перехват и исследование трафика	70
3. Киберсквоттинг	71
4. Другое	72
Практическое занятие № 14. Компьютерная криминалистика	74
1. Шифрованный трафик	74
2. Исследование статистики трафика	75
Практическое занятие № 15. Компьютерная криминалистика	77
1. Исследование системных логов	77
1. Исследование логов мейл-сервера и заголовков электронной почты	78
2. Избирательный перехват	79
3. Исследование логов веб-сервера	80
Практическое занятие № 16. Компьютерная криминалистика	83
1. Установление принадлежности и расположения IP-адреса	83
2. Установление принадлежности доменного имени	84

Методические указания к лабораторным работам

Практическая работа № 1 Экспертиза по гражданским и уголовным делам

Цель занятия: изучить существующие классификации компьютерных преступлений

1. Нормативно-правовые акты, регламентирующие деятельность эксперта

Компьютерная преступность (преступление с использованием компьютера) – представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом, компьютерная информация является предметом или средством совершения преступления. Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга. В юридическом понятии, компьютерных преступлений, как преступлений специфических не существует. Виды компьютерных преступлений

Основные виды преступлений:

Внедрение компьютерного вируса – процесс внедрения вредоносной программы с целью нарушения работы ПК. Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер. Вирус может проявлять себя в разных формах. Это могут быть замедления в выполнении программ; увеличение объема программных файлов и наконец, эти проявления могут привести к стиранию файлов и уничтожению программного обеспечения.

Несанкционированный доступ к информации – может осуществляться с целью её хищения[прояснить](копирование на свой носитель и последующее блокирование доступа к информации) или же ради развлечения или[прояснить] последующего использования данной информации. Существуют множество способов осуществления несанкционированного доступа к системе, как правило, с использованием чужого имени; подбором паролей; изменением адресов устройств; использованием информации, оставшейся после решения задач; модификацией программного и информационного обеспечения, хищением носителей информации; установкой аппаратуры записи и т. д. **Подделка выходной информации** – подделка информации может преследовать различные цели. Итогом подделки является то, что конечному потребителю информации будут предоставлены недостоверные данные. Примером могут служить подтасовка результатов выборов или же хищение различного вида товаров, путем ввода в программу фальшивых данных; подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков; изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов.

Несанкционированное копирование конфиденциальной информации – в процессе работы каждой компании неизбежны случаи утечки конфиденциальной информации.

Несмотря на то, что защитные системы, отвечающие за хранение и доступ к внутренней информации, постоянно совершенствуются, проблема продолжает существовать. Организации несут огромные потери из-за несанкционированного распространения конфиденциальной информации. Несанкционированное копирование может осуществляться посредством изъятия средств компьютерной техники; перехвата информации; несанкционированного доступа к технике, а также манипуляции данными и управляющими командами.

2. Наказания за преступления в области компьютерной криминалистики

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. Ниже приведены названия способов совершения подобных преступлений, соответствующих кодификатору Генерального Секретариата Интерпола. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен НЦБ более чем 100 стран [5].

Все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы Q. Для характеристики преступления

могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного[6].

QA – Несанкционированный доступ и перехват QAH – компьютерный абордаж

QAI – перехват

QAT – кража времени

QAZ – прочие виды несанкционированного доступа и перехвата QD – Изменение компьютерных данных

QUL – логическая бомба QDT – троянский конь

QDV – компьютерный вирус 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 [7]

Кратко охарактеризуем некоторые виды компьютерных преступлений согласно приведенному кодификатору.

Согласно приведенному кодификатору кратко охарактеризую некоторые виды компьютерных преступлений.

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 объектам непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup). Современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата[8].

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

1. "Жучок" (bugging) – характеризует установку микрофона в компьютере с целью

перехвата разговоров обслуживающего персонала;

2. "Откачивание данных" (data leakage) – отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе;

3. "Уборка мусора" (scavenging) – 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;

4. метод следования "За дураком" (piggybacking), характеризующий несанкционированное проникновение как в пространственные, так и электронные закрытые зоны. Его суть состоит в следующем. 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;

5. метод "За хвост" (between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе;

6. метод "Неспешного выбора" (browsing). В этом случае несанкционированный доступ 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;

7. метод "Поиск бреши" (trapdoor entry), при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;

8. метод "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[9];

9. метод "Маскарад" (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;

10. метод "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 коды пользователя.

QAT – кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты. 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 программу 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[10].

Процесс заражения компьютера программой-вирусом и его последующее лечение имеют ряд черт, свойственных медицинской практике. По крайней мере, эта терминология весьма близка к медицинской:

11. резервирование – копирование FAT, ежедневное ведение архивов измененных файлов – это самый важный и основной метод защиты от вирусов. Остальные методы не могут заменить ежедневного архивирования, хотя и повышают общий уровень защиты; 12. профилактика – раздельное хранение вновь полученных и уже эксплуатируемых программ, разбиение дисков на "непотопляемые отсеки" – зоны с установленным режимом "только для чтения", хранение неиспользуемых программ в архивах, использование специальной "инкубационной" зоны для записи новых программ с дискет, систематическая проверка ВООТ-сектора используемых дискет и др.;

13. анализ – ревизия вновь полученных программ специальными средствами и их запуск в контролируемой среде, систематическое использование контрольных сумм при хранении и передаче программ. Каждая новая программа, полученная без контрольных сумм, должна тщательно проверяться компетентными специалистами по меньшей мере на известные виды компьютерных вирусов и в течение определенного времени за ней должно быть организовано наблюдение;

14. фильтрация – использование резидентных программ типа FluShot Plus, MaseVaccinee и других для обнаружения попыток выполнить несанкционированные действия;

15. вакцинирование – специальная обработка файлов, дисков, каталогов, запуск специальных резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса, для определения заражения программы или всего диска;

16. терапия – деактивация конкретного вируса в отраженных программах с помощью специальной антивирусной программы или восстановление первоначального состояния программ путем уничтожения всех экземпляров вируса в каждом из зараженных файлов или дисков с помощью программы-фага[11].

Понятно, что избавиться от компьютерного вируса гораздо сложнее, чем обеспечить действенные меры по его профилактике.

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 (карточек и пр.).

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% всех 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[12].

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 преступлений:

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 законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества; QZS – использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера.

Некоторые специалисты по компьютерной преступности в особую группу выделяют методы манипуляции, которые имеют специфические жаргонные названия[13].

17. "Временная бомба" – разновидность логической бомбы, которая срабатывает при достижении определенного момента времени;

18. "Асинхронная атака" (asynchronous attack) состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей.

19. "Моделирование" (simulation modelling) используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления. Таким образом, осуществляется "оптимизация" способа совершения преступления

Оборудование и материалы:

-

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Изучить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выровнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и

описанный процесс выполнения вашей работы. В конце отчета приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Компьютерная преступность
2. Основные виды преступлений
3. Внедрение компьютерного вируса
4. Несанкционированный доступ к информации
5. Подделка выходной информации
6. Несанкционированное копирование конфиденциальной информации

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. –476.
1. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
4. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическая работа № 2. Компьютерная криминалистика

Цель занятия: изучить существующие классификации компьютерных преступлений

Формируемые компетенции:

1. Двойное назначение компьютерной криминалистики.

Рассмотрим некоторые приемы, применяемые в компьютерных преступлениях.

Способ, не требующий специфических знаний в области информационных технологий, заключается в том, что путем хищения, разбоя, вымогательства изымаются системные блоки или отдельные носители информации, содержащие важную информацию. Как правило, такие действия квалифицируются как «некомпьютерные» преступления. Используя средства аудио-, видео- и электромагнитного наблюдения злоумышленники могут получать доступ к важной информации либо к учетным записям пользователей, для последующего несанкционированного доступа. Объектами таких атак становятся линии связи и телекоммуникационное оборудование.

Используется для вывода из строя системы, например, с помощью одновременных множественных запросов к оборудованию. Используется либо для создания условий, при которых «вражеский» ресурс перестанет быть доступен, либо для создания аварийной ситуации, позволяющей перейти к несанкционированному доступу.

В этом случае злоумышленники, используя различные способы (вирусы, перебор паролей, ошибки в программном обеспечении, ошибки в настройках сетевых служб и т.п.), получают доступ к информации, не предназначенной для публичного использования.

Важнейшим и определяющим элементом криминалистической характеристики любого, в том числе и компьютерного, преступления является совокупность данных, характеризующих способ его совершения.

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 классифицируются на пять основных групп. При этом в качестве основного классифицирующего признака выступает метод использования преступником тех или иных действий, направленных на получение доступа к средствам компьютерной техники. Руководствуясь этим признаком, выделяются следующие общие группы:

- изъятие средств компьютерной техники (СКТ);
- перехват информации;
- несанкционированный доступ к СКТ;
- манипуляция данными и управляющими

командами; комплексные методы.

К первой группе нами относятся традиционные способы совершения обычных видов («некомпьютерных») 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, широко практикуемых в оперативно-розыскной деятельности правоохранительных

органов.

Непосредственный 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.

Электромагнитный (пассивный) перехват основан на фиксации электромагнитных излучений, возникающих при функционировании многих средств компьютерной техники, включая и средства коммуникации. Волны, излучаемые электронно-лучевой трубкой дисплея, несущие в себе определенную информацию с помощью специальных приборов можно принимать на расстоянии до 1000 м.

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

Видеоперехват заключается в действиях преступника, направленных на получение информации путем использования различной видеооптической техники.

“Уборка мусора” представляет собой неправомерное использование преступником технологических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой. Например, даже удаленная из памяти компьютера информация, подлежит быстрому восстановлению и несанкционированному изъятию с помощью специальных программных средств.

К третьей группе способов совершения компьютерных преступлений относятся действия преступника, направленные на получение несанкционированного доступа к средствам компьютерной техники. К ним относятся нижеследующие.

“За дураком”. 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.

“За хвост”. 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.

“Компьютерный абордаж”, по существу являющийся подготовительной стадией компьютерного преступления.

Данный способ совершения компьютерного преступления осуществляется преступником путем случайного перебора абонентного номера компьютерной системы с использованием модемного устройства. Иногда для этих целей используется специально созданная самодельная, либо заводская программа автоматического поиска пароля. Алгоритм ее работы заключается в том, чтобы используя быстрое действие современных компьютерных устройств, перебирать все возможные варианты комбинаций букв, цифр и специальных символов, и в случае совпадения комбинации символов производить автоматическое соединение указанных абонентов.

Используя одну из таких программ, провели эксперимент по подбору пароля путем простого перебора. В результате было установлено, что 6-ти символьные пароли подбираются примерно за 6-дневной непрерывной работы компьютера. Элементарный подсчет показывает, что уже для подбора 7-ми символьных паролей потребуется от 150 дней для английского языка до 200 дней для русского. А если есть буквы заглавные, то эти цифры надо умножить еще на 2. Таким образом, простой перебор представляется чрезвычайно трудновыполнимым.

Исходя из этого, 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.

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

Этот способ чрезвычайно распространен среди так называемых 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 взламывающих программ, вирусов, вопросов их создания и распространения.

“Брешь”. В отличие от “неспешного выбора”, когда производится поиск уязвимых мест защите компьютерной системы, при данном способе преступником осуществляется их конкретизация: определяются участки, имеющие ошибку или неудачную логику программного строения. Выявленные таким образом “бреши” могут использоваться преступником многократно, пока не будут обнаружены.

“Люк”. Данный способ является логическим продолжением предыдущего. В этом случае в найденной “бреши” программа “разрывается” и туда дополнительно преступник вводит одну или несколько команд. Такой “люк” “открывается” по необходимости, а включенные команды автоматически выполняются.

Необходимо заметить, что подобный “черный вход” в якобы защищенную систему имеется в любой сертифицированной государством программе, но об этом не принято распространяться вслух.

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 экономическими преступлениями.

Наиболее широко используются следующие способы совершения компьютерных преступлений, относящихся к этой группе.

Подмена данных - наиболее простой и поэтому очень часто применяемый способ совершения преступления. Действия преступников в этом случае направлены на изменение или введение новых данных, которые осуществляются, как правило, при вводевыводе информации.

“Троянский конь”. Данный способ заключается в тайном введении в чужое программное обеспечение специально созданных программ, которые, попадая в информационно- вычислительные системы, начинают выполнять новые, не планировавшиеся законным владельцем программы, с одновременным сохранением прежней ее работоспособности.

В соответствии со ст. 273 Уголовного кодекса Российской Федерации под такой программой понимается “программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети”.

По существу, “троянский конь” - это модернизация уже рассмотренного нами способа “люк” с той лишь разницей, что он “открывается” не при помощи непосредственных действий самого преступника (“вручную”), а автоматически - с использованием специально подготовленной для этих целей программы без дальнейшего непосредственного участия самого преступника.

С помощью данного способа преступники обычно отчисляют на заранее открытый счет определенную сумму с каждой операции. Возможен здесь и вариант увеличения преступниками избыточных сумм на счетах при автоматическом пересчете рублевых

остатков, связанных с переходом к коммерческому курсу соответствующей валюты. Разновидностями такого способа совершения компьютерных преступлений является внедрение в программы “логических” и “временных бомб”, разнообразных компьютерных вирусов.

С уголовно-правовой точки зрения, согласно ст. 273 Уголовного кодекса РФ, под компьютерным вирусом следует понимать вредоносную программу для ЭВМ, способную самопроизвольно присоединяться к другим программам (“заражать” их) и при запуске последних выполнять различные нежелательные действия: порчу файлов, искажение, стирание данных и информации, переполнение машинной памяти и создание помех в работе ЭВМ.

Копирование (тиражирование) программ с преодолением программных средств защиты. Этот способ предусматривает незаконное создание копии ключевой дискеты, модификацию кода системы защиты, моделирование обращения к ключевой дискете, снятие системной защиты из памяти ЭВМ и т.п.

Не секрет, что подавляющая часть программного обеспечения, используемого в России, является пиратскими копиями взломанных хакерами программ. Самой популярной операционной системой в России является Microsoft Windows'95. По статистике, на долю этой платформы приходится свыше 77 процентов отечественного рынка операционных систем. Своим бесспорным успехом на российском рынке Windows'95 обязана деятельности компьютерных пиратов. По данным антипиратской организации BSA, свыше 90 процентов используемых в России программ установлены на компьютеры без лицензий, тогда как в США не более 24 процентов.

Можно привести в качестве примера и широко известную отечественную программу “Консультант-плюс” содержащую периодически обновляемую компьютерную базу российского законодательства. Несмотря на постоянную работу программистов фирмы по улучшению систем защиты, тысячи нелегальных копий взломанной программы имеют хождение на территории страны. Последняя уже шестая версия “Консультанта” была “привязана” к дате создания компьютера, записанной в его постоянной памяти. Не прошло и двух недель после выхода этой версии, как хакерами была создана программа, эмулирующая нужную дату на любой ЭВМ. Теперь любой желающий может найти такую программу в компьютерных сетях и бесплатно установить на свой компьютер базу данных стоимостью более 1000\$ США.

Успехи хакеров настолько велики, что, например, США намерены использовать их в информационной войне.

С момента официального признания в 1993 году военно-политическим руководством США “информационной войны” в качестве одной из составляющих национальной военной стратегии, ускоренными темпами идут поиски методов, форм и средств ее ведения. Так, в последние годы все чаще говорят о целесообразности привлечения хакеров на различных стадиях “информационной войны”. 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. Кроме того, обозначенная видимость законного пользователя дает возможность хакеру-разведчику сформировать ложную систему и ввести ее в сеть противника в качестве законного пользователя информации.

Не менее эффективным может являться применение опыта хакеров в электронной войне при решении задач дезинформирования и пропаганды через информационные системы и сети противника. Для хакеров не составляет проблемы манипулирование данными, находящимися в базах данных противника. Им также не трудно лишить противника возможности доступа к

информационным ресурсам, использование которых входило в его планы. Для этого могут использоваться способы загрузки систем большим количеством сообщений, передаваемых по электронной почте, или заражение систем противника компьютерными вирусами.

По сообщениям зарубежных СМИ, проблема использования хакеров в интересах информационной войны в настоящее время не только ограничивается изучением их опыта, но и реализуется на практике. Спецслужбы США и некоторых европейских стран уже прибегают к услугам этой категории компьютерщиков.

2. Неотложные действия после инцидента

Меры предупреждения компьютерных преступлений можно разделить на три группы: правовые, организационные и технические.

К **правовым мерам** необходимо отнести разработку законодательных актов, устанавливающих ответственность за преступления, разработку норм, защищающих авторские права. Отсутствие таких актов и норм дает возможность злоумышленникам пользоваться несовершенством законодательства и избегать ответственности за совершенные преступления.

Вступлением в силу Уголовного кодекса РФ отечественное уголовное законодательство приведено в соответствие с общепринятыми международными правовыми нормами развитых в этом отношении зарубежных стран. Теперь очередь за принятием нового уголовно- процессуального законодательства, регламентирующего все возможные следственные действия и механизм их осуществления применительно к специфике компьютерных преступлений.

Проблемы, затрудняющие предупреждение и расследование компьютерных преступлений, включают в себя:

выявившееся несовершенство УК (состав преступлений ст.ст.272, 274 - материальный (требует наличие перечисленных в законе общественно опасных последствий);

дефицит специалистов в МВД;

отсутствие наработок (методических рекомендаций по изъятию, обыску, осмотру места происшествия и т.п.);

несовершенство УПК (в частности неясно, как принимать в качестве доказательства электронный документ) и некоторые другие проблемы.

Организационные меры включают в себя подборку и проверку персонала, работающего с информацией, доступ к которой необходимо ограничивать. Наличие прав работы с информацией у людей с сомнительным прошлым или относящихся к работе небрежно может привести к утечкам данных на сторону.

Необходим инструктаж сотрудников о хранении и правилах работы с данными, а также о правилах создания, смены и хранения паролей доступа. В качестве примера можно привести случай, когда при анализе уязвимостей в одной из фирм было выявлено, что сотрудники хранили пароли на листочках, приклеенных к мониторам. И такие случаи далеко не единичны. Небрежное хранение паролей, а также «легкие» пароли (например, 12345, god и т.п.), дают злоумышленникам шансы на проникновение в систему. В некоторых случаях на предприятиях составляются детальные планы по спасению либо надежному уничтожению информации в аварийных ситуациях (пожар, теракт). Кроме того, предприятия часто не указывают в договоре с сотрудником пункт о неразглашении коммерческой и служебной тайн. Это позволяет недобросовестному сотруднику чувствовать себя в относительной безопасности. Наличие такого пункта в договоре и соответствующие инструкции на рабочем месте дисциплинирует сотрудников, заставляя их более внимательно обращаться с вверенной им информацией. Отсутствие лица, отвечающего за информационную безопасность на предприятии и бесконтрольность действий сотрудников, также повышает вероятность проникновения в систему постороннего лица и утечки данных.

Всегда надо помнить, что большинство взломов, утечек и успешных атак проводится не благодаря высокому профессиональному уровню атакующего, а в результате безалаберности

безграмотности пользователей.

Технические меры делятся на две группы: аппаратные и программные.

Аппаратные меры включают в себя наличие технических устройств, обеспечивающих защиту. Например, таких как:

- источники бесперебойного питания, предохраняющие от скачкообразных перепадов или снятия напряжения;
- устройства экранирования аппаратуры и линий проводной связи;
- устройства защиты телефонии от прослушивания;
- устройства, санкционирующее физический доступ пользователя на охраняемые объекты (шифрозамки, биометрические устройства идентификации личности и т.п.);
- средства охранно-пожарной сигнализации;

Также проникновение в систему может произойти с помощью программ, принесенных на мобильных носителях информации, таких как flash-память, cd- и dvd-диски и т.п. В некоторых случаях стоит ограничивать техническую возможность использования таких носителей информации.

Набор *программных средств* обеспечения безопасности компьютерных систем в настоящий момент очень широк. В первую очередь надо отметить встроенные средства операционной системы, позволяющие разделять права пользователей, работающих за компьютером. При этом важно понимать, что каждое повышение привилегий ведет за собой увеличение вероятности проникновения в систему. Следовательно, не стоит давать пользователям прав, более чем необходимо для конкретных работ.

Следующая мера программного характера – это антивирусная защита, позволяющая обезопасить компьютеры от вредоносного программного обеспечения. Современные антивирусные программы предоставляют собой достаточно высокую степень защиты как от известных вирусов, так и от новых, за счет алгоритмов, умеющих распознавать нежелательные действия.

При работе с глобальными сетями есть вероятность проведения атаки с удаленных компьютеров на компьютеры и серверы предприятия и частных лиц. Для повышения защищенности в этом случае используют специальные программы-фильтры, позволяющие блокировать нежелательный трафик (поток данных). Такие программы получили название межсетевой экран, файрвол (**firewall**) или брандмауэр (Brandmauer). В современных операционных системах, как правило, уже имеется встроенный брандмауэр с возможностью обучения для нужд пользователя.

Кроме мер активного противодействия атакам, необходимо использовать средства протоколирования и наблюдения. Первые позволяют вести так называемые логи (logs), куда записываются все действия пользователей и сообщения различных служб компьютера. Впоследствии такие записи позволяют анализировать и выявлять действия злоумышленников.

Средства наблюдения за сетью дают возможность просматривать и контролировать трафик, на предмет излишней активности или подозрительных операций. Такие программы называются мониторы. Кроме того, есть специальные программы-сканеры для выявления узких мест и уязвимостей в системе.

Еще один способ защиты информации – шифрование данных. Шифрование может использоваться при передаче данных по линиям связи либо при хранении данных.

Оборудование и материалы:

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

- Изучить рекомендуемую литературу.

- Выполнить практическую работу.
- Ответить на контрольные вопросы.
- Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выровнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчета приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте. **Контрольные вопросы:**

1. Способы совершения компьютерных преступлений.
2. Что понимается под способом совершения преступления
3. Что понимается под непосредственным активным перехватам
4. Что понимается под аудиоперехватом
5. Что понимается под видеоперехватом
6. Меры предупреждения компьютерных преступлений

Список литературы, рекомендуемый к использованию по данной

теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. –476.
6. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
7. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
9. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическая работа № 3 Компьютерная криминалистика

Все способы совершения компьютерных преступлений можно объединить в **три основные группы**:

- методы перехвата;
- методы несанкционированного доступа;
- методы манипуляции.

1. Цели расследования инцидента

Непосредственный перехват - 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.

Электромагнитный перехват. Перехват информации осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Может осуществляться преступником, находящимся на достаточном удалении от объекта перехвата.

2. Формирование круга подозреваемых

Эти методы в профессиональной среде получили следующие специфические названия. **Метод следования "За дураком"**. Имеет целью несанкционированное проникновение в пространственные и электронные закрытые зоны. Его суть состоит в следующем. 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.

Метод "За хвост". Используя этот метод, можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе.

Метод "Компьютерный абордаж". Обычно используется для проникновения в чужие информационные сети. Злоумышленник пытается с помощью автоматического перебора абонентских номеров соединиться с тем или иным компьютером, подключенным к телефонной сети. Делается это до тех пор, пока на другом конце линии не отзовется другой компьютер. После этого достаточно подключить собственный компьютер. Угадав код можно внедриться в чужую информационную систему.

Метод "Неспешного выбора". В этом случае несанкционированный доступ 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.

Метод "Поиск бреши". Данный метод основан на использовании ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно. **Метод "Люк"** является развитием предыдущего. В найденной "бреши" программа "разрывается" и туда вставляется необходимое число команд. По мере необходимости "люк" открывается, а встроенные команды автоматически осуществляют свою задачу.

Метод "Маскарад". В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя.

Метод "Мистификация". 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 коды пользователя. **Метод "Аварийный"**. Этот прием основан на использовании того обстоятельства, что в любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ. Такая программа - мощный и опасный инструмент в руках злоумышленника.

Метод "Склад без стен". Несанкционированный доступ осуществляется в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных.

Особую опасность представляет несанкционированный доступ в компьютерные системы финансовых учреждений с целью хищения финансовых средств. Рассмотрим некоторые типичные примеры.

Пример.

По оценкам отечественных специалистов, уже сейчас хищения с применением компьютерной техники и средств электронного платежа представляют серьезную угрозу для безопасности России. В ближайшем будущем прогнозируется значительный рост преступности в данной сфере и увеличение ее доли в общем количестве преступлений.

Способы совершения компьютерных преступлений методом манипуляции

Сущность методов манипуляции состоит в подмене данных, которая осуществляется, как правило, при вводе-выводе данных. Это простейший и потому очень часто применяемый способ.

Пример.

Вариантом подмены данных является подмена кода. Рассмотрим некоторые конкретные методы:

Манипуляция с пультом управления. Манипуляция с пультом управления относится к злоупотреблению механическими элементами управления ЭВМ. Характеристика манипуляции с вычислительной техникой заключается в том, что в результате механического воздействия на технические средства машины создаются возможности манипуляции данными.

Пример.

Некоторые из таких нарушений связаны с компьютерами телефонных сетей.

Пример.

"Троянский конь" - способ, состоящий в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность;

Пример.

Действия такого рода часто совершаются сотрудниками, которые стремятся отомстить за несправедливое, по их мнению, отношение к себе либо оказать воздействие на администрацию предприятия с корыстной целью.

Пример.

"Логическая бомба" - тайное встраивание в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

"Временная бомба" - разновидность логической бомбы, которая срабатывает при достижении определенного момента времени.

"Асинхронная атака" состоит в смешивании команд двух или нескольких пользователей, чьи команды компьютерная система выполняет одновременно.

Моделирование используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления.

Реверсивная модель. Существо метода заключается в следующем. Создается модель конкретной системы. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем, исходя из полученных правильных результатов, подбираются правдоподобные желательные результаты. Затем модель прогоняется назад, к исходной точке, и

становится ясно, какие манипуляции с входными данными нужно проводить. В принципе, прокручивание модели "вперед-назад" может проходить не один раз, чтобы через несколько итераций добиться желаемого. После этого остается только осуществить задуманное.

Пример.

"Воздушный змей". В простейшем случае требуется открыть в двух банках по небольшому счету. Далее, деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так, чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз до тех пор, пока на счете не оказывается приличная сумма (фактически, она постоянно "перескакивает" с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются и владелец счетов скрывается. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике, в такую игру включают большое число банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

Пример.

Манипулирование данными осуществляется также и самими руководителями коммерческих структур с целью нанесения ущерба государству.

Пример.

Как правило, компьютерные преступления совершаются с помощью различных комбинаций вышеописанных способов.

Использование компьютера при совершении преступлений

В зависимости от способа использования компьютера при совершении преступлений Марк Экенвайлер выделяет три основные категории:

Компьютер является объектом правонарушения, когда цель преступника - похитить информацию или нанести вред интересующей его системе.

Компьютеры используются как средства, способствующие совершению такого преступления как, например, попытка преодоления защиты системы (атака), или более традиционного преступления (например, мошенничества), совершаемого с помощью электронных средств. Компьютер используется как запоминающее устройство.

При совершении ряда преступлений могут иметь место все три способа использования компьютера.

Рассмотрим каждый из видов более подробно.

1. Компьютер как объект преступления. Можно выделить две разновидности преступлений, где компьютер является объектом посягательства:

а) Изъятие средств компьютерной техники. К этой группе относятся традиционные способы совершения обычных видов преступлений, в которых действия преступника направлены на изъятие чужого имущества.

Пример.

б) Атака на компьютер с целью несанкционированного доступа в целях получения доступа к хранящейся на нем информации (хищения информации), бесплатного использования данной системы (кража услуг) или ее повреждения.

Большинство таких нарушений предполагают несанкционированный доступ к системе, т.е. ее "взлом". В общем виде используемые компьютерными преступниками методики несанкционированного доступа сводится к двум разновидностям:

"Взлом" изнутри: преступник имеет физический доступ к терминалу, с которого доступна интересующая его информация и может определенное время работать на нем без постороннего контроля.

"Взлом" извне: преступник не имеет непосредственного доступа к компьютерной системе, но имеет возможность каким-либо способом (обычно посредством удаленного

доступа через сети) проникнуть в защищенную систему для внедрения специальных программ, произведения манипуляций с обрабатываемой или хранящейся в системе информацией, или осуществления других противозаконных действий.

В данной категории преступлений выделяют также:

а) преступления, совершаемые в отношении компьютерной информации, находящейся в компьютерных сетях, в том числе сети Интернет;

б) преступления, совершаемые в отношении компьютерной информации, находящейся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (пейджер, сотовый телефон, кассовый аппарат и т.п.).

Отмечается тенденция к переходу от разовых преступлений по проникновению в системы со своих или соседних рабочих мест к совершению сетевых компьютерных преступлений путем "взлома" защитных систем организаций.

Хищение информации. Правонарушения, связанные с хищением информации, могут принимать различные формы в зависимости от характера системы, в отношении которой осуществляется несанкционированный доступ. Информация, являющаяся объектом преступного посягательства, может быть отнесена к одному из четырех типов:

- персональные данные;
- корпоративная информация, составляющая коммерческую тайну;
- объекты интеллектуальной собственности и материалы, защищенные авторским правом;
- глобальная информация, имеющая значение для развития отраслей промышленности, экономики отдельных регионов и государств.

Похищаются сведения об новейших научно-технических разработках, планах компании по маркетингу своей продукции и заключаемых сделках.

Пример.

Типичным злоупотреблением, посягающим на объекты авторских прав, являются преступления, связанные с несанкционированным размножением компьютерных программ. Предметом хищения может быть также другая экономически важная информация, в частности, реквизиты банковских счетов и номера кредитных карточек.

Пример.

Можно выделить два основных специальности действий преступников:

- электронная атака на узловые серверы и броузеры сети WWW в целях перехвата информационных потоков;
- поиск в защитных системах локальных компьютерных сетей уязвимых места и проникновение в базы данных с целью съема находящейся в них информации.

Хищение услуг. К данной группе правонарушений относится получение несанкционированного доступа к какой-то системе, чтобы бесплатно воспользоваться предоставляемыми ею услугами.

Примером преступления данной категории является фрун-фрейкинг - использование компьютера для проникновения в коммутационную телефонную систему с целью незаконного пользования услугами по предоставлению междугородной телефонной связи. Сюда же можно отнести использование ресурсов систем - объектов несанкционированного доступа для решения задач, требующих сложных расчетов, например, для определения закодированных паролей, которые они похищают с других узлов.

Уивинг - одно из наиболее распространенных преступлений этого вида, связанное с кражей услуг, происходит в процессе "запутывания следов". Злоумышленник проходит через многочисленные системы и многочисленные телекоммуникационные сети - Интернет, системы сотовой и наземной телефонной связи, чтобы скрыть свое подлинное имя и местонахождение. При такой ситуации причиной проникновения в данный компьютер является намерение использовать его как средство для атаки на другие системы. Повреждение системы. Данная группа объединяет преступления, совершаемых с целью разрушить или изменить данные, являющиеся важными для владельца или одного или многих пользователей

системы - объекта несанкционированного доступа. Данная деятельность осуществляется по двум основным специальностям:

- проводится массированная подача электронных сигналов на серверы WWW и локальных сетей в целях вывода их из строя, для чего используются специально разработанные программы.

- в базы данных ЭВМ и корпоративных сетей вводятся вирусы-роботы, которые в заданный момент искажают или уничтожают компьютерные файлы.

- манипуляции данными.

Объектом подобных атак могут стать компьютеры, соединенные с Интернетом. Маршрутизаторы - компьютеры, определяющие путь, по которому пакеты информации перемещаются по Интернету - аналогичны телефонным коммутаторам и поэтому являются объектами для опытных хакеров, которые хотят нарушить или даже изменить маршрут "трафика" в сети.

Использование вирусов. Применение данного средства повреждения компьютерных систем доступно в настоящее время не только профессиональным программистам, но и людям, обладающим лишь поверхностными познаниями в этой сфере. Во многом это обусловлено доступностью самих вредоносных программ и наличием простой технологии их создания. Непредставляет сложности купить CD-диски с программами взлома систем защиты компьютерных сетей, а также CD-диски с пакетами вирусов, которые можно использовать для заражения средств вычислительной техники. Также продается специальная программа конструктор для генерации вирусов. С ее помощью даже не специалист может создать штамм вируса из готовых стандартных составных частей различных вредоносных программ. Причем каждый новый вирус, сгенерированный программой-конструктором, не определяется

антивирусом, пока его копия не попадет к авторам антивирусных программ. Таким образом, в пользование различных лиц свободно попадают вирусные программы, а также программы конструкторы по их созданию, что может привести к тяжелым последствиям.

Особую опасность представляют злоупотребления, связанные с распространением вирусов через Интернет.

2. Компьютер как орудие преступления. Компьютеры могут использоваться в качестве орудия незаконных действий двояким способом:

а) как средство совершения традиционных преступлений (различного рода мошенничества ит.п.);

б) как средство атаки на другой компьютер.

Рассмотрим особенности этих способов использования компьютера в преступных целях. Компьютер как орудие совершения обычных преступлений. Значительная часть преступлений данной категории совершается с использованием Интернет. К ним относятся: мошенничество с предоплатой; пирамиды и письма по цепочке; виртуальные финансовые пирамиды; азартные игры он-лайн; распространение порнографических материалов и ряд других.

Компьютер как средство атаки на другие компьютеры. В некоторых случаях компьютер может одновременно являться объектом несанкционированного доступа и средством атаки. Однако в большинстве случаев атаки на компьютеры совершаются с других компьютеров, находящихся в той же сети. Поскольку такие сети - состоят из сотен или тысяч узлов на многих континентах, соответственно существует больше возможностей для несанкционированного доступа или других нарушений.

Существует две основных категории дистанционных нарушений: несанкционированный доступ и отказ в обслуживании.

При нарушении с несанкционированным доступом преступник пытается воспользоваться пробелами в области обеспечения безопасности системы в качестве средства для получения доступа к самой системе. Если ему это удастся, он может похитить или уничтожить информацию или использовать поврежденную систему в качестве платформы, с которой он сможет совершить нарушения в отношении других машин. Значительной

опасностью характеризуются подобные злоупотребления в Интернет.

При нарушении, влекущем за собой отказ в предоставлении обслуживания, цель преступника состоит в выведении из строя данной системы. При этом преступник не обязательно стремится получить к ней доступ. Наибольшее распространение получили подобные нарушения в сети Интернет.

3. Компьютер как запоминающее устройство. В данной своей функции компьютер играет в преступной деятельности роль пассивного запоминающего устройства. Часто при этом компьютер является объектом несанкционированного доступа.

Например, после взлома системы создается специальная директория для хранения файлов, содержащих программные средства преступника, пароли для других узлов, списки украденных номеров кредитных карточек. Возможности подобного использования компьютера в преступных целях многократно возрастают при использовании сети Интернет. Таблица, составленная по результатам опроса представителей служб безопасности 492 компаний, дает представление о наиболее опасных способах совершения компьютерных преступлений.

Наивысшая угроза	
Виды атак, выявленные за последние 12 месяцев	
Вирус	83%
Злоупотребление сотрудниками компании доступом к Internet	69%
Кража мобильных компьютеров	58%
Неавторизованный доступ со стороны сотрудников компании	40%
Мошенничество при передаче средствами телекоммуникаций	27%
Кража внутренней информации	21%
Проникновение в систему	20%
Допускалось несколько вариантов ответов.	

Оборудование и материалы:

—

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Изучить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выровнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и

описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Непосредственный перехват
2. Электромагнитный перехват
3. Способы совершения компьютерных преступлений методом несанкционированного доступа
4. Способы совершения компьютерных преступлений методом манипуляции

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.
1. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
4. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическая работа № 4 Компьютерная криминалистика

Цель занятия: изучить существующие классификации компьютерных преступлений

1. Основные субъекты для производства расследования

По ст. 272 УК ответственность за деяние наступает: если неправомерный доступ к компьютерной информации повлек за собой хотя бы одно из следующих негативных последствий: уничтожение, блокирование, модификацию либо копирование компьютерной информации

Информация и информационные правоотношения все чаще становятся новым предметом преступного посягательства.

При расследовании неправомерного доступа к компьютерной информации обстоятельства содеянного устанавливаются в такой очередности:

- 1) факт неправомерного доступа к информации в компьютерной системе или сети;
- 2) место несанкционированного проникновения в эту систему или сеть;
- 3) время совершения преступления;
- 4) способ несанкционированного доступа;
- 5) степень надежности средств защиты компьютерной информации;
- 6) лица, совершившие неправомерный доступ, их виновность и мотивы преступления;
- 7) вредные последствия содеянного;
- 8) выявление обстоятельств, способствовавших преступлению.

Для рассматриваемых преступлений характерны такие ситуации начала расследования:

1. Собственник компьютерной системы обнаружил нарушение ее целостности и (или) конфиденциальности, установил виновное лицо и заявил о случившемся в правоохранительные органы.

2. Собственник самостоятельно выявил названные нарушения, однако не смог установить злоумышленника и заявил о случившемся.

3. Сведения о нарушении целостности и (или) конфиденциальности информации и виновном субъекте стали известны или непосредственно обнаружены компетентным органом, владелец компьютерной системы этот факт скрывает.

4. Правоохранительным органом обнаружены признаки противоправного вторжения в компьютерную систему, виновное лицо и владелец информации неизвестны.

Факт неправомерного доступа к информации обнаруживают, как правило, пользователи компьютерной системы или сети. Такие факты иногда устанавливаются в ходе оперативно-розыскной деятельности органов внутренних дел, ФСБ, ФСНП России. Их можно выявить и в ходе прокурорских проверок, ревизий, судебных экспертиз, следственных действий по расследуемым делам.

2. Последовательность действий при расследовании

Признаками несанкционированного доступа или подготовки к нему могут служить:

а) появление в компьютере искаженных данных - является следствием воздействия специальных программ, использованных для преодоления систем защиты, либо преднамеренного искажения файлов, к которым и был осуществлён неправомерный доступ;

б) длительное необновление кодов, паролей и других защитных средств компьютерной системы - указывает на то, что преступником может являться лицо, официально работающее с данной системой, поскольку другим лицам сложно осуществить несанкционированное управление системой без привлечения к себе внимания пользователей и обслуживающего персонала системы;

в) увеличение числа сбоев в работе ЭВМ - указывает на использование специальных

программ, для преодоления системы защиты, изменения или копирования информации; г) участвовавшие жалобы пользователей компьютерной системы или сети. Таким фактам могут предшествовать или сопутствовать:

- 1) осуществление без необходимости сверхурочных работ;
- 2) немотивированные отказы отдельных сотрудников, обслуживающих компьютерную систему или сеть, от очередного отпуска;
- 3) приобретение работником для личного пользования дорогостоящего компьютера;
- 4) чистые дискеты или диски, принесенные на работу кем-то из сотрудников компьютерной системы под предлогом копирования программ для компьютерных игр;
- 5) участвовавшие случаи перезаписи отдельных данных без серьезных на то причин;
- 6) необоснованный интерес некоторых работников к содержанию чужих принтерных распечаток;
- 7) повторный ввод в компьютер одной и той же информации и др.

Необходимо выяснить также признаки неправомерного доступа, выражающиеся в отступлениях от установленного порядка обработки документов. Имеются в виду:

- а) нарушения принятых правил оформления документов и изготовления машинограмм;
- б) лишние документы, подготовленные для обработки на ЭВМ;
- в) несоответствие информации, содержащейся в первичных документах, данным машинограмм;
- г) преднамеренные утрата или уничтожение первичных документов и машинных носителей информации, внесение искажений в данные их регистрации. Следует, однако, помнить, что перечисленные признаки могут быть результатом не только злоупотреблений, но и других причин, например халатности персонала, случайных ошибок и сбоев компьютерной техники. Место несанкционированного проникновения в компьютерную систему или сеть удается установить с определенными трудностями, поскольку таких мест может быть несколько. На практике чаще обнаруживается место неправомерного доступа к компьютерной информации с целью хищения денежных средств, но для этого также приходится выявлять все места работы компьютеров, имеющих единую телекоммуникационную связь.

Гораздо проще это место устанавливается тогда, когда расследуется несанкционированный доступ к единичному компьютеру. Обыкновенно доступ имеют ограниченное количество лиц. Также проще определить способ доступа к информации. Но и тут нужно учитывать, что информация на машинных носителях может храниться в других помещениях.

Во много раз труднее определить место непосредственного применения технических средств удаленного несанкционированного доступа, которые не входят в данную компьютерную систему или сеть. Это может быть как элементарное видеонаблюдение, так и считывание электромагнитных излучений компьютера и его элементов. Излучение можно считывать даже с клавиатуры, во время набора текста, в том числе и паролей и кодов. К установлению подобного доступа необходимо привлекать соответствующих специалистов. Необходимо выяснить также место хранения информации на машинных носителях, добытой преступником в результате неправомерного доступа к компьютерной системе или сети.

Время несанкционированного доступа можно определить с помощью программ общесистемного назначения. В работающем компьютере они обычно фиксируют текущее время. Если данная программа функционирует, то при несанкционированном входе в систему или сеть время работы на компьютере любого пользователя и производства конкретной операции автоматически фиксируется в оперативной памяти. Тогда время несанкционированного доступа можно определить в ходе следственного осмотра компьютера, его распечаток или дискет, производимого с участием специалиста, чтобы информация, находящаяся в оперативной памяти ЭВМ или на дискете, не была случайно стерта. В качестве

специалистов могут выступать, например, сотрудники информационных центров МВД, ГУВД, УВД субъектов Российской Федерации. Время несанкционированного доступа устанавливается и путем допроса свидетелей из числа сотрудников данной компьютерной системы. Выясняется, когда именно каждый из них работал на ЭВМ, если это не было зафиксировано в автоматическом режиме.

Способы преступных манипуляций в сфере компьютерной информации

Способы преступных манипуляций в сфере компьютерной информации могут быть разделены на две большие группы. Первая группа осуществляется без использования компьютерных устройств в качестве инструмента для проникновения извне в информационные системы или воздействия на них. Это могут быть: хищение машинных носителей информации в виде блоков и элементов ЭВМ; использование визуальных, оптических и акустических средств наблюдения за ЭВМ; считывание и расшифровка различных электромагнитных излучений компьютера и обеспечивающих систем; фотографирование информации в процессе ее обработки; изготовление бумажных дубликатов входных и выходных документов, копирование распечаток; использование оптических и акустических средств наблюдения за лицами, имеющими отношение к необходимой злоумышленнику информации, фиксация их разговоров; осмотр и изучение не полностью утилизированных отходов деятельности компьютерных систем; вступление в прямой контакт с лицами, имеющими отношение к необходимой злоумышленнику информации, получение от них под разными предлогами нужных сведений и др. Для таких действий, как правило, характерна достаточно локальная следовая картина. Она определяется тем, что место совершения преступных действий и дислокация объекта преступного посягательства расположены вблизи друг от друга или совпадают. Приемы их исследования достаточно традиционны.

Вторая группа преступных действий осуществляется с использованием компьютерных и коммуникационных устройств. Тогда несанкционированный доступ реализуется с помощью различных способов: подбором пароля, использованием чужого имени, отысканием и применением пробелов в программе, удалённым использованием различных специализированных программ, таких как «кей-логгер» - считывает и передаёт все нажатия клавиш клавиатуры, «ред-админ» - позволяет полный удалённый контроль над компьютером, а также других мер преодоления защиты компьютерной информации. Конкретный способ несанкционированного доступа можно установить путем допроса свидетелей из числа лиц, обслуживающих компьютерную систему, и ее разработчиков. При этом следует учитывать выявленную следовую картину. У них необходимо выяснить как преступник мог проникнуть в защищенную систему, например, узнать идентификационный номер законного пользователя, код, пароль для доступа, получить сведения о других средствах защиты системы или сети ЭВМ.

Чрезвычайно важны и другие действия, направленные на фиксацию факта нарушения целостности (конфиденциальности) компьютерной системы и его последствий, следов преступных манипуляций виновного субъекта, отразившихся в ЭВМ и на машинных носителях информации, в линиях связи и др.

Способ несанкционированного доступа надежнее установить путем производства судебной информационно-технической экспертизы. Перед экспертом ставится вопрос: "Каким способом был осуществлен несанкционированный доступ в данную компьютерную систему?" Для этого эксперту нужно представить всю проектную документацию на взломанную компьютерную систему, а также данные о ее сертификации. При производстве такой экспертизы не обойтись без использования компьютерного оборудования той же системы, которую взломал преступник, либо специальных технических и программных средств.

В ряде случаев целесообразен следственный эксперимент для проверки возможности преодоления средств защиты компьютерной системы одним из предполагаемых способов. Одновременно может быть проверена возможность появления на экране дисплея

конфиденциальной информации или ее распечатки вследствие ошибочных, неумышленных действий оператора либо случайного технического сбоя в электронном оборудовании.

Выясняя надежность средств защиты компьютерной информации, прежде всего, следует установить, предусмотрены ли в данной системе или сети ЭВМ меры защиты от несанкционированного доступа, в том числе к определенным файлам. Это возможно в ходе допросов разработчиков и пользователей системы, а также при изучении проектной документации и инструкций по эксплуатации системы. Как правило, неправомерный доступ облегчается халатностью администратора системы или пользователя компьютера, что происходит в 99% случаев. Изучая инструкции, нужно обращать особое внимание на раздельно мерах защиты информации, порядке допуска пользователей к конкретным данным, разграничении их полномочий, организации контроля за доступом. При установлении лиц, совершивших несанкционированный доступ к конфиденциальной компьютерной информации, следует учитывать, что он является технологически весьма сложным. Осуществить его могут только специалисты, обладающие достаточно высокой квалификацией. Поэтому поиск подозреваемых рекомендуется начинать с технического персонала взломанных компьютерных систем или сетей. Это в первую очередь их разработчики, а также руководители, операторы, программисты, инженеры связи, специалисты по защите информации, другие сотрудники.

Следственная практика свидетельствует, что чем технически сложнее способ проникновения в компьютерную систему или сеть, тем легче установить подозреваемого, ибо круг специалистов, обладающих соответствующими способностями, весьма ограничен. С другой стороны среди «хакеров» очень популярно оставлять на месте преступления, т.е. в системе взломанного компьютера, улики, непосредственно указывающие на совершение преступления как раз лицом, официально работающим с системой. Подобные уловки могут легко завести следствие в ненужном направлении, что часто и происходит, учитывая высокую латентность подобного рода преступлений. В системе или в сети могут быть указания на то, что доступ был совершён с компьютера определённого лица. Секрет подобной уловки знает каждый начинающий хакер, для этого существует огромное количество специальных программ, помогающих получить анонимный доступ к сети, либо доступ через компьютер

«подставляемого» лица. Поэтому на практике следователь всегда должен быть крайне осторожен при определении подозреваемого или обвиняемого.

Доказыванию виновности конкретного субъекта в несанкционированном доступе к компьютерной информации способствует использование различных следов, обнаруживаемых при осмотре ЭВМ и ее компонентов. Это, например, следы пальцев, записи на внешней упаковке дискет и др. Для их исследования назначаются криминалистические экспертизы дактилоскопическая, почерковедческая и др.

Для установления лиц, обязанных обеспечивать надлежащий режим доступа к компьютерной системе или сети, следует, прежде всего, ознакомиться с должностными инструкциями, определяющими полномочия сотрудников, ответственных за защиту конфиденциальной информации. Их необходимо допросить для выяснения, кто запускал нештатную программу, и фиксировалось ли это каким-либо способом. Нужно также выяснить, кто особо увлекается программированием, учится или учился на курсах программистов, интересуется системами защиты информации.

У субъектов, заподозренных в неправомерном доступе к компьютерной информации, производится обыск в целях обнаружения: ЭВМ различных конфигураций, принтеров, средств телекоммуникационной связи с компьютерными сетями, записных книжек, в том числе электронных, с уличающими записями, дискет и дисков с информацией, могущей иметь значение для дела, особенно если это коды, пароли, идентификационные номера пользователей данной компьютерной системы, а также сведения о них.

При обыске нужно изымать также литературу и методические материалы по компьютерной технике и программированию. К производству обыска и осмотру изъятых предметов рекомендуется привлекать специалиста по компьютерной технике,

незаинтересованного в исходе дела.

Доказать виновность и выяснить мотивы лиц, осуществивших несанкционированный доступ к компьютерной информации, можно лишь по результатам всего расследования. Решающими здесь будут показания свидетелей, подозреваемых, обвиняемых, потерпевших, заключения судебных экспертиз, главным образом информационно-технологических и информационнотехнических, а также результаты обысков. В ходе расследования выясняется:

8) с какой целью совершен несанкционированный доступ к компьютерной информации;

9) знал ли правонарушитель о системе ее защиты;

10) желал ли преодолеть эту систему и какими мотивами при этом руководствовался.

Вредные последствия неправомерного доступа к компьютерной системе или сети могут заключаться в хищении денежных средств или материальных ценностей, завладении компьютерными программами, а также информацией путем изъятия машинных носителей либо копирования. Это может быть также незаконное изменение, уничтожение, блокирование информации, выведение из строя компьютерного оборудования, внедрение в компьютерную систему вредоносного вируса, ввод заведомо ложных данных и др.

Хищения денежных средств чаще всего совершаются в банковских электронных системах путем несанкционированного доступа к их информационным ресурсам, внесения в последние изменений и дополнений. Такие посягательства обычно обнаруживают сами работники банков, устанавливаются они и в ходе оперативно-розыскных мероприятий. Сумма хищения определяется посредством судебно-бухгалтерской экспертизы.

Факты неправомерного завладения компьютерными программами вследствие несанкционированного доступа к той или иной системе и их незаконного использования выявляют, как правило, потерпевшие. Максимальный вред причиняет незаконное получение информации из различных компьютерных систем, ее копирование и размножение с целью продажи либо использования в других преступных целях.

Похищенные программы и базы данных могут быть обнаружены в ходе обысков у обвиняемых, а также при оперативно-розыскных мероприятиях.

Если незаконно полученная информация конфиденциальна или имеет категорию государственной тайны, то вред, причиненный ее разглашением, определяется представителями Гостехкомиссии России.

Факты незаконного изменения, уничтожения, блокирования информации, выведения из строя компьютерного оборудования, "закачки" в информационную систему заведомо ложных сведений выявляются прежде всего самими пользователями компьютерной системы или сети. Следует учитывать, что не все эти негативные последствия наступают в результате умышленных действий. Их причиной могут стать случайные сбои в работе компьютерного оборудования, происходящие довольно часто.

При определении размера вреда, причиненного несанкционированным доступом, учитываются не только прямые затраты на ликвидацию негативных последствий, но и упущенная выгода. Такие последствия устанавливаются в ходе следственного осмотра компьютерного оборудования и носителей информации с анализом баз и банков данных. Помогут здесь и допросы технического персонала, владельцев информационных ресурсов. Вид и размер ущерба обычно определяются посредством комплексной экспертизы, проводимой с участием специалистов в области информатизации, средств вычислительной техники и связи, экономики, финансовой деятельности и товароведения.

На заключительном этапе расследования формируется целостное представление об обстоятельствах, которые облегчили несанкционированный доступ к компьютерной информации. Здесь важно последовательное изучение различных документов, особенно относящихся к защите информации. Весьма значимы материалы ведомственного (служебного) расследования.

К этим обстоятельствам относятся:

- 1) неэффективность методов защиты компьютерной информации от несанкционированного доступа;
- 2) совмещение функций разработки и эксплуатации программного обеспечения в рамках одного структурного подразделения;
- 3) неприменение в технологическом процессе всех имеющихся средств и процедур регистрации операций, действий программ и обслуживающего персонала;
- 4) нарушение сроков изменения паролей пользователей, а также сроков хранения копий программ и компьютерной информации

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Изучить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выровнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчета приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. В какой очереди устанавливается расследование неправомерного доступа к компьютерной информации.
2. Что может служить признакам несанкционированного доступа или подготовки к нему.
3. Способы преступных манипуляций в сфере компьютерной информации могут быть разделены на две большие группы.

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.
1. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
4. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическая работа № 5 Компьютерная криминалистика

Цель занятия: изучить существующие классификации компьютерных преступлений

Время, отводимое на занятие – 2ч.

1. Основные принципы изъятия компьютерной техники

При осуществлении прокурорского надзора за расследованием преступлений в сфере компьютерной информации прокурору необходимо руководствоваться не только положениями уголовно-процессуального законодательства, но и требованиями приказа Генерального прокурора Российской Федерации от 02.06.2011 N 162 "Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия".

Учитывая сложность расследования преступлений в сфере компьютерной информации, уже отмечавшуюся низкую квалификацию следственных работников, необходимость применения при расследовании специальных знаний, прокурорский надзор за расследованием данных преступлений должен осуществляться на протяжении всего периода расследования.

С целью предотвращения нарушений и затягивания сроков следствия прокурору необходимо осуществлять постоянное взаимодействие с руководителем следственного органа, привлекая прокурора, который в последующем будет поддерживать государственное обвинение в судебном заседании.

Организовать такое взаимодействие возможно в виде совместных оперативных совещаний по обсуждению хода следствия при прокуроре, проводимых как при принятии важных процессуальных решений по уголовному делу, например, при оценке достаточности доказательств для предъявления обвинения, при назначении экспертиз и обсуждении их выводов для последующего планирования расследования, при окончании предварительного следствия, при рассмотрении поступающих к прокурору жалоб и заявлений.

Более того, во многих субъектах Российской Федерации изданы межведомственные приказы и иные нормативные документы, регулирующие порядок взаимодействия при расследовании уголовных дел между следственными органами и прокурорами. Это позволяет избежать многих нарушений и недостатков предварительного расследования, которые, в свою очередь, могут повлечь за собой возвращение уголовного дела прокурором для дополнительного расследования или судом прокурору в порядке ст. 237 УПК РФ. Учитывая особенности рассматриваемой категории преступлений, прокурору следует тщательно изучать собранные в ходе предварительного расследования доказательства, которые должны в полной мере устанавливать все обстоятельства, предусмотренные ст. 73 УПК РФ. При этом, как отмечалось ранее, по составам преступлений, предусмотренных главой 28 УК РФ, помимо основных признаков преступления определяется причинноследственная связь между деянием и наступившими последствиями.

2. Мероприятия при исследовании компьютерной техники

Специфика преступлений в сфере компьютерной информации обуславливает необходимость проведения по уголовным делам данной категории ряда специальных судебных экспертиз. В связи с этим важно осуществлять прокурорский надзор уже на первоначальном этапе расследования. Изучая в процессе расследования уголовное дело, прокурор должен установить, в полной ли мере данные экспертные заключения отвечают на поставленные следователем вопросы, все ли необходимые вопросы поставлены перед экспертом и достаточно ли в конечном итоге информации, содержащейся в заключении эксперта, для подтверждения обстоятельств совершения преступления. Несомненно, надзирающий прокурор должен обладать специальными знаниями о видах судебных экспертиз, проводимых по уголовным делам данной категории, давать руководителю

следственного органа соответствующие рекомендации.

Так, при расследовании преступлений данной категории помимо традиционных видов экспертиз (криминалистической, дактилоскопической и т.д.) должны проводиться специальные судебные экспертизы - информационно-технологическая и информационно-техническая.

Объединяет эти виды судебных экспертиз компьютерная информация, исследуемая, однако, с разных сторон - технологической либо технической. Различаются они и по непосредственным объектам исследования.

Проведение указанных судебных экспертиз необходимо для исследования собственно информационно-технологических процессов сбора (накопления, хранения, поиска, актуализации, распространения) информации и представления ее потребителю в условиях функционирования автоматизированных информационных систем и сетей и отдельно взятых технических и иных средств обеспечения этих процессов.

К подобным техническим средствам относятся компьютерные устройства, включающие в себя системный блок, устройство внешней памяти, устройства ввода и вывода информации, периферийные устройства, а также средства связи и телекоммуникации. К иным средствам следует отнести программы для компьютеров. Эти средства, обеспечивающие обработку информации, и составляют основу информационно-компьютерной технологии.

Объектом информационно-технологической экспертизы является установленный порядок обработки информации, осуществляемый по заданным алгоритмам, или информационная технология, основанная на применении современной информационно-вычислительной техники, средств связи и телекоммуникаций, составляющих основу информатизации общества.

Непосредственными предметами информационно-технологической экспертизы могут быть:

проектная документация на разработку и эксплуатацию компьютерных систем и сетей, отражающая процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

документированная информация (документ), то есть зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать (отдельные документы и массивы документов в информационных системах), в том числе конфиденциальная информация; материалы сертификации информационных систем, технологий и средств их обеспечения и лицензирования деятельности по формированию и использованию информационных ресурсов;

приказы и распоряжения администрации, инструкции, протоколы, договоры, положения, уставы и методики по эксплуатации компьютерных систем и сетей, отражающие порядок формирования информационных массивов и доступа к ним (важнейшими из этих предметов исследования могут быть должностные инструкции сотрудников соответствующих информационных подразделений);

схемы движения информации от источников к потребителю с указанием пунктов ее сбора, контроля, накопления, обработки и использования; табель распределения выходных данных (перечень пользователей с указанием

периодичности, объема и сроков поступления информации), а также другие документы, позволяющие наиболее полно раскрыть сущность информационной технологии данной компьютерной системы или сети (они обычно прилагаются к техническому заданию на их разработку);

входные и выходные документы, установленные для данной автоматизированной информационной системы;

словари, тезаурусы и классификаторы;

иные эксплуатационные и сопроводительные документы (особое значение для расследования компьютерных преступлений имеют журналы и другие виды учета работы операторов, регистрации сбойных ситуаций и обращений в компьютерную систему или

сеть).

Несомненно, что все указанные документы должны быть изъяты своевременно и с соблюдением установленных законом норм. На необходимость этого прокурор должен обращать внимание следователя (в том числе на межведомственных оперативных совещаниях при обсуждении хода расследования уголовного дела), ориентируя последнего на соблюдение разумных сроков уголовного судопроизводства, установленных ст. 6.1 УПК РФ.

Практическая работа № 6 Компьютерная криминалистика

1. Правила осмотра компьютерной техники

Информационно-технологическая экспертиза назначается в тех случаях, когда для возникающих в ходе расследования вопросов требуются специальные познания в технологии информационных процессов.

Возможности этой экспертизы достаточно широки. С ее помощью можно определить: соответствие существующего технологического процесса компьютерной обработки информации проектной и эксплуатационной документации на конкретную информационную систему либо сеть; конкретные отклонения от установленной информационной технологии, а также непосредственных исполнителей, допустивших нарушение установленной информационной технологии; надежность организационно-технологических мер защиты компьютерной информации; вредные последствия, наступившие из-за неправомерного нарушения установленной технологии компьютерной обработки информации;

обстоятельства, способствовавшие преступному нарушению технологии электронной обработки информации.

Изучая заключение информационно-технологической экспертизы, прокурору следует обратить внимание на то, выяснено ли следователем:

соответствие процессов сбора, обработки, накопления, хранения, поиска и распространения информации установленной проектной и эксплуатационной документации информационной технологии в данной компьютерной системе или сети;

какие конкретно отклонения от нее допущены;

кем нарушены технологические требования в процессе эксплуатации данной компьютерной системы или сети;

кто из должностных лиц должен был обеспечить соблюдение установленной технологии электронной обработки данных;

какие организационно-технологические меры защиты компьютерной системы, предусмотренные эксплуатационной документацией, были приняты;

какие вредные последствия связаны с нарушением установленной технологии электронной обработки информации;

является ли указанное отклонение от технологии обработки данных причиной наступивших последствий;

каковы причины нарушения установленной обработки компьютерной информации; какие меры необходимо принять для их устранения.

Объектом информационно-технической экспертизы является техническое обеспечение информационной безопасности компьютерных систем и сетей.

Предметы информационно-технической экспертизы очень разнообразны. Иными словами, это инструменты, с помощью которых осуществляется доступ к информационным технологиям.

Условно их можно разделить на три основные группы:

1) технические средства обработки информации;

2) машинные носители информации и машинограммы, создаваемые средствами вычислительной техники;

3) программные средства и базы данных.

К первой группе относятся: компьютеры, отдельные узлы, устройства ввода и вывода информации; печатающие устройства (принтеры); периферийные устройства; устройства для связи между пользователями (модемы и факс-модемы); технические устройства и приспособления, специально разработанные для обхода средств защиты компьютерных систем и сетей от несанкционированного доступа; технические средства защиты информации и другие устройства.

Ко второй группе относятся: накопители на жестких дисках ("винчестеры"); накопители на гибких магнитных дисках (дискеты); устройства для быстрого сохранения всей информации, находящейся на жестком диске (стримеры); оптические диски; пластиковые

карты; аудио- и видеокассеты и другие носители информации, обрабатываемые компьютерами.

К третьей группе относятся программы для электронных вычислительных машин и базы данных.

Следует отметить, что исходя из анализа предметов указанных двух экспертиз, каждая из них имеет свои характерные особенности.

Информационно-техническая экспертиза назначается в том случае, когда в ходе следствия возникает необходимость в специальных исследованиях непосредственно технической части (отдельных узлов, блоков, периферийных устройств, оборудования, составляющих компьютерные системы или сети, пластиковых карт, дисков, дискет, других носителей информации, обрабатываемых компьютерами, а также программных средств). К ее основным задачам относятся:

- определение технического состояния компьютерного оборудования и пригодности его для решения задач, предусмотренных проектной и эксплуатационной документацией на данную автоматизированную систему; техническое исполнение конкретных технологических информационных процессов и отдельных операций, ставших предметом предварительного следствия, установление конкретного терминала, с которого совершен несанкционированный доступ в данную компьютерную систему или сеть;

- восстановление содержания поврежденных информационных массивов, отдельных файлов на магнитных носителях;

- выявление технических причин сбойных ситуаций в работе компьютера;

- установление подлинности информации, записанной на машинных носителях (дисках, дискетах, пластиковых картах), и внесенных в них изменений;

- выявление в компьютерной программе разного рода неправомерных изменений, дополнений, вставок преступного характера;

- установление вида компьютерного вируса, источника его проникновения в исследуемую систему и причиненных им вредных последствий;

- установление соответствия средств защиты информации от несанкционированного доступа и проникновения компьютерного вируса сертификационным требованиям.

Изучая заключение информационно-технической экспертизы, прокурору необходимо выяснить, установлено ли:

- техническое состояние компьютерного оборудования и его пригодность для решения в полном объеме задач, предусмотренных проектной и эксплуатационной документацией на данную компьютерную систему или сеть;

- с какого терминала и какими средствами связи и телекоммуникации мог быть совершен несанкционированный доступ в компьютерную систему или сеть;

- возможность восстановления записанной прежде информации на частично поврежденном машинном носителе и ее содержание;

- причина выявленных в ходе следствия сбоев данного компьютерного оборудования и наличие возможности их предотвращения с помощью технических средств;

- перечень действий, предусмотренных соответствующими правилами для предотвращения сбоя, несанкционированного доступа, уничтожения файла, неправомерного копирования компьютерной информации, и не выполненных ответственным лицом; признаки несанкционированных изменений информации, записанной на сменные диски (дискеты) и их содержание;

- возможность использования в данной компьютерной системе посторонних программ безавтоматической регистрации ее использования;

- наличие в программе преднамеренной "закладки" (зарезервированного места в программе на случай необходимости последующей вставки дополнительных команд), ее назначение и автор;

- средства защиты от вредоносных программ, предусмотренные в данной системе, их надежность, наличие сертификата и соответствие средств его требованиям;

процедура заражения данной системы компьютерным вирусом; класс (тип) вируса, заразившего данную компьютерную систему и источник его происхождения;
размер и характер вреда, причиненного компьютерным вирусом.

Разумеется, круг вопросов по двум указанным видам экспертиз предлагаемыми перечнями не исчерпывается. С учетом характера каждого конкретного преступления могут быть поставлены и другие вопросы, объем которых определяется следователем в зависимости от расследуемого события и выяснения обстоятельств информационно-технологического или информационно-технического характера.

Так, по делам о неправомерном доступе к охраняемой законом компьютерной информации перед информационно-технологической экспертизой могут быть поставлены более частные вопросы, относящиеся к режиму ее обработки и охраны, главным образом к организационно-административным мерам защиты этой информации.

В настоящее время встречаются и другие виды экспертиз компьютерно-технической информации, что обусловлено динамичным развитием сферы высоких технологий, например, экспертиза электронно-цифровой подписи; экспертиза процесса разработки и использования программного обеспечения; компьютерно-сетевая экспертиза, экспертиза обстоятельств создания и использования файлов и баз данных и др. Все они отличаются, как правило, предметом, целью исследования и вопросами, которые могут быть поставлены перед экспертом.

В процессе расследования преступлений в сфере компьютерной информации может возникнуть необходимость производства и других видов экспертиз.

Например, идентификационная задача может быть решена с помощью комплексной компьютерно-технической и судебно-автороведческой экспертизы, позволяющей проверить, не написана ли данная компьютерная программа конкретным лицом.

Для проведения носящих комплексный характер экспертных исследований в сфере компьютерной информации приглашаются высококвалифицированные специалисты в области информатики, вычислительной техники и программирования, а также традиционных видов криминалистической экспертизы, экономической, финансовой, бухгалтерской и товароведческой экспертиз.

В ходе комплексной судебно-бухгалтерской экспертизы и экспертизы программного обеспечения устанавливают: возможность несанкционированного скрытого доступа к программному обеспечению с целью внесения изменений, влияющих на результаты расчетов и отчетность, механизм совершения таких изменений, их характер и последствия;

кто из работников учреждения, обслуживающих и эксплуатирующих эти средства, имеет указанные выше возможности;

размер причиненного материального ущерба;

какие нарушения правил, регламентирующих ведение бухгалтерского учета и отчетности, могли способствовать образованию ущерба;

какая операционная система использована в конкретном компьютере; не вносились ли в программу данного системного продукта какие-либо коррективы, изменяющие выполнение операций (какие именно); возможно ли получение доступа к конфиденциальной финансовой информации, имеющейся в данной сети, и каким образом может быть осуществлен этот доступ.

Поскольку подлинная информация на машинных носителях при производстве экспертиз может быть безвозвратно уничтожена, следует убедиться в ее наличии в уголовном деле в качестве вещественного доказательства и направлении для проведения экспертного исследования ее копии.

В случае, если прокурор установит, что какие-либо вопросы в заключении эксперта раскрыты не полностью или невозможно сделать однозначный вывод об исследуемых обстоятельствах на основании данного заключения, целесообразно ориентировать следователя провести допрос эксперта с целью устранения указанных недостатков. Учитывая, что необходимо осуществлять надзор также и за соблюдением разумных сроков уголовного судопроизводства, нарушение которого ущемляет права потерпевших, назначать

дополнительную судебную экспертизу следует только в том случае, если возникшие вопросы нельзя выяснить в ходе допроса эксперта. Невыяснение всех необходимых вопросов в ходе экспертного исследования может впоследствии негативно сказаться на сроках судебного рассмотрения уголовного дела.

Если же прокурор выявляет уже допущенное в ходе предварительного расследования нарушение, то он должен использовать предоставленные ему Уголовно-процессуальным кодексом Российской Федерации полномочия и внести требование об устранении нарушений, допущенных в ходе предварительного следствия.

Как известно, предварительное следствие оканчивается ознакомлением обвиняемого и его защитника с материалами дела, составлением и подписанием следователем обвинительного заключения и передачей уголовного дела прокурору для решения вопроса о его направлении в суд.

2. Правила оформления документации при осмотре техники

Процессуальный порядок реализации полномочий прокурора по уголовному делу, поступившему с обвинительным заключением, регламентирован ст. 221, 222 УПК РФ.

В соответствии со ст. 221 УПК РФ прокурор или его заместитель обязаны рассмотреть поступившее уголовное дело в срок, не превышающий десяти суток, и принять одно из следующих решений:

об утверждении обвинительного заключения и о направлении уголовного дела в суд; о возвращении уголовного дела следователю для производства дополнительного следствия, изменения объема обвинения либо квалификации действий обвиняемых или пересоставления обвинительного заключения и устранения выявленных недостатков со своими письменными указаниями; о направлении уголовного дела вышестоящему прокурору для утверждения обвинительного заключения, если оно подсудно вышестоящему суду.

Признав, что имеются основания для специальности дела в суд, прокурор на первой странице обвинительного заключения ставит свою подпись об утверждении обвинительного заключения. Для принятия такого решения прокурором по материалам уголовного дела должны быть установлены следующие обстоятельства:

- достаточность доказательств для рассмотрения дела в суде;
- возможность поддержания с имеющимися доказательствами государственного обвинения; относимость и допустимость собранных по делу доказательств;
- соответствие предъявленного обвинения собранным доказательствам;
- отсутствие обстоятельств, влекущих прекращение уголовного дела или уголовного преследования;
- отсутствие процессуальных нарушений, исключающих возможность рассмотрения дела в суде;
- соответствие обвинительного заключения требованиям закона.

Особое внимание прокурору при изучении дел о преступлениях в сфере компьютерной информации, поступивших для утверждения обвинительного заключения, следует обращать на предъявленное обвинение, которое должно полностью подтверждаться имеющимися в уголовном деле доказательствами, и содержать текст идентичный тексту постановления о привлечении в качестве обвиняемого.

Прокурор согласно п. 2 ч. 1 ст. 221 УПК РФ вправе вернуть уголовное дело следователю для производства дополнительного следствия, изменения объема обвинения либо квалификации действий обвиняемых или пересоставления обвинительного заключения и устранения выявленных недостатков со своими письменными указаниями. В настоящее время суд не имеет такого права, однако он может вернуть уголовное дело прокурору, при наличии оснований, предусмотренных ст. 237 УПК РФ, что, как правило, свидетельствует о ненадлежащем прокурорском надзоре за ходом предварительного следствия.

Хотя уголовно-процессуальным законом и предусмотрена возможность восполнения государственным обвинителем неполноты следствия, в том числе и путем предоставления

суду новых доказательств, изначально отталкиваться от такой возможности при наличии нарушений, допущенных следователем и выявленных на стадии утверждения обвинительного заключения, нецелесообразно, поскольку направлять в суд с утвержденным обвинительным заключением уголовное дело, имеющее заведомые недостатки, прокурор не имеет права.

Поэтому при выявлении прокурором обстоятельств, препятствующих рассмотрению уголовного дела судом, в том числе и неустановлении обстоятельств, подлежащих доказыванию, он обязан своим мотивированным постановлением возвратить уголовное дело следователю для дополнительного следствия, изменения объема обвинения либо квалификации действий обвиняемого или составления нового обвинительного заключения и устранения выявленных недостатков.

Таким образом, в условиях увеличения числа преступлений в сфере компьютерной информации возрастает и роль прокурорского надзора за исполнением законов при расследовании преступлений указанной категории. Надлежащая организация прокурорского надзора позволяет обеспечить защиту прав и законных интересов лиц и организаций, потерпевших от преступлений, и личности от незаконного и необоснованного обвинения, осуждения, ограничения ее прав и свобод, восстановить уже нарушенные права и предотвратить совершение новых преступлений.

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

- a. Изучить рекомендуемую литературу.
- b. Выполнить практическую работу.
- c. Ответить на контрольные вопросы.
- d. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выровнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчета приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Цели и задачи прокурорского надзора
2. Виды судебных экспертиз
3. Информационно-технологическая экспертиза
4. Процессуальный порядок реализации полномочий прокурора

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.
1. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной

деятельности».

2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».

4. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическое занятие № 7 Компьютерная криминалистика

Цель занятия: изучить существующие классификации компьютерных преступлений

1. Оперативность

Компьютерная преступность (преступление с использованием компьютера) – представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом, компьютерная информация является предметом или средством совершения преступления. Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга. В юридическом понятии, компьютерных преступлений, как преступлений специфических не существует. Виды компьютерных преступлений **Основные виды преступлений:**

Внедрение компьютерного вируса – процесс внедрения вредоносной программы с целью нарушения работы ПК. Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер. Вирус может проявлять себя в разных формах. Это могут быть замедления в выполнении программ; увеличение объёма программных файлов и наконец, эти проявления могут привести к стиранию файлов и уничтожению программного обеспечения.

Несанкционированный доступ к информации – может осуществляться с целью её хищения[прояснить](копирование на свой носитель и последующее блокирование доступа к информации) или же ради развлечения или[прояснить] последующего использования данной информации. Существуют множество способов осуществления несанкционированного доступа к системе, как правило, с использованием чужого имени; подбором паролей; изменением адресов устройств; использованием информации, оставшейся после решения задач; модификацией программного и информационного обеспечения, хищением носителей информации; установкой аппаратуры записи и т. д. **Подделка выходной информации** – подделка информации может преследовать различные цели. Итогом подделки является то, что конечному потребителю информации будут предоставлены недостоверные данные. Примером могут служить подтасовка результатов выборов или же хищение различного вида товаров, путем ввода в программу фальшивых данных; подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков; изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов.

Несанкционированное копирование конфиденциальной информации – в процессе работы каждой компании неизбежны случаи утечки конфиденциальной информации.

Несмотря на то, что защитные системы, отвечающие за хранение и доступ к внутренней информации, постоянно совершенствуются, проблема продолжает существовать. Организации несут огромные потери из-за несанкционированного распространения конфиденциальной информации. Несанкционированное копирование может осуществляться посредством изъятия средств компьютерной техники; перехвата информации; несанкционированного доступа к технике, а также манипуляции данными и управляющими командами.

2. Приоритетность расследования

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. Ниже приведены названия способов совершения подобных преступлений, соответствующих кодификатору Генерального Секретариата Интерпола. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен НЦБ более чем 100 стран[5].

Все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы Q. Для характеристики преступления могут использоваться до пяти

кодов, расположенных в порядке убывания значимости совершенного[6].

QA – Несанкционированный доступ и перехват QAN – компьютерный абордаж

QAI – перехват

QAT – кража времени

QAZ – прочие виды несанкционированного доступа и перехвата QD – Изменение компьютерных данных

QUL – логическая бомба QDT – троянский конь

QDV – компьютерный вирус 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 [7].

Кратко охарактеризуем некоторые виды компьютерных преступлений согласно приведенному кодификатору.

Согласно приведенному кодификатору кратко охарактеризую некоторые виды компьютерных преступлений.

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

QAN – "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 объектам непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup). Современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата[8].

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

1. "Жучок" (bugging) – характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала;

2. "Откачивание данных" (data leakage) – отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в

системе;

3. "Уборка мусора" (scavenging) – 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;

4. метод следования "За дураком" (piggybacking), характеризующий несанкционированное проникновение как в пространственные, так и электронные закрытые зоны. Его суть состоит в следующем. 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;

5. метод "За хвост" (between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе;

6. метод "Неспешного выбора" (browsing). В этом случае несанкционированный доступ 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;

7. метод "Поиск бреши" (trapdoor entry), при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;

8. метод "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[9];

9. метод "Маскарад" (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;

10. метод "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 коды пользователя.

QAT – кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты. 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 программу 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[10].

Процесс заражения компьютера программой-вирусом и его последующее лечение имеют ряд черт, свойственных медицинской практике. По крайней мере, эта терминология

весьма близка к медицинской:

резервирование – копирование FAT, ежедневное ведение архивов измененных файлов – это самый важный и основной метод защиты от вирусов. Остальные методы не могут заменить ежедневного архивирования, хотя и повышают общий уровень защиты;

профилактика – раздельное хранение вновь полученных и уже эксплуатируемых программ, разбиение дисков на "непотопляемые отсеки" – зоны с установленным режимом "только для чтения", хранение неиспользуемых программ в архивах, использование специальной "инкубационной" зоны для записи новых программ с дискет, систематическая проверка BOOT-сектора используемых дискет и др.;

анализ – ревизия вновь полученных программ специальными средствами и их запуск в контролируемой среде, систематическое использование контрольных сумм при хранении и передаче программ. Каждая новая программа, полученная без контрольных сумм, должна тщательно проверяться компетентными специалистами по меньшей мере на известные виды компьютерных вирусов и в течение определенного времени за ней должно быть организовано наблюдение;

фильтрация – использование резидентных программ типа FluShot Plus, MaceVaccine и других для обнаружения попыток выполнить несанкционированные действия;

вакцинирование – специальная обработка файлов, дисков, каталогов, запуск специальных резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса, для определения заражения программы или всего диска;

терапия – деактивация конкретного вируса в отраженных программах с помощью специальной антивирусной программы или восстановление первоначального состояния программ путем уничтожения всех экземпляров вируса в каждом из зараженных файлов или дисков с помощью программы-фага [11].

Понятно, что избавиться от компьютерного вируса гораздо сложнее, чем обеспечить действенные меры по его профилактике.

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 (карточек и пр.).

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% всех 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 [12].

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 преступлений:

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 законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества; QZS – использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера.

Некоторые специалисты по компьютерной преступности в особую группу выделяют методы манипуляции, которые имеют специфические жаргонные названия [13].

"Временная бомба" – разновидность логической бомбы, которая срабатывает при достижении определенного момента времени;

"Асинхронная атака" (asynchronous attack) состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей.

"Моделирование" (simulation modelling) используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления. Таким образом, осуществляется "оптимизация" способа совершения преступления

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Изучить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выровнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчета приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Компьютерная преступность
2. Основные виды преступлений
3. Внедрение компьютерного вируса

4. Несанкционированный доступ к информации
5. Подделка выходной информации
6. Несанкционированное копирование конфиденциальной информации

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.
6. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
7. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
9. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическое занятие № 8. Компьютерная криминалистика

Цель занятия: изучить существующие классификации компьютерных преступлений

1. Онлайн-мошенничество.

Рассмотрим некоторые приемы, применяемые в компьютерных преступлениях.

Способ, не требующий специфических знаний в области информационных технологий, заключается в том, что путем хищения, разбоя, вымогательства изымаются системные блоки или отдельные носители информации, содержащие важную информацию. Как правило, такие действия квалифицируются как «некомпьютерные» преступления. Используя средства аудио-, видео- и электромагнитного наблюдения злоумышленники могут получать доступ к важной информации либо к учетным записям пользователей, для последующего несанкционированного доступа. Объектами таких атак становятся линии связи и телекоммуникационное оборудование.

Используется для вывода из строя системы, например, с помощью одновременных множественных запросов к оборудованию. Используется либо для создания условий, при которых «вражеский» ресурс перестанет быть доступен, либо для создания аварийной ситуации, позволяющей перейти к несанкционированному доступу.

В этом случае злоумышленники, используя различные способы (вирусы, перебор паролей, ошибки в программном обеспечении, ошибки в настройках сетевых служб и т.п.), получают доступ к информации, не предназначенной для публичного использования.

Важнейшим и определяющим элементом криминалистической характеристики любого, в том числе и компьютерного, преступления является совокупность данных, характеризующих способ его совершения.

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 классифицируются на пять основных групп. При этом в качестве основного классифицирующего признака выступает метод использования преступником тех или иных действий, направленных на получение доступа к средствам компьютерной техники. Руководствуясь этим признаком, выделяются следующие общие группы:

- ~ изъятие средств компьютерной техники (СКТ);
- ~ перехват информации;
- ~ несанкционированный доступ к СКТ;
- ~ манипуляция данными и управляющими командами; комплексные методы.

К первой группе нами относятся традиционные способы совершения обычных видов («некомпьютерных») 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, широко практикуемых в оперативно-розыскной деятельности правоохранительных органов.

Непосредственный 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.

Электромагнитный (пассивный) перехват основан на фиксации электромагнитных излучений, возникающих при функционировании многих средств компьютерной техники, включая и средства коммуникации. Волны, излучаемые электронно-лучевой трубкой дисплея, несущие в себе определенную информацию с помощью специальных приборов можно принимать на расстоянии до 1000 м.

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

Видеоперехват заключается в действиях преступника, направленных на получение информации путем использования различной видеооптической техники.

“Уборка мусора” представляет собой неправомерное использование преступником технологических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой. Например, даже удаленная из памяти компьютера информация, подлежит быстрому восстановлению и несанкционированному изъятию с помощью специальных программных средств.

К третьей группе способов совершения компьютерных преступлений относятся действия преступника, направленные на получение несанкционированного доступа к средствам компьютерной техники. К ним относятся нижеследующие.

“За дураком”. 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.

“За хвост”. 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.

“Компьютерный абордаж”, по существу являющийся подготовительной стадией компьютерного преступления.

Данный способ совершения компьютерного преступления осуществляется преступником путем случайного перебора абонентного номера компьютерной системы с использованием модемного устройства. Иногда для этих целей используется специально созданная самодельная, либо заводская программа автоматического поиска пароля. Алгоритм ее работы заключается в том, чтобы используя быстроедействие современных компьютерных устройств, перебирать все возможные варианты комбинаций букв, цифр и специальных символов, и в случае совпадения комбинации символов производить автоматическое соединение указанных абонентов.

Используя одну из таких программ, провели эксперимент по подбору пароля путем простого перебора. В результате было установлено, что 6-ти символьные пароли подбираются примерно за 6-дневной непрерывной работы компьютера. Элементарный подсчет показывает, что уже для подбора 7-ми символьных паролей потребуется от 150 дней для английского языка до 200 дней для русского. А если есть буквы заглавные, то эти цифры надо умножить еще на 2. Таким образом, простой перебор представляется чрезвычайно трудновыполнимым.

Исходя из этого, 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.

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

Этот способ чрезвычайно распространен среди так называемых 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 взламывающих программ, вирусов, вопросов их создания и распространения.

“Брешь”. В отличие от “неспешного выбора”, когда производится поиск уязвимых мест в защите компьютерной системы, при данном способе преступником осуществляется их конкретизация: определяются участки, имеющие ошибку или неудачную логику программного строения. Выявленные таким образом “бреши” могут использоваться преступником многократно, пока не будут обнаружены.

“Люк”. Данный способ является логическим продолжением предыдущего. В этом случае в найденной “бреши” программа “разрывается” и туда дополнительно преступник вводит одну или несколько команд. Такой “люк” “открывается” по необходимости, а включенные команды автоматически выполняются.

Необходимо заметить, что подобный “черный вход” в якобы защищенную систему имеется в любой сертифицированной государством программе, но об этом не принято распространяться вслух.

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 экономическими преступлениями.

Наиболее широко используются следующие способы совершения компьютерных преступлений, относящихся к этой группе.

Подмена данных - наиболее простой и поэтому очень часто применяемый способ совершения преступления. Действия преступников в этом случае направлены на изменение или введение новых данных, которые осуществляются, как правило, при вводевыводе информации.

“Троянский конь”. Данный способ заключается в тайном введении в чужое программное обеспечение специально созданных программ, которые, попадая в информационно- вычислительные системы, начинают выполнять новые, не планировавшиеся законным владельцем программы, с одновременным сохранением прежней ее работоспособности.

В соответствии со ст. 273 Уголовного кодекса Российской Федерации под такой программой понимается “программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети”.

По существу, “троянский конь” - это модернизация уже рассмотренного нами способа “люк” с той лишь разницей, что он “открывается” не при помощи непосредственных действий самого преступника (“вручную”), а автоматически - с использованием специально подготовленной для этих целей программы без дальнейшего непосредственного участия самого преступника.

С помощью данного способа преступники обычно отчисляют на заранее открытый счет определенную сумму с каждой операции. Возможен здесь и вариант увеличения преступниками избыточных сумм на счетах при автоматическом пересчете рублевых остатков, связанных с переходом к коммерческому курсу соответствующей валюты. Разновидностями такого способа совершения компьютерных преступлений является

внедрение в программы “логических” и “временных бомб”, разнообразных компьютерных вирусов.

С уголовно-правовой точки зрения, согласно ст. 273 Уголовного кодекса РФ, под компьютерным вирусом следует понимать вредоносную программу для ЭВМ, способную самопроизвольно присоединяться к другим программам (“заражать” их) и при запуске последних выполнять различные нежелательные действия: порчу файлов, искажение, стирание данных и информации, переполнение машинной памяти и создание помех в работе ЭВМ.

Копирование (тиражирование) программ с преодолением программных средств защиты. Этот способ предусматривает незаконное создание копии ключевой дискеты, модификацию кода системы защиты, моделирование обращения к ключевой дискете, снятие системы защиты из памяти ЭВМ и т.п.

Не секрет, что подавляющая часть программного обеспечения, используемого в России, является пиратскими копиями взломанных хакерами программ. Самой популярной операционной системой в России является Microsoft Windows'95. По статистике, на долю этой платформы приходится свыше 77 процентов отечественного рынка операционных систем. Своим бесспорным успехом на российском рынке Windows'95 обязана деятельности компьютерных пиратов. По данным антипиратской организации BSA, свыше 90 процентов используемых в России программ установлены на компьютеры без лицензий, тогда как в США не более 24 процентов.

Можно привести в качестве примера и широко известную отечественную программу “Консультант-плюс” содержащую периодически обновляемую компьютерную базу российского законодательства. Несмотря на постоянную работу программистов фирмы по улучшению систем защиты, тысячи нелегальных копий взломанной программы имеют хождение на территории страны. Последняя уже шестая версия “Консультанта” была “привязана” к дате создания компьютера, записанной в его постоянной памяти. Не прошло и двух недель после выхода этой версии, как хакерами была создана программа, эмулирующая нужную дату на любой ЭВМ. Теперь любой желающий может найти такую программу в компьютерных сетях и бесплатно установить на свой компьютер базу данных стоимостью более 1000\$ США.

Успехи хакеров настолько велики, что, например, США намерены использовать их в информационной войне.

С момента официального признания в 1993 году военно-политическим руководством США “информационной войны” в качестве одной из составляющих национальной военной стратегии, ускоренными темпами идут поиски методов, форм и средств ее ведения. Так, в последние годы все чаще говорят о целесообразности привлечения хакеров на различных стадиях “информационной войны”. 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. Кроме того, обозначенная видимость законного пользователя дает возможность хакеру-разведчику сформировать ложную систему и ввести ее в сеть противника в качестве законного пользователя информации.

Не менее эффективным может являться применение опыта хакеров в электронной войне при решении задач дезинформирования и пропаганды через информационные системы и сети противника. Для хакеров не составляет проблемы манипулирование данными, находящимися в базах данных противника. Им также не трудно лишить противника возможности доступа к информационным ресурсам, использование которых входило в его планы. Для этого могут использоваться способы загрузки систем большим количеством сообщений, передаваемых по

электронной почте, или заражение систем противника компьютерными вирусами.

По сообщениям зарубежных СМИ, проблема использования хакеров в интересах информационной войны в настоящее время не только ограничивается изучением их опыта, но и реализуется на практике. Спецслужбы США и некоторых европейских стран уже прибегают к услугам этой категории компьютерщиков.

2. Клевета, оскорбления и экстремистские действия в Сети

Меры предупреждения компьютерных преступлений можно разделить на три группы: правовые, организационные и технические.

К **правовым мерам** необходимо отнести разработку законодательных актов, устанавливающих ответственность за преступления, разработку норм, защищающих авторские права. Отсутствие таких актов и норм дает возможность злоумышленникам пользоваться несовершенством законодательства и избегать ответственности за совершенные преступления.

Вступлением в силу Уголовного кодекса РФ отечественное уголовное законодательство приведено в соответствие с общепринятыми международными правовыми нормами развитых в этом отношении зарубежных стран. Теперь очередь за принятием нового уголовно- процессуального законодательства, регламентирующего все возможные следственные действия и механизм их осуществления применительно к специфике компьютерных преступлений.

Проблемы, затрудняющие предупреждение и расследование компьютерных преступлений, включают в себя:

выявившееся несовершенство УК (состав преступлений ст.ст.272, 274 - материальный (требует наличие перечисленных в законе общественно опасных последствий);

дефицит специалистов в МВД;

отсутствие наработок (методических рекомендаций по изъятию, обыску, осмотру места происшествия и т.п.);

несовершенство УПК (в частности неясно, как принимать в качестве доказательства электронный документ) и некоторые другие проблемы.

Организационные меры включают в себя подборку и проверку персонала, работающего с информацией, доступ к которой необходимо ограничивать. Наличие прав работы с информацией у людей с сомнительным прошлым или относящихся к работе небрежно может привести к утечкам данных на сторону.

Необходим инструктаж сотрудников о хранении и правилах работы с данными, а также о правилах создания, смены и хранения паролей доступа. В качестве примера можно привести случай, когда при анализе уязвимостей в одной из фирм было выявлено, что сотрудники хранили пароли на листочках, приклеенных к мониторам. И такие случаи далеко не единичны. Небрежное хранение паролей, а также «легкие» пароли (например, 12345, god и т.п.), дают злоумышленникам шансы на проникновение в систему. В некоторых случаях на предприятиях составляются детальные планы по спасению либо надежному уничтожению информации в аварийных ситуациях (пожар, теракт). Кроме того, предприятия часто не указывают в договоре с сотрудником пункт о неразглашении коммерческой и служебной тайн. Это позволяет недобросовестному сотруднику чувствовать себя в относительной безопасности. Наличие такого пункта в договоре и соответствующие инструкции на рабочем месте дисциплинирует сотрудников, заставляя их более внимательно обращаться с вверенной им информацией. Отсутствие лица, отвечающего за информационную безопасность на предприятии и бесконтрольность действий сотрудников, также повышает вероятность проникновения в систему постороннего лица и утечки данных.

Всегда надо помнить, что большинство взломов, утечек и успешных атак проводится не благодаря высокому профессиональному уровню атакующего, а в результате безалаберности и безграмотности пользователей.

Технические меры делятся на две группы: аппаратные и программные.

Аппаратные меры включают в себя наличие технических устройств, обеспечивающих защиту. Например, таких как:

- источники бесперебойного питания, предохраняющие от скачкообразных перепадов или снятия напряжения;
- устройства экранирования аппаратуры и линий проводной связи;
- устройства защиты телефонии от прослушивания;
- устройства, санкционирующее физический доступ пользователя на охраняемые объекты (шифрозамки, биометрические устройства идентификации личности и т.п.);
- средства охранно-пожарной сигнализации;

Также проникновение в систему может произойти с помощью программ, принесенных на мобильных носителях информации, таких как flash-память, cd- и dvd-диски и т.п. В некоторых случаях стоит ограничивать техническую возможность использования таких носителей информации.

Набор *программных средств* обеспечения безопасности компьютерных систем в настоящий момент очень широк. В первую очередь надо отметить встроенные средства операционной системы, позволяющие разделять права пользователей, работающих за компьютером. При этом важно понимать, что каждое повышение привилегий ведет за собой увеличение вероятности проникновения в систему. Следовательно, не стоит давать пользователям прав, более чем необходимо для конкретных работ.

Следующая мера программного характера – это антивирусная защита, позволяющая обезопасить компьютеры от вредоносного программного обеспечения. Современные антивирусные программы предоставляют собой достаточно высокую степень защиты как от известных вирусов, так и от новых, за счет алгоритмов, умеющих распознавать нежелательные действия.

При работе с глобальными сетями есть вероятность проведения атаки с удаленных компьютеров на компьютеры и серверы предприятия и частных лиц. Для повышения защищенности в этом случае используют специальные программы-фильтры, позволяющие блокировать нежелательный трафик (поток данных). Такие программы получили название межсетевой экран, файрвол (**firewall**) или брандмауэр (Brandmauer). В современных операционных системах, как правило, уже имеется встроенный брандмауэр с возможностью обучения для нужд пользователя.

Кроме мер активного противодействия атакам, необходимо использовать средства протоколирования и наблюдения. Первые позволяют вести так называемые логи (logs), куда записываются все действия пользователей и сообщения различных служб компьютера. Впоследствии такие записи позволяют анализировать и выявлять действия злоумышленников.

Средства наблюдения за сетью дают возможность просматривать и контролировать трафик, на предмет излишней активности или подозрительных операций. Такие программы называются мониторами. Кроме того, есть специальные программы-сканеры для выявления узких мест и уязвимостей в системе.

Еще один способ защиты информации – шифрование данных. Шифрование может использоваться при передаче данных по линиям связи либо при хранении данных.

Оборудование и материалы:

—

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выровнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчета приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

3. Способы совершения компьютерных преступлений.
4. Что понимается под способом совершения преступления
5. Что понимается под непосредственным активным перхватом
6. Что понимается под аудиоперехватом
7. Что понимается под видеоперехватом
- 6 Меры предупреждения компьютерных преступлений

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. –476.
6. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
7. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
9. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическое занятие № 9 Компьютерная криминалистика

1. DoS-атаки

Непосредственный перехват - 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.

Электромагнитный перехват. Перехват информации осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Может осуществляться преступником, находящимся на достаточном удалении от объекта перехвата.

2. Вредоносные программы

Эти методы в профессиональной среде получили следующие специфические названия. **Метод следования "За дураком"**. Имеет целью несанкционированное проникновение в пространственные и электронные закрытые зоны. Его суть состоит в следующем. 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.

Метод "За хвост". Используя этот метод, можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе.

Метод "Компьютерный абордаж". Обычно используется для проникновения в чужие информационные сети. Злоумышленник пытается с помощью автоматического перебора абонентских номеров соединиться с тем или иным компьютером, подключенным к телефонной сети. Делается это до тех пор, пока на другом конце линии не отзовется другой компьютер. После этого достаточно подключить собственный компьютер. Угадав код можно внедриться в чужую информационную систему.

Метод "Неспешного выбора". В этом случае несанкционированный доступ 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.

Метод "Поиск бреши". Данный метод основан на использовании ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно. **Метод "Люк"** является развитием предыдущего. В найденной "бреши" программа "разрывается" и туда вставляется необходимое число команд. По мере необходимости "люк" открывается, а встроенные команды автоматически осуществляют свою задачу.

Метод "Маскарад". В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя.

Метод "Мистификация". 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 коды пользователя. **Метод "Аварийный"**. Этот прием основан на использовании того обстоятельства, что в любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ. Такая программа - мощный и опасный инструмент в руках злоумышленника.

Метод "Склад без стен". Несанкционированный доступ осуществляется в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он

может получить доступ к не принадлежащим ему частям банка данных.

Особую опасность представляет несанкционированный доступ в компьютерные системы финансовых учреждений с целью хищения финансовых средств. Рассмотрим некоторые типичные примеры.

Пример.

По оценкам отечественных специалистов, уже сейчас хищения с применением компьютерной техники и средств электронного платежа представляют серьезную угрозу для безопасности России. В ближайшем будущем прогнозируется значительный рост преступности в данной сфере и увеличение ее доли в общем количестве преступлений.

Практическое занятие № 10 Компьютерная криминалистика

1. Кардерство

Сущность методов манипуляции состоит в подмене данных, которая осуществляется, как правило, при вводе-выводе данных. Это простейший и потому очень часто применяемый способ.

Пример.

Вариантом подмены данных является подмена кода. Рассмотрим некоторые конкретные методы:

Манипуляция с пультом управления. Манипуляция с пультом управления относится к злоупотреблению механическими элементами управления ЭВМ. Характеристика манипуляции с вычислительной техникой заключается в том, что в результате механического воздействия на технические средства машины создаются возможности манипуляции данными.

Пример.

Некоторые из таких нарушений связаны с компьютерами телефонных сетей.

Пример.

"Троянский конь" - способ, состоящий в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность;

Пример.

Действия такого рода часто совершаются сотрудниками, которые стремятся отомстить за несправедливое, по их мнению, отношение к себе либо оказать воздействие на администрацию предприятия с корыстной целью.

Пример.

"Логическая бомба" - тайное встраивание в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

"Временная бомба" - разновидность логической бомбы, которая срабатывает при достижении определенного момента времени.

"Асинхронная атака" состоит в смешивании команд двух или нескольких пользователей, чьи команды компьютерная система выполняет одновременно.

Моделирование используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления.

Реверсивная модель. Сущность метода заключается в следующем. Создается модель конкретной системы. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем, исходя из полученных правильных результатов, подбираются правдоподобные желательные результаты. Затем модель прогоняется назад, к исходной точке, и становится ясно, какие манипуляции с входными данными нужно проводить. В принципе, прокручивание модели "вперед-назад" может проходить не один раз, чтобы через несколько итераций добиться желаемого. После этого остается только осуществить задуманное.

Пример.

"Воздушный змей". В простейшем случае требуется открыть в двух банках по

небольшому счету. Далее, деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так, чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз до тех пор, пока на счете не оказывается приличная сумма (фактически, она постоянно "перескакивает" с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются и владелец счетов скрывается. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике, в такую игру включают большое число банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

Пример.

Манипулирование данными осуществляется также и самими руководителями коммерческих структур с целью нанесения ущерба государству.

Пример.

Как правило, компьютерные преступления совершаются с помощью различных комбинаций вышеописанных способов.

Использование компьютера при совершении преступлений

В зависимости от способа использования компьютера при совершении преступлений Марк Экенвайлер выделяет три основные категории:

Компьютер является объектом правонарушения, когда цель преступника - похитить информацию или нанести вред интересующей его системе.

Компьютеры используются как средства, способствующие совершению такого преступления как, например, попытка преодоления защиты системы (атака), или более традиционного преступления (например, мошенничества), совершаемого с помощью электронных средств. Компьютер используется как запоминающее устройство.

При совершении ряда преступлений могут иметь место все три способа использования компьютера.

Рассмотрим каждый из видов более подробно.

1. Компьютер как объект преступления. Можно выделить две разновидности преступлений, где компьютер является объектом посяательства:

а) Изъятие средств компьютерной техники. К этой группе относятся традиционные способы совершения обычных видов преступлений, в которых действия преступника направлены на изъятие чужого имущества.

Пример.

б) Атака на компьютер с целью несанкционированного доступа в целях получения доступа к хранящейся на нем информации (хищения информации), бесплатного использования данной системы (кража услуг) или ее повреждения.

Большинство таких нарушений предполагают несанкционированный доступ к системе, т.е. ее "взлом". В общем виде используемые компьютерными преступниками методики несанкционированного доступа сводится к двум разновидностям:

"Взлом" изнутри: преступник имеет физический доступ к терминалу, с которого доступна интересующая его информация и может определенное время работать на нем без постороннего контроля.

"Взлом" извне: преступник не имеет непосредственного доступа к компьютерной системе, но имеет возможность каким-либо способом (обычно посредством удаленного доступа через сети) проникнуть в защищенную систему для внедрения специальных программ, произведения манипуляций с обрабатываемой или хранящейся в системе информацией, или осуществления других противозаконных действий.

В данной категории преступлений выделяют также:

а) преступления, совершаемые в отношении компьютерной информации, находящейся

в компьютерных сетях, в том числе сети Интернет;

б) преступления, совершаемые в отношении компьютерной информации, находящейся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (пейджер, сотовый телефон, кассовый аппарат и т.п.).

Отмечается тенденция к переходу от разовых преступлений по проникновению в системы со своих или соседних рабочих мест к совершению сетевых компьютерных преступлений путем "взлома" защитных систем организаций.

Хищение информации. Правонарушения, связанные с хищением информации, могут принимать различные формы в зависимости от характера системы, в отношении которой осуществляется несанкционированный доступ. Информация, являющаяся объектом преступного посягательства, может быть отнесена к одному из четырех типов:

- персональные данные;
- корпоративная информация, составляющая коммерческую тайну;
- объекты интеллектуальной собственности и материалы, защищенные авторским правом;

- глобальная информация, имеющая значение для развития отраслей промышленности, экономики отдельных регионов и государств.

Похищаются сведения об новейших научно-технических разработках, планах компании по маркетингу своей продукции и заключаемых сделках.

Пример.

Типичным злоупотреблением, посягающим на объекты авторских прав, являются преступления, связанные с несанкционированным размножением компьютерных программ. Предметом хищения может быть также другая экономически важная информация, в частности, реквизиты банковских счетов и номера кредитных карточек.

Пример.

Можно выделить два основных специальности действий преступников:

- электронная атака на узловые серверы и броузеры сети WWW в целях перехвата информационных потоков;

- поиск в защитных системах локальных компьютерных сетей уязвимых места и проникновение в базы данных с целью съема находящейся в них информации.

Хищение услуг. К данной группе правонарушений относится получение несанкционированного доступа к какой-то системе, чтобы бесплатно воспользоваться предоставляемыми ею услугами.

Примером преступления данной категории является фрун-фрейкинг - использование компьютера для проникновения в коммутационную телефонную систему с целью незаконного пользования услугами по предоставлению междугородной телефонной связи. Сюда же можно отнести использование ресурсов систем - объектов несанкционированного доступа для решения задач, требующих сложных расчетов, например, для определения закодированных паролей, которые они похищают с других узлов.

Уивинг - одно из наиболее распространенных преступлений этого вида, связанное с кражей услуг, происходит в процессе "запутывания следов". Злоумышленник проходит через многочисленные системы и многочисленные телекоммуникационные сети - Интернет, системы сотовой и наземной телефонной связи, чтобы скрыть свое подлинное имя и местонахождение. При такой ситуации причиной проникновения в данный компьютер является намерение использовать его как средство для атаки на другие системы. Повреждение системы. Данная группа объединяет преступления, совершаемых с целью разрушить или изменить данные, являющиеся важными для владельца или одного или многих пользователей системы - объекта несанкционированного доступа. Данная деятельность осуществляется по двум основным специальностям:

- проводится массированная подача электронных сигналов на серверы WWW и локальных сетей в целях вывода их из строя, для чего используются специально разработанные программы.

- в базы данных ЭВМ и корпоративных сетей вводятся вирусы-роботы, которые в заданный момент искажают или уничтожают компьютерные файлы.
- манипуляции данными.

Объектом подобных атак могут стать компьютеры, соединенные с Интернетом. Маршрутизаторы - компьютеры, определяющие путь, по которому пакеты информации перемещаются по Интернету - аналогичны телефонным коммутаторам и поэтому являются объектами для опытных хакеров, которые хотят нарушить или даже изменить маршрут "трафика" в сети.

Использование вирусов. Применение данного средства повреждения компьютерных систем доступно в настоящее время не только профессиональным программистам, но и людям, обладающим лишь поверхностными познаниями в этой сфере. Во многом это обусловлено доступностью самих вредоносных программ и наличием простой технологии их создания. Непредставляет сложности купить CD-диски с программами взлома систем защиты компьютерных сетей, а также CD-диски с пакетами вирусов, которые можно использовать для заражения средств вычислительной техники. Также продается специальная программа конструктор для генерации вирусов. С ее помощью даже не специалист может создать штамм вируса из готовых стандартных составных частей различных вредоносных программ. Причем каждый новый вирус, сгенерированный программой-конструктором, не определяется

антивирусом, пока его копия не попадет к авторам антивирусных программ. Таким образом, в пользование различных лиц свободно попадают вирусные программы, а также программы-конструкторы по их созданию, что может привести к тяжелым последствиям.

2. Посреднические онлайн-сервисы. Почему мошенничество?

3. Компьютер как орудие преступления. Компьютеры могут использоваться в качестве орудия незаконных действий двояким способом:

- а) как средство совершения традиционных преступлений (различного рода мошенничества ит.п.);
- б) как средство атаки на другой компьютер.

Рассмотрим особенности этих способов использования компьютера в преступных целях. Компьютер как орудие совершения обычных преступлений. Значительная часть преступлений данной категории совершается с использованием Интернет. К ним относятся: мошенничество с предоплатой; пирамиды и письма по цепочке; виртуальные финансовые пирамиды; азартные игры он-лайн; распространение порнографических материалов и ряд других.

Компьютер как средство атаки на другие компьютеры. В некоторых случаях компьютер может одновременно являться объектом несанкционированного доступа и средством атаки. Однако в большинстве случаев атаки на компьютеры совершаются с других компьютеров, находящихся в той же сети. Поскольку такие сети - состоят из сотен или тысяч узлов на многих континентах, соответственно существует больше возможностей для несанкционированного доступа или других нарушений.

Существует две основных категории дистанционных нарушений: несанкционированный доступ и отказ в обслуживании.

При нарушении с несанкционированным доступом преступник пытается воспользоваться пробелами в области обеспечения безопасности системы в качестве средства для получения доступа к самой системе. Если ему это удастся, он может похитить или уничтожить информацию или использовать поврежденную систему в качестве платформы, с которой он сможет совершить нарушения в отношении других машин. Значительной опасностью характеризуются подобные злоупотребления в Интернет.

При нарушении, влекущем за собой отказ в предоставлении обслуживания, цель преступника состоит в выведении из строя данной системы. При этом преступник не обязательно стремится получить к ней доступ. Наибольшее распространение получили подобные нарушения в сети Интернет.

4. Компьютер как запоминающее устройство. В данной своей функции компьютер играет в преступной деятельности роль пассивного запоминающего устройства. Часто при этом компьютер является объектом несанкционированного доступа.

Например, после взлома системы создается специальная директория для хранения файлов, содержащих программные средства преступника, пароли для других узлов, списки украденных номеров кредитных карточек. Возможности подобного использования компьютера в преступных целях многократно возрастают при использовании сети Интернет. Таблица, составленная по результатам опроса представителей служб безопасности 492 компаний, дает представление о наиболее опасных способах совершения компьютерных преступлений.

Наивысшая угроза	
Виды атак, выявленные за последние 12 месяцев	
Вирус	83%
Злоупотребление сотрудниками компании доступом к Internet	69%
Кража мобильных компьютеров	58%
Неавторизованный доступ со стороны сотрудников компании	40%
Мошенничество при передаче средствами телекоммуникаций	27%
Кража внутренней информации	21%
Проникновение в систему	20%
Допускалось несколько вариантов ответов.	

Оборудование и материалы:

—

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Изучить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выровнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчета приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1

– Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Непосредственный перехват
2. Электромагнитный перехват
3. Способы совершения компьютерных преступлений методом несанкционированного доступа
4. Способы совершения компьютерных преступлений методом манипуляции

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
4. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.
5. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
6. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
8. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическое занятие № 11 Компьютерная криминалистика

Цель занятия: изучить существующие классификации компьютерных преступлений

1. Мошенничество с трафиком

По ст. 272 УК ответственность за деяние наступает: если неправомерный доступ к компьютерной информации повлек за собой хотя бы одно из следующих негативных последствий: уничтожение, блокирование, модификацию либо копирование компьютерной информации

Информация и информационные правоотношения все чаще становятся новым предметом преступного посягательства.

При расследовании неправомерного доступа к компьютерной информации обстоятельства содеянного устанавливаются в такой очередности:

- 1) факт неправомерного доступа к информации в компьютерной системе или сети;
- 2) место несанкционированного проникновения в эту систему или сеть;
- 3) время совершения преступления;
- 4) способ несанкционированного доступа;
- 5) степень надежности средств защиты компьютерной информации;
- 6) лица, совершившие неправомерный доступ, их виновность и мотивы преступления;
- 7) вредные последствия содеянного;
- 8) выявление обстоятельств, способствовавших преступлению.

Для рассматриваемых преступлений характерны такие ситуации начала расследования:

- 1) Собственник компьютерной системы обнаружил нарушение ее целостности и (или) конфиденциальности, установил виновное лицо и заявил о случившемся в правоохранительные органы.
- 2) Собственник самостоятельно выявил названные нарушения, однако не смог установить злоумышленника и заявил о случившемся.
- 3) Сведения о нарушении целостности и (или) конфиденциальности информации и виновном субъекте стали известны или непосредственно обнаружены компетентным органом, владелец компьютерной системы этот факт скрывает.
- 4) Правоохранительным органом обнаружены признаки противоправного вторжения в компьютерную систему, виновное лицо и владелец информации неизвестны.

Факт неправомерного доступа к информации обнаруживают, как правило, пользователи компьютерной системы или сети. Такие факты иногда устанавливаются в ходе оперативно-розыскной деятельности органов внутренних дел, ФСБ, ФСНП России. Их можно выявить и в ходе прокурорских проверок, ревизий, судебных экспертиз, следственных действий по расследуемым делам.

2. Нарушение авторских прав в офлайне

Признаками несанкционированного доступа или подготовки к нему могут служить:

- а) появление в компьютере искаженных данных - является следствием воздействия специальных программ, использованных для преодоления систем защиты, либо преднамеренного искажения файлов, к которым и был осуществлён неправомерный доступ;
- б) длительное необновление кодов, паролей и других защитных средств компьютерной системы - указывает на то, что преступником может являться лицо, официально работающее с данной системой, поскольку другим лицам сложно осуществить несанкционированное управление системой без привлечения к себе внимания пользователей и обслуживающего персонала системы;
- в) увеличение числа сбоев в работе ЭВМ - указывает на использование специальных программ, для преодоления системы защиты, изменения или копирования информации; г)

участившиеся жалобы пользователей компьютерной системы или сети. Таким фактам могут предшествовать или сопутствовать:

- 1) осуществление без необходимости сверхурочных работ;
- 2) немотивированные отказы отдельных сотрудников, обслуживающих компьютерную систему или сеть, от очередного отпуска;
- 3) приобретение работником для личного пользования дорогостоящего компьютера;
- 4) чистые дискеты или диски, принесенные на работу кем-то из сотрудников компьютерной системы под предлогом копирования программ для компьютерных игр;
- 5) участившиеся случаи перезаписи отдельных данных без серьезных на то причин;
- 6) необоснованный интерес некоторых работников к содержанию чужих принтерных распечаток;
- 7) повторный ввод в компьютер одной и той же информации и др.

Необходимо выяснить также признаки неправомерного доступа, выражающиеся в отступлениях от установленного порядка обработки документов. Имеются в виду:

- а) нарушения принятых правил оформления документов и изготовления машинограмм;
- б) лишние документы, подготовленные для обработки на ЭВМ;
- в) несоответствие информации, содержащейся в первичных документах, данным машинограмм;
- г) преднамеренные утрата или уничтожение первичных документов и машинных носителей информации, внесение искажений в данные их регистрации. Следует, однако, помнить, что перечисленные признаки могут быть результатом не только злоупотреблений, но и других причин, например халатности персонала, случайных ошибок и сбоев компьютерной техники. Место несанкционированного проникновения в компьютерную систему или сеть удается установить с определенными трудностями, поскольку таких мест может быть несколько. На практике чаще обнаруживается место неправомерного доступа к компьютерной информации с целью хищения денежных средств, но для этого также приходится выявлять все места работы компьютеров, имеющих единую телекоммуникационную связь.

Гораздо проще это место устанавливается тогда, когда расследуется несанкционированный доступ к единичному компьютеру. Обыкновенно доступ имеют ограниченное количество лиц. Также проще определить способ доступа к информации. Но и тут нужно учитывать, что информация на машинных носителях может храниться в других помещениях.

Во много раз труднее определить место непосредственного применения технических средств удаленного несанкционированного доступа, которые не входят в данную компьютерную систему или сеть. Это может быть как элементарное видеонаблюдение, так и считывание электромагнитных излучений компьютера и его элементов. Излучение можно считывать даже с клавиатуры, во время набора текста, в том числе и паролей и кодов. К установлению подобного доступа необходимо привлекать соответствующих специалистов. Необходимо выяснить также место хранения информации на машинных носителях, добытой преступником в результате неправомерного доступа к компьютерной системе или сети.

Время несанкционированного доступа можно определить с помощью программ общесистемного назначения. В работающем компьютере они обычно фиксируют текущее время. Если данная программа функционирует, то при несанкционированном входе в систему или сеть время работы на компьютере любого пользователя и производства конкретной операции автоматически фиксируется в оперативной памяти. Тогда время несанкционированного доступа можно определить в ходе следственного осмотра компьютера, его распечаток или дискет, производимого с участием специалиста, чтобы информация, находящаяся в оперативной памяти ЭВМ или на дискете, не была случайно стерта. В качестве специалистов могут выступать, например, сотрудники информационных центров МВД, ГУВД, УВД субъектов Российской Федерации. Время несанкционированного доступа

устанавливается и путем допроса свидетелей из числа сотрудников данной компьютерной системы. Выясняется, когда именно каждый из них работал на ЭВМ, если это не было зафиксировано в автоматическом режиме.

Способы преступных манипуляций в сфере компьютерной информации

Способы преступных манипуляций в сфере компьютерной информации могут быть разделены на две большие группы. Первая группа осуществляется без использования компьютерных устройств в качестве инструмента для проникновения извне в информационные системы или воздействия на них. Это могут быть: хищение машинных носителей информации в виде блоков и элементов ЭВМ; использование визуальных, оптических и акустических средств наблюдения за ЭВМ; считывание и расшифровка различных электромагнитных излучений компьютера и обеспечивающих систем; фотографирование информации в процессе ее обработки; изготовление бумажных дубликатов входных и выходных документов, копирование распечаток; использование оптических и акустических средств наблюдения за лицами, имеющими отношение к необходимой злоумышленнику информации, фиксация их разговоров; осмотр и изучение не полностью утилизированных отходов деятельности компьютерных систем; вступление в прямой контакт с лицами, имеющими отношение к необходимой злоумышленнику информации, получение от них под разными предлогами нужных сведений и др. Для таких действий, как правило, характерна достаточно локальная следовая картина. Она определяется тем, что место совершения преступных действий и дислокация объекта преступного посягательства расположены вблизи друг от друга или совпадают. Приемы их исследования достаточно традиционны.

Вторая группа преступных действий осуществляется с использованием компьютерных и коммуникационных устройств. Тогда несанкционированный доступ реализуется с помощью различных способов: подбором пароля, использованием чужого имени, отысканием и применением пробелов в программе, удаленным использованием различных специализированных программ, таких как «кей-логгер» - считывает и передает все нажатия клавиш клавиатуры, «ред-админ» - позволяет полный удаленный контроль над компьютером, а также других мер преодоления защиты компьютерной информации. Конкретный способ несанкционированного доступа можно установить путем допроса свидетелей из числа лиц, обслуживающих компьютерную систему, и ее разработчиков. При этом следует учитывать выявленную следовую картину. У них необходимо выяснить как преступник мог проникнуть в защищенную систему, например, узнать идентификационный номер законного пользователя, код, пароль для доступа, получить сведения о других средствах защиты системы или сети ЭВМ.

Чрезвычайно важны и другие действия, направленные на фиксацию факта нарушения целостности (конфиденциальности) компьютерной системы и его последствий, следов преступных манипуляций виновного субъекта, отразившихся в ЭВМ и на машинных носителях информации, в линиях связи и др.

Способ несанкционированного доступа надежнее установить путем производства судебной информационно-технической экспертизы. Перед экспертом ставится вопрос: "Каким способом был осуществлен несанкционированный доступ в данную компьютерную систему?" Для этого эксперту нужно представить всю проектную документацию на взломанную компьютерную систему, а также данные о ее сертификации. При производстве такой экспертизы не обойтись без использования компьютерного оборудования той же системы, которую взломал преступник, либо специальных технических и программных средств.

В ряде случаев целесообразен следственный эксперимент для проверки возможности преодоления средств защиты компьютерной системы одним из предполагаемых способов. Одновременно может быть проверена возможность появления на экране дисплея конфиденциальной информации или ее распечатки вследствие ошибочных, неумышленных

действий оператора либо случайного технического сбоя в электронном оборудовании.

Выясняя надежность средств защиты компьютерной информации, прежде всего, следует установить, предусмотрены ли в данной системе или сети ЭВМ меры защиты от несанкционированного доступа, в том числе к определенным файлам. Это возможно в ходе допросов разработчиков и пользователей системы, а также при изучении проектной документации и инструкций по эксплуатации системы. Как правило, неправомерный доступ облегчается халатностью администратора системы или пользователя компьютера, что происходит в 99% случаев. Изучая инструкции, нужно обращать особое внимание на разделы мер защиты информации, порядке допуска пользователей к конкретным данным, разграничении их полномочий, организации контроля за доступом. При установлении лиц, совершивших несанкционированный доступ к конфиденциальной компьютерной информации, следует учитывать, что он является технологически весьма сложным. Осуществить его могут только специалисты, обладающие достаточно высокой квалификацией. Поэтому поиск подозреваемых рекомендуется начинать с технического персонала взломанных компьютерных систем или сетей. Это в первую очередь их разработчики, а также руководители, операторы, программисты, инженеры связи, специалисты по защите информации, другие сотрудники.

Следственная практика свидетельствует, что чем технически сложнее способ проникновения в компьютерную систему или сеть, тем легче установить подозреваемого, ибо круг специалистов, обладающих соответствующими способностями, весьма ограничен. С другой стороны среди «хакеров» очень популярно оставлять на месте преступления, т.е. в системе взломанного компьютера, улики, непосредственно указывающие на совершение преступления как раз лицом, официально работающим с системой. Подобные уловки могут легко завести следствие в ненужном направлении, что часто и происходит, учитывая высокую латентность подобного рода преступлений. В системе или в сети могут быть указания на то, что доступ был совершён с компьютера определённого лица. Секрет подобной уловки знает каждый начинающий хакер, для этого существует огромное количество специальных программ, помогающих получить анонимный доступ к сети, либо доступ через компьютер «подставляемого» лица. Поэтому на практике следователь всегда должен быть крайне осторожен при определении подозреваемого или обвиняемого.

Доказыванию виновности конкретного субъекта в несанкционированном доступе к компьютерной информации способствует использование различных следов, обнаруживаемых при осмотре ЭВМ и ее компонентов. Это, например, следы пальцев, записи на внешней упаковке дискет и др. Для их исследования назначаются криминалистические экспертизы дактилоскопическая, почерковедческая и др.

Для установления лиц, обязанных обеспечивать надлежащий режим доступа к компьютерной системе или сети, следует, прежде всего, ознакомиться с должностными инструкциями, определяющими полномочия сотрудников, ответственных за защиту конфиденциальной информации. Их необходимо допросить для выяснения, кто запускал нештатную программу, и фиксировалось ли это каким-либо способом. Нужно также выяснить, кто особо увлекается программированием, учится или учился на курсах программистов, интересуется системами защиты информации.

У субъектов, заподозренных в неправомерном доступе к компьютерной информации, производится обыск в целях обнаружения: ЭВМ различных конфигураций, принтеров, средств телекоммуникационной связи с компьютерными сетями, записных книжек, в том числе электронных, с уличающими записями, дискет и дисков с информацией, могущей иметь значение для дела, особенно если это коды, пароли, идентификационные номера пользователей данной компьютерной системы, а также сведения о них.

При обыске нужно изымать также литературу и методические материалы по компьютерной технике и программированию. К производству обыска и осмотру изъятых предметов рекомендуется привлекать специалиста по компьютерной технике, незаинтересованного в исходе дела.

Доказать виновность и выяснить мотивы лиц, осуществивших несанкционированный доступ к компьютерной информации, можно лишь по результатам всего расследования. Решающими здесь будут показания свидетелей, подозреваемых, обвиняемых, потерпевших, заключения судебных экспертиз, главным образом информационно-технологических и информационно-технических, а также результаты обысков. В ходе расследования выясняется:

1) с какой целью совершен несанкционированный доступ к компьютерной информации;

2) знал ли правонарушитель о системе ее защиты;

3) желал ли преодолеть эту систему и какими мотивами при этом руководствовался.

Вредные последствия неправомерного доступа к компьютерной системе или сети могут заключаться в хищении денежных средств или материальных ценностей, завладении компьютерными программами, а также информацией путем изъятия машинных носителей либо копирования. Это может быть также незаконное изменение, уничтожение, блокирование информации, выведение из строя компьютерного оборудования, внедрение в компьютерную систему вредоносного вируса, ввод заведомо ложных данных и др.

Хищения денежных средств чаще всего совершаются в банковских электронных системах путем несанкционированного доступа к их информационным ресурсам, внесения в последние изменений и дополнений. Такие посяательства обычно обнаруживают сами работники банков, устанавливаются они и в ходе оперативно-розыскных мероприятий. Сумма хищения определяется посредством судебно-бухгалтерской экспертизы.

Факты неправомерного завладения компьютерными программами вследствие несанкционированного доступа к той или иной системе и их незаконного использования выявляют, как правило, потерпевшие. Максимальный вред причиняет незаконное получение информации из различных компьютерных систем, ее копирование и размножение с целью продажи либо использования в других преступных целях.

Похищенные программы и базы данных могут быть обнаружены в ходе обысков у обвиняемых, а также при оперативно-розыскных мероприятиях.

Если незаконно полученная информация конфиденциальна или имеет категорию государственной тайны, то вред, причиненный ее разглашением, определяется представителями Гостехкомиссии России.

Факты незаконного изменения, уничтожения, блокирования информации, выведения из строя компьютерного оборудования, "закачки" в информационную систему заведомо ложных сведений выявляются прежде всего самими пользователями компьютерной системы или сети. Следует учитывать, что не все эти негативные последствия наступают в результате умышленных действий. Их причиной могут стать случайные сбои в работе компьютерного оборудования, происходящие довольно часто.

При определении размера вреда, причиненного несанкционированным доступом, учитываются не только прямые затраты на ликвидацию негативных последствий, но и упущенная выгода. Такие последствия устанавливаются в ходе следственного осмотра компьютерного оборудования и носителей информации с анализом баз и банков данных. Помогут здесь и допросы технического персонала, владельцев информационных ресурсов. Вид и размер ущерба обычно определяются посредством комплексной экспертизы, проводимой с участием специалистов в области информатизации, средств вычислительной техники и связи, экономики, финансовой деятельности и товароведения.

На заключительном этапе расследования формируется целостное представление об обстоятельствах, которые облегчили несанкционированный доступ к компьютерной информации. Здесь важно последовательное изучение различных документов, особенно относящихся к защите информации. Весьма значимы материалы ведомственного (служебного) расследования.

К этим обстоятельствам относятся:

1) неэффективность методов защиты компьютерной информации от несанкционированного доступа;

- 2) совмещение функций разработки и эксплуатации программного обеспечения в рамках одного структурного подразделения;
- 3) неприменение в технологическом процессе всех имеющихся средств и процедур регистрации операций, действий программ и обслуживающего персонала;
- 4) нарушение сроков изменения паролей пользователей, а также сроков хранения копий программ и компьютерной информации.

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Изучить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выровнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчета приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. В какой очереди устанавливается расследование неправомерного доступа к компьютерной информации.
2. Что может служить признакам несанкционированного доступа или подготовки к нему.
3. Способы преступных манипуляций в сфере компьютерной информации могут быть разделены на две большие группы.

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.
6. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
7. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
9. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическое занятие № 12. Компьютерная криминалистика

Цель занятия: изучить существующие классификации компьютерных преступлений

1. Нарушение авторских прав в Сети

При осуществлении прокурорского надзора за расследованием преступлений в сфере компьютерной информации прокурору необходимо руководствоваться не только положениями уголовно-процессуального законодательства, но и требованиями приказа Генерального прокурора Российской Федерации от 02.06.2011 N 162 "Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия".

Учитывая сложность расследования преступлений в сфере компьютерной информации, уже отмечавшуюся низкую квалификацию следственных работников, необходимость применения при расследовании специальных знаний, прокурорский надзор за расследованием данных преступлений должен осуществляться на протяжении всего периода расследования.

С целью предотвращения нарушений и затягивания сроков следствия прокурору необходимо осуществлять постоянное взаимодействие с руководителем следственного органа, привлекая прокурора, который в последующем будет поддерживать государственное обвинение в судебном заседании.

Организовать такое взаимодействие возможно в виде совместных оперативных совещаний по обсуждению хода следствия при прокуроре, проводимых как при принятии важных процессуальных решений по уголовному делу, например, при оценке достаточности доказательств для предъявления обвинения, при назначении экспертиз и обсуждении их выводов для последующего планирования расследования, при окончании предварительного следствия, при рассмотрении поступающих к прокурору жалоб и заявлений.

Более того, во многих субъектах Российской Федерации изданы межведомственные приказы и иные нормативные документы, регулирующие порядок взаимодействия при расследовании уголовных дел между следственными органами и прокурорами. Это позволяет избежать многих нарушений и недостатков предварительного расследования, которые, в свою очередь, могут повлечь за собой возвращение уголовного дела прокурором для дополнительного расследования или судом прокурору в порядке ст. 237 УПК РФ. Учитывая особенности рассматриваемой категории преступлений, прокурору следует тщательно изучать собранные в ходе предварительного расследования доказательства, которые должны в полной мере устанавливать все обстоятельства, предусмотренные ст. 73 УПК РФ. При этом, как отмечалось ранее, по составам преступлений, предусмотренных главой 28 УК РФ, помимо основных признаков преступления определяется причинно-следственная связь между деянием и наступившими последствиями.

2. Фишинг

Специфика преступлений в сфере компьютерной информации обуславливает необходимость проведения по уголовным делам данной категории ряда специальных судебных экспертиз. В связи с этим важно осуществлять прокурорский надзор уже на первоначальном этапе расследования. Изучая в процессе расследования уголовное дело, прокурор должен установить, в полной ли мере данные экспертные заключения отвечают на поставленные следователем вопросы, все ли необходимые вопросы поставлены перед экспертом и достаточно ли в конечном итоге информации, содержащейся в заключении эксперта, для подтверждения обстоятельств совершения преступления. Несомненно, надзирающий прокурор должен обладать специальными знаниями о видах судебных экспертиз, проводимых по уголовным делам данной категории, давать руководителю следственного органа соответствующие рекомендации.

Так, при расследовании преступлений данной категории помимо традиционных видов экспертиз (криминалистической, дактилоскопической и т.д.) должны проводиться специальные судебные экспертизы - информационно-технологическая и информационно-техническая.

Объединяет эти виды судебных экспертиз компьютерная информация, исследуемая, однако, с разных сторон - технологической либо технической. Различаются они и по непосредственным объектам исследования.

Проведение указанных судебных экспертиз необходимо для исследования собственно информационно-технологических процессов сбора (накопления, хранения, поиска, актуализации, распространения) информации и представления ее потребителю в условиях функционирования автоматизированных информационных систем и сетей и отдельно взятых технических и иных средств обеспечения этих процессов.

К подобным техническим средствам относятся компьютерные устройства, включающие в себя системный блок, устройство внешней памяти, устройства ввода и вывода информации, периферийные устройства, а также средства связи и телекоммуникации. К иным средствам следует отнести программы для компьютеров. Эти средства, обеспечивающие обработку информации, и составляют основу информационно-компьютерной технологии.

Объектом информационно-технологической экспертизы является установленный порядок обработки информации, осуществляемый по заданным алгоритмам, или информационная технология, основанная на применении современной информационно-вычислительной техники, средств связи и телекоммуникаций, составляющих основу информатизации общества.

Непосредственными предметами информационно-технологической экспертизы могут быть:

- проектная документация на разработку и эксплуатацию компьютерных систем и сетей, отражающая процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

- документированная информация (документ), то есть зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать (отдельные документы и массивы документов в информационных системах), в том числе конфиденциальная информация; материалы сертификации информационных систем, технологий и средств их обеспечения и лицензирования деятельности по формированию и использованию информационных ресурсов;

- приказы и распоряжения администрации, инструкции, протоколы, договоры, положения, уставы и методики по эксплуатации компьютерных систем и сетей, отражающие порядок формирования информационных массивов и доступа к ним (важнейшими из этих предметов исследования могут быть должностные инструкции сотрудников соответствующих информационных подразделений);

- схемы движения информации от источников к потребителю с указанием пунктов ее сбора, контроля, накопления, обработки и использования; табель распределения выходных данных (перечень пользователей с указанием

- периодичности, объема и сроков поступления информации), а также другие документы, позволяющие наиболее полно раскрыть сущность информационной технологии данной компьютерной системы или сети (они обычно прилагаются к техническому заданию на их разработку);

- входные и выходные документы, установленные для данной автоматизированной информационной системы;

- словари, тезаурусы и классификаторы;

- иные эксплуатационные и сопроводительные документы (особое значение для расследования компьютерных преступлений имеют журналы и другие виды учета работы операторов, регистрации сбойных ситуаций и обращений в компьютерную систему или сеть).

Несомненно, что все указанные документы должны быть изъяты своевременно и с соблюдением установленных законом норм. На необходимость этого прокурор должен обращать внимание следователя (в том числе на межведомственных оперативных совещаниях при обсуждении хода расследования уголовного дела), ориентируя последнего на соблюдение разумных сроков уголовного судопроизводства, установленных ст. 6.1 УПК РФ.

Практическое занятие № 13 Компьютерная криминалистика

1. Оперативно-розыскные мероприятия

Информационно-технологическая экспертиза назначается в тех случаях, когда для возникающих в ходе расследования вопросов требуются специальные познания в технологии информационных процессов.

Возможности этой экспертизы достаточно широки. С ее помощью можно определить: соответствие существующего технологического процесса компьютерной обработки информации проектной и эксплуатационной документации на конкретную информационную систему либо сеть;

конкретные отклонения от установленной информационной технологии, а также непосредственных исполнителей, допустивших нарушение установленной информационной технологии;

надежность организационно-технологических мер защиты компьютерной информации;

вредные последствия, наступившие из-за неправомерного нарушения установленной технологии компьютерной обработки информации;

обстоятельства, способствовавшие преступному нарушению технологии электронной обработки информации.

Изучая заключение информационно-технологической экспертизы, прокурору следует обратить внимание на то, выяснено ли следователем:

соответствие процессов сбора, обработки, накопления, хранения, поиска и распространения информации установленной проектной и эксплуатационной документации информационной технологии в данной компьютерной системе или сети;

какие конкретно отклонения от нее допущены;

кем нарушены технологические требования в процессе эксплуатации данной компьютерной системы или сети;

кто из должностных лиц должен был обеспечить соблюдение установленной технологии электронной обработки данных;

какие организационно-технологические меры защиты компьютерной системы, предусмотренные эксплуатационной документацией, были приняты;

какие вредные последствия связаны с нарушением установленной технологии электронной обработки информации;

является ли указанное отклонение от технологии обработки данных причиной наступивших последствий;

каковы причины нарушения установленной обработки компьютерной информации; какие меры необходимо принять для их устранения.

Объектом информационно-технической экспертизы является техническое обеспечение информационной безопасности компьютерных систем и сетей.

Предметы информационно-технической экспертизы очень разнообразны. Иными словами, это инструменты, с помощью которых осуществляется доступ к информационным технологиям.

Условно их можно разделить на три основные группы:

- 1) технические средства обработки информации;
- 2) машинные носители информации и машинограммы, создаваемые средствами вычислительной техники;
- 3) программные средства и базы данных.

К первой группе относятся: компьютеры, отдельные узлы, устройства ввода и вывода информации; печатающие устройства (принтеры); периферийные устройства; устройства для связи между пользователями (модемы и факс-модемы); технические устройства и приспособления, специально разработанные для обхода средств защиты компьютерных систем и сетей от несанкционированного доступа; технические средства защиты информации

другие устройства.

Ко второй группе относятся: накопители на жестких дисках ("винчестеры"); накопители на гибких магнитных дисках (дискеты); устройства для быстрого сохранения всей информации, находящейся на жестком диске (стримеры); оптические диски; пластиковые карты; аудио- и видеокассеты и другие носители информации, обрабатываемые компьютерами.

К третьей группе относятся программы для электронных вычислительных машин и базы данных.

Следует отметить, что исходя из анализа предметов указанных двух экспертиз, каждая из них имеет свои характерные особенности.

Информационно-техническая экспертиза назначается в том случае, когда в ходе следствия возникает необходимость в специальных исследованиях непосредственно технической части (отдельных узлов, блоков, периферийных устройств, оборудования, составляющих компьютерные системы или сети, пластиковых карт, дисков, дискет, других носителей информации, обрабатываемых компьютерами, а также программных средств). К ее основным задачам относятся:

- определение технического состояния компьютерного оборудования и пригодности его для решения задач, предусмотренных проектной и эксплуатационной документацией на данную автоматизированную систему;

- техническое исполнение конкретных технологических информационных процессов и отдельных операций, ставших предметом предварительного следствия, установление конкретного терминала, с которого совершен несанкционированный доступ в данную компьютерную систему или сеть;

- восстановление содержания поврежденных информационных массивов, отдельных файлов на магнитных носителях;

- выявление технических причин сбойных ситуаций в работе компьютера;

- установление подлинности информации, записанной на машинных носителях (дисках, дискетах, пластиковых картах), и внесенных в них изменений;

- выявление в компьютерной программе разного рода неправомерных изменений, дополнений, вставок преступного характера;

- установление вида компьютерного вируса, источника его проникновения в исследуемую систему и причиненных им вредных последствий;

- установление соответствия средств защиты информации от несанкционированного доступа и проникновения компьютерного вируса сертификационным требованиям.

Изучая заключение информационно-технической экспертизы, прокурору необходимо выяснить, установлено ли:

- техническое состояние компьютерного оборудования и его пригодность для решения в полном объеме задач, предусмотренных проектной и эксплуатационной документацией на данную компьютерную систему или сеть;

- с какого терминала и какими средствами связи и телекоммуникации мог быть совершен несанкционированный доступ в компьютерную систему или сеть;

- возможность восстановления записанной прежде информации на частично поврежденном машинном носителе и ее содержание;

- причина выявленных в ходе следствия сбоев данного компьютерного оборудования и наличие возможности их предотвращения с помощью технических средств;

- перечень действий, предусмотренных соответствующими правилами для предотвращения сбоя, несанкционированного доступа, уничтожения файла, неправомерного копирования компьютерной информации, и не выполненных ответственным лицом;

- признаки несанкционированных изменений информации, записанной на сменные диски (дискеты) и их содержание;

- возможность использования в данной компьютерной системе посторонних программ без автоматической регистрации ее использования;

наличие в программе преднамеренной "закладки" (зарезервированного места в программе на случай необходимости последующей вставки дополнительных команд), ее назначение и автор;

средства защиты от вредоносных программ, предусмотренные в данной системе, их надежность, наличие сертификата и соответствие средств его требованиям; процедура заражения данной системы компьютерным вирусом; класс (тип) вируса, заразившего данную компьютерную систему и источник его происхождения;

размер и характер вреда, причиненного компьютерным вирусом.

Разумеется, круг вопросов по двум указанным видам экспертиз предлагаемыми перечнями не исчерпывается. С учетом характера каждого конкретного преступления могут быть поставлены и другие вопросы, объем которых определяется следователем в зависимости от расследуемого события и выяснения обстоятельств информационно-технологического или информационно-технического характера.

Так, по делам о неправомерном доступе к охраняемой законом компьютерной информации перед информационно-технологической экспертизой могут быть поставлены более частные вопросы, относящиеся к режиму ее обработки и охраны, главным образом к организационно-административным мерам защиты этой информации.

В настоящее время встречаются и другие виды экспертиз компьютерно-технической информации, что обусловлено динамичным развитием сферы высоких технологий, например, экспертиза электронно-цифровой подписи; экспертиза процесса разработки и использования программного обеспечения; компьютерно-сетевая экспертиза, экспертиза обстоятельств создания и использования файлов и баз данных и др. Все они отличаются, как правило, предметом, целью исследования и вопросами, которые могут быть поставлены перед экспертом.

В процессе расследования преступлений в сфере компьютерной информации может возникнуть необходимость производства и других видов экспертиз.

Например, идентификационная задача может быть решена с помощью комплексной компьютерно-технической и судебно-автороветческой экспертизы, позволяющей проверить, не написана ли данная компьютерная программа конкретным лицом.

2. Перехват и исследование трафика

Для проведения носящих комплексный характер экспертных исследований в сфере компьютерной информации приглашаются высококвалифицированные специалисты в области информатики, вычислительной техники и программирования, а также традиционных видов криминалистической экспертизы, экономической, финансовой, бухгалтерской и товароведческой экспертиз.

В ходе комплексной судебно-бухгалтерской экспертизы и экспертизы программного обеспечения устанавливают: возможность несанкционированного скрытого доступа к программному обеспечению с целью внесения изменений, влияющих на результаты расчетов и отчетность, механизм совершения таких изменений, их характер и последствия;

кто из работников учреждения, обслуживающих и эксплуатирующих эти средства, имеет указанные выше возможности;

размер причиненного материального ущерба;

какие нарушения правил, регламентирующих ведение бухгалтерского учета и отчетности, могли способствовать образованию ущерба;

какая операционная система использована в конкретном компьютере; не вносились ли в программу данного системного продукта какие-либо коррективы, изменяющие выполнение операций (какие именно);

возможно ли получение доступа к конфиденциальной финансовой информации, имеющейся в данной сети, и каким образом может быть осуществлен этот доступ.

Поскольку подлинная информация на машинных носителях при производстве экспертиз может быть безвозвратно уничтожена, следует убедиться в ее наличии в уголовном деле в качестве вещественного доказательства и направлении для проведения экспертного

исследования ее копии.

В случае, если прокурор установит, что какие-либо вопросы в заключении эксперта раскрыты не полностью или невозможно сделать однозначный вывод об исследуемых обстоятельствах на основании данного заключения, целесообразно ориентировать следователя провести допрос эксперта с целью устранения указанных недостатков. Учитывая, что необходимо осуществлять надзор также и за соблюдением разумных сроков уголовного судопроизводства, нарушение которого ущемляет права потерпевших, назначать дополнительную судебную экспертизу следует только в том случае, если возникшие вопросы нельзя выяснить в ходе допроса эксперта. Невыяснение всех необходимых вопросов в ходе экспертного исследования может впоследствии негативно сказаться на сроках судебного рассмотрения уголовного дела.

Если же прокурор выявляет уже допущенное в ходе предварительного расследования нарушение, то он должен использовать предоставленные ему Уголовно-процессуальным кодексом Российской Федерации полномочия и внести требование об устранении нарушений, допущенных в ходе предварительного следствия.

Как известно, предварительное следствие оканчивается ознакомлением обвиняемого и его защитника с материалами дела, составлением и подписанием следователем обвинительного заключения и передачей уголовного дела прокурору для решения вопроса о его направлении в суд.

3. Киберсквоттинг

Процессуальный порядок реализации полномочий прокурора по уголовному делу, поступившему с обвинительным заключением, регламентирован ст. 221, 222 УПК РФ.

В соответствии со ст. 221 УПК РФ прокурор или его заместитель обязаны рассмотреть поступившее уголовное дело в срок, не превышающий десяти суток, и принять одно из следующих решений:

об утверждении обвинительного заключения и о направлении уголовного дела в суд; о возвращении уголовного дела следователю для производства дополнительного следствия, изменения объема обвинения либо квалификации действий обвиняемых или пересоставления обвинительного заключения и устранения выявленных недостатков со своими письменными указаниями;

о направлении уголовного дела вышестоящему прокурору для утверждения обвинительного заключения, если оно подсудно вышестоящему суду.

Признав, что имеются основания для специальности дела в суд, прокурор на первой странице обвинительного заключения ставит свою подпись об утверждении обвинительного заключения. Для принятия такого решения прокурором по материалам уголовного дела должны быть установлены следующие обстоятельства:

достаточность доказательств для рассмотрения дела в суде;

возможность поддержания с имеющимися доказательствами государственного обвинения;

относимость и допустимость собранных по делу доказательств; соответствие предъявленного обвинения собранным доказательствам;

отсутствие обстоятельств, влекущих прекращение уголовного дела или уголовного преследования;

отсутствие процессуальных нарушений, исключающих возможность рассмотрения дела в суде;

соответствие обвинительного заключения требованиям закона.

Особое внимание прокурору при изучении дел о преступлениях в сфере компьютерной информации, поступивших для утверждения обвинительного заключения, следует обращать на предъявленное обвинение, которое должно полностью подтверждаться имеющимися в уголовном деле доказательствами, и содержать текст идентичный тексту постановления о привлечении в качестве обвиняемого.

Прокурор согласно п. 2 ч. 1 ст. 221 УПК РФ вправе вернуть уголовное дело

следователю для производства дополнительного следствия, изменения объема обвинения либо квалификации действий обвиняемых или пересоставления обвинительного заключения или устранения выявленных недостатков со своими письменными указаниями. В настоящее время суд не имеет такого права, однако он может вернуть уголовное дело прокурору, при наличии оснований, предусмотренных ст. 237 УПК РФ, что, как правило, свидетельствует о ненадлежащем прокурорском надзоре за ходом предварительного следствия.

4. Другое

Хотя уголовно-процессуальным законом и предусмотрена возможность восполнения государственным обвинителем неполноты следствия, в том числе и путем предоставления суду новых доказательств, изначально отталкиваясь от такой возможности при наличии нарушений, допущенных следователем и выявленных на стадии утверждения обвинительного заключения, нецелесообразно, поскольку направлять в суд с утвержденным обвинительным заключением уголовное дело, имеющее заведомые недостатки, прокурор не имеет права.

Поэтому при выявлении прокурором обстоятельств, препятствующих рассмотрению уголовного дела судом, в том числе и неустановлении обстоятельств, подлежащих доказыванию, он обязан своим мотивированным постановлением возвратить уголовное дело следователю для дополнительного следствия, изменения объема обвинения либо квалификации действий обвиняемого или составления нового обвинительного заключения и устранения выявленных недостатков.

Таким образом, в условиях увеличения числа преступлений в сфере компьютерной информации возрастает и роль прокурорского надзора за исполнением законов при расследовании преступлений указанной категории. Надлежащая организация прокурорского надзора позволяет обеспечить защиту прав и законных интересов лиц и организаций, потерпевших от преступлений, и личности от незаконного и необоснованного обвинения, осуждения, ограничения ее прав и свобод, восстановить уже нарушенные права и предотвратить совершение новых преступлений.

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выровнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчета приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Цели и задачи прокурорского надзора
2. Виды судебных экспертиз
3. Информационно-технологическая экспертиза
4. Процессуальный порядок реализации полномочий прокурора

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием

12.12.1993).

2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.
6. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
7. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
9. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическое занятие № 14. Компьютерная криминалистика

1. Шифрованный трафик

Зашифрование

Процесс преобразования открытых данных в закрытые (зашифрованные). В данном программном продукте используется алгоритм шифрования ГОСТ 2814789. Это симметричный алгоритм, что означает, что для шифрования и расшифрования используется одинаковый ключ.

Расшифрование

Процесс преобразования закрытых данных в открытые (расшифрованные).

Ключ, ключевая система

Конкретное секретное значение криптографического преобразования, определяющее ход процесса преобразования данных. В данном пакете программ в качестве ключей шифрования могут использоваться: 🌐 Ключ Пользователя; 🌐 Сетевой ключ.

При работе с ключами всегда производится анализ имитоприставки. Узел Замены (УЗ)

Долговременный элемент ключевой системы ГОСТ 28147-89. Обычно хранится в файле uz.db3 на ключевом носителе и является первым ключевым элементом, вводимым в устройство шифрования при инициализации. Все компьютеры, между которыми предполагается обмен зашифрованной информацией (например, локальная сеть), должны использовать один и тот же УЗ, т. к. несоответствие Узлов Замены приведет к невозможности расшифрования файлов с другой машины.

Главный Ключ (ГК)

Секретный ключ, используется для шифрования других ключей. Обычно хранится в файле gk.db3 на ключевом носителе. Может быть зашифрован на пароле. Создается администратором. При инициализации устройства шифрования загружается в него и находится там до выключения питания ЭВМ. Пароль

Последовательность символов, вводимых с клавиатуры. Пароль защищает ключи от несанкционированного использования в случае их хищения или потери. В пакете КРИПТОН® Шифрование максимальная длина пароля для ключей шифрования - 37 символов; минимальная длина - 4 символа. Длина пароля определяет стойкость системы. Поэтому рекомендуется использовать длинные пароли с неповторяющимися символами. Символы разных регистров (прописные и строчные буквы) различаются. Использовать символы с кодами меньше 32 и больше 127 (управляющие символы, псевдографику и русские буквы) не рекомендуется.

Ключ пользователя (ПК)

Секретный ключ, используется для шифрования файлов и других ключей. Хранится в файле с расширением ".KEY", обычно в зашифрованном виде.

Сетевой ключ

Секретный ключ, используется для шифрования файлов с целью передачи их между узлами криптографической сети. Все узлы сети нумеруются. Для каждого узла, с которым планируется обмен информацией, необходимо иметь свой сетевой ключ. Задача обеспечения сетевыми ключами возлагается на администратора сети. Сетевые ключи хранятся в Сетевом Наборе.

Имитовставка, имитоприставка

Применяется для обеспечения защиты системы шифрования от навязывания ложных данных. Имитовставка представляет собой отрезок информации фиксированной длины, полученный из открытых данных и ключа. Создается при зашифровании данных и добавляется к ним. При расшифровании данных также вычисляется имитовставка и сравнивается с хранимой.

В случае несовпадения можно выделить следующие причины:

изменен Узел Замены;

изменен ключ, на котором были зашифрованы данные; изменены сами зашифрованные

данные;

если для зашифрования использовался пароль, то при расшифровании он был неверно введен;

неисправно устройство шифрования.

2. Исследование статистики трафика

Криптографическая сеть

Множество компьютеров, называемых узлами, между которыми тем или иным способом осуществляется направленный обмен зашифрованной информацией, называется криптографической сетью. Направленный обмен подразумевает возможность зашифровать передаваемую информацию таким образом, чтобы расшифровать ее мог только тот узел, для которого она предназначалась. Обмен информацией между узлами криптографической сети может осуществляться как посредством локальных и глобальных сетей, так и с помощью сменных носителей. В пакете КРИПТОН® Шифрование для защиты данных в криптографической сети используется симметричный алгоритм шифрования - ГОСТ 28147-89.

Сетевой ключ

Секретный ключ, используется для зашифрования файлов с целью передачи их между узлами криптографической сети. Все узлы сети нумеруются. Для каждого узла, с которым планируется обмен информацией, необходимо иметь свой сетевой ключ. Задача обеспечения сетевыми ключами возлагается на администратора сети. Сетевые ключи хранятся в Сетевом Наборе.

Сетевая Таблица

Для обмена зашифрованной информацией между N узлами необходимо $N*(N-1)$ ключей (каждый с каждым). Фактически, это таблица, где в заголовках строк и столбцов проставлены номера узлов, а в ячейках хранятся ключи. Эта матрица симметрична, т. е. ключ для передачи от узла А узлу Б (сетевой ключ АБ) в точности равен сетевому ключу Б-А. Сетевая Таблица при создании зашифровывается на Ключе Сетевой Таблицы (КСТ).

Сетевой Набор

Из полной Сетевой Таблицы необходимо для каждого из узлов сформировать набор ключей для связи с другими узлами. Фактически, такой набор представляет собой одну из строк таблицы. Сетевой Набор хранится в файле NNNNN.SYS в каталоге сетевых ключей, где NNNNN - пятизначный десятичный номер данного узла. Он всегда зашифрован на Ключе Сетевого Набора (КСН), хранящемся в файле NNNNN.KEY в каталоге сетевых ключей.

КСН получают вместе с Сетевым Набором от администратора криптографической сети. При получении КСН обычно зашифрован на главном ключе, поэтому рекомендуется перешифровать его на пароле.

Организация криптографической сети

Для организации криптографической сети администратор должен выполнить следующие действия

Создать Сетевую Таблицу. Для этого необходимо указать количество узлов криптографической сети и имя Сетевой Таблицы. В результате автоматически создается новый Ключ Сетевой Таблицы NET_SYS.KEY, на котором автоматически зашифровывается Сетевая Таблица KEY_NET.SYS

Создать Сетевые Наборы (СН) для узлов криптографической сети.

По умолчанию создаются СН для всех узлов и в каждом сетевом наборе все узлы являются доступными. При необходимости можно создать такие СН, чтобы узел мог шифровать данные только для ограниченного множества узлов криптографической сети. В результате получается множество Ключей Сетевого Набора (NNNNN.KEY) и Сетевых Наборов (NNNNN.SYS) для узлов криптографической сети.

Каждому узлу присвоить свой номер NNNNN. Распределить Ключи Сетевого Набора и Сетевые Наборы по соответствующим узлам криптографической сети. Узлу с номером NNNNN необходимо передать два файла: NNNNN.KEY и NNNNN.SYS.

Шифрование файлов для передачи в криптографической сети

Файл данных, передаваемый узлом А узлу Б, зашифровывается на Файловом (сеансовом) Ключе. Файловый Ключ создается автоматически при зашифровании файла данных и передается вместе с ним. Так как файловый ключ не может передаваться в открытом виде, то он зашифровывается на Сетевом Ключе А-Б. Этот ключ узел А берет из своего Сетевого Набора.

Сетевой Набор узла А зашифрован на Ключе Сетевого Набора (КСН) узла А, который, в свою очередь, тоже может быть зашифрован на каких-либо ключах узла А (как правило, ГК).

Узел Б, по информации, присовокупленной к зашифрованному файлу, понимает, что файл пришел от узла А. Используя свои ключи, узел Б расшифровывает свой КСН.

Затем, используя КСН, узел Б расшифровывает свой набор и извлекает из него Сетевой Ключ А-Б. Так как этот Сетевой Ключ совпадает с тем Сетевым Ключом, который использовал узел А для зашифрования, то узел Б может расшифровать Файловый Ключ, пришедший вместе с файлом.

Наконец, с помощью Файлового Ключа расшифровывается сам файл.

Настройка параметров

После запуска Мастера ключей шифрования и выбора настройки параметров (рисунок 17.1) правая сторона панели содержит следующие настраиваемые параметры: "Каталог Ключей Пользователя".

Следует ввести каталог Ключей Пользователя. В этом каталоге будет производиться поиск Ключей Пользователя в следующих ситуациях: - Зашифровании файла на Ключе Пользователя.

Расшифровании файла, зашифрованного на Ключе Пользователя. Перешифровании файла, зашифрованного на Ключе Пользователя.

Требуемый каталог можно указать также с помощью кнопки обзора каталогов. По данной кнопке на экран выводится меню "Диски"/"Карточки", позволяющее указать каталог с помощью стандартного диалога Windows или диалога выбора устройств SCApi.

Практическое занятие № 15. Компьютерная криминалистика

1. Исследование системных логов

Организация взаимосвязи пользователей.

Обмен открытыми ключами через сертификационный центр (СЦ)

Организуется центр для сертификации пользователей. В СЦ поступают открытые ключи и сопровождающие их документы (см. рисунок 19.1).

В ответ пользователь получает: зарегистрированные открытые ключи (или базу данных (БД) зарегистрированных открытых ключей) всех владельцев (в том числе и свой);

файл с полномочиями этих владельцев (и с подписями);

ключ-сертификат как в виде файла, так и в виде юридического документа.

Владелец при получении должен проверить истинность ключа- сертификата, а затем проверить подписи всех полученных открытых ключей и файлов. Также необходимо проверить свой открытый ключ. При положительных результатах проверки БД открытых ключей записываются в соответствующий каталог.

Время от времени СЦ должен пополнять Вашу базу данных открытых ключей и полномочий.

При такой организации работ пользователь формирует подпись документов и не заботится об обмене открытыми ключами и полномочиями. Однако большая нагрузка ложится на СЦ по рассылке баз открытых ключей и полномочий. Кроме этого, администратор этого центра в принципе может включить в базу данных ложный открытый ключ, что обязательно выявится. Если есть сомнения, можно запросить открытый ключ и полномочия напрямую.

Можно оставить за СЦ только сертификацию ключей и полномочий, освободив его от рассылки баз данных. В этом случае при первой посылке в любой адрес документов пользователю необходимо послать по этому адресу также зарегистрированные открытые ключи и полномочия. Можно зарегистрироваться в разных не связанных друг с другом СЦ или же связать СЦ в любую сеть для обмена либо только ключами-сертификатами, либо дополнительно еще и базами данных. Тогда пользователю достаточно зарегистрироваться только в одном из СЦ.

Пакет КРИПТОН® Подпись обеспечивает возможность организации работы по всем описанным выше вариантам.

Генерация секретных ключей

После установки пакета КРИПТОН® Подпись и создания дискеты с ключами для первоначального входа можно приступить к генерации ключей. Обычно этим занимается специально выделенный человек, называемый администратором.

Для генерации ключей необходимо:

запустить программу конфигурации пакета КРИПТОН® Подпись;

указать каталоги для секретного и открытых ключей (для секретного ключа можно сразу указать дискету или другой ключевой носитель);

запустить программу "Мастер ключей подписи";

вставить ключевой носитель и выполнить команду "Файл \ Ключи

\ Сгенерировать";

повторить последнюю команду столько раз, сколько ключей необходимо создать; создать новую базу данных открытых ключей;

выполнить команду "Добавить ключи из файла", добавить все ключи в базу данных.

Два последних пункта не являются обязательными, но обмен открытыми ключами удобнее вести, если они находятся в базе данных, а не в отдельных файлах.

Таким способом генерируются ключи для операторов, самого администратора и работника, который будет проводить сертификацию открытых ключей (это может быть и сам администратор). Последние в обязательном порядке закрываются паролем. Ключи могут передаваться по специальной связи, однако секретные ключи более правильно вообще не

передавать по сети.

Оператор при получении секретного ключа может закрыть его на своем собственном пароле. Сертификация открытых ключей

Сертификация рекомендуется выполнять в сертификационном центре на защищенной ЭВМ специальным человеком в следующей последовательности:

при помощи программы "КРИПТОН® Подпись - Конфигурация" устанавливаются параметры: "Каталог расположения или имя файла секретного ключа" должен указывать на секретный ключ сертификационного центра, "Каталог расположения ключей- сертификатов" должен указывать на каталог, в котором расположены файлы ключей- сертификатов или базы данных ключей-сертификатов;

запускается на выполнение "Мастер ключей подписи";

формируются подписи у всех открытых ключей (команда "Файл \Ключи \ Сертифицировать");

создается новая база открытых ключей (или сертифицированные открытые ключи добавляются в старую);

выход из менеджера баз данных.

Сертифицированный секретный ключ имеет срок своего действия, по истечении которого должна проводиться плановая смена всех ключей.

Базы данных с сертифицированными открытыми ключами рассылаются всем владельцам. Возможно заново сертифицировать открытые ключи, удалив у них старую подпись.

1. Исследование логов мейл-сервера и заголовков электронной почты

Основные этапы алгоритма DES при шифровании текста: Генерируется (задается) случайная последовательность Q из 56 бит.

В последовательность Q , для контроля четности, добавляются восемь контрольных битов в позиции

8, 16, 24, ..., 64.

Получается блок U размером в 64 бита.

Для удаления контрольных битов из блока U и формирования ключа K для шифрования, блок U преобразуют, используя функцию $G(U)$. Функция G определяется в виде стандартной таблицы, которую надо использовать в неизменном виде. В результате преобразования получают блок

$K=G(U)$

размером в 56 бит. Блок K разбивают на две половины $C0$ и $D0$ по 28 бит.

Используя $C0$ и $D0$, последовательно определяются Ci и Di , $i = 1, 2, \dots, 16$. Для формирования Ci и Di применяют операции циклического сдвига влево на один или два бита. Величина сдвига определяется стандартной таблицей. Операции сдвига для Ci и Di выполняются независимо. Последовательность $C5$ получается из $C4$ посредством циклического сдвига влево на 2 бита, а $D5$ — посредством циклического сдвига влево на 2 бита $D4$ (см. таблицу сдвигов для вычисления ключа). В результате четвертого этапа формируется 16 ключей для 16 раундов алгоритма DES.

Завершающий этап формирования ключей. Используя перестановку H , которая задается стандартной таблицей, каждый ключ размером в 56 бит преобразуется в блок из 48 бит. Данным преобразованием завершается этап формирования ключей.

Текущий блок открытого текста размером в 64 бит, представленный в виде двух 32 битовых блоков ($L0R0$) преобразуется начальной перестановкой IP , которая задается фиксированной стандартной таблицей.

Выполняется 16 раундов преобразований по следующим формулам $Li = Ri-1$,

$Ri = Li _ f(Ri-1, Ki)$, $i = 1, 2, \dots, 16$.

Функция $f(Ri-1, Ki)$ представляет собой некоторую суперпозицию простых

преобразований, детальное описание которых будет дано ниже. Отметим, что функция $f(Ri-1, Ki)$ является нелинейной. Нелинейность функции $f(Ri-1, Ki)$ обеспечивается S- блоками.

Алгоритм вычисления функции шифрования $f(Ri-1, Ki)$

К блоку $Ri-1$ применяют функцию расширения $E(Ri-1)$, которая 32битовый блок $Ri-1$ преобразовывает в блок $R' = E(Ri-1)$ размером в 48 бит. Функция $E(Ri-1)$ определяется стандартной таблицей. Алгоритм вычисления функции шифрования формулируется следующим образом.

Вычисляется новый блок размером в 48 бит по формуле $B = E(Ri-1) \cdot Ki$.

Блок B размером в 48 бит разбивается на восемь блоков $Bj, j=1,2,\dots, 8$, по шесть битов каждый

$$B = B1B2B3B4B5B6B7B8.$$

Каждый блок Bj размером в шесть бит, используя свою функцию Sj , преобразуется в блок $Sj(Bj)$ размером в четыре бита. В результате получается следующий блок данных

$$B' = S1(B1) S2(B2) S3(B3) S4(B4) S5(B5) S6(B6) S7(B7) S8(B8)$$

размером в 32 бита.

Алгоритм преобразования блока Bj размером в шесть бит в блок $Sj(Bj)$ размером в четыре бита следующий. Каждая функция Sj представляет собой стандартную таблицу, которая состоит из четырех строк с номерами 0, 1, 2, 3, и шестнадцати столбцов с номерами 0,1,2,...,15. Пусть, например, некоторый блок

$$Bj = b1 \ b2 \ b3 \ b4 \ b5 \ b6 = 110010, j = 1, 2, \dots, 8.$$

Тогда имеет место:

биты $b1b6 = 10$ формируют номер столбца (двоичное число 10 равно десятичному числу 2) таблицы Sj , биты $b2 \ b3 \ b4 \ b5 = 1001$ формируют номер строки (двоичное число 1001 равно десятичному числу 9) таблицы Sj . Блок $Bj = b1 \ b2 \ b3 \ b4 \ b5 \ b6$

$= 110010$ заменяют двоичным значением числа таблицы Sj , которое находится на пересечение строки с номером $b1b6 = 10$ (2) со столбцом с номером $b2 \ b3 \ b4 \ b5 = 1001$ (9). Преобразуя каждое $Bj, j = 1, 2, \dots, 8$, из блока B , получим новый блок B' размером в 32 бита.

2. Избирательный перехват

Добавляются биты к исходному сообщению. Если L – длина сообщения, то для L должна выполняться формула

$$L \equiv 448 \bmod 512.$$

Это означает, что длина дополненного сообщения в битах должна быть на 64 бита меньше, чем ближайшее кратное целого числа 512. Структура дополнения следующая: первый бит дополняемого значения равен 1, а остальные – равны 0.

К сообщению из шага 1 добавляется значение длины. К результату шага 1 добавляется 64-битовое значение длины исходного сообщения, т.е.

длины сообщения до шага 1.

Результат шага 2 разбивается на блоки по 512 бит

$$M1, M2 \dots, MK,$$

где K число таких блоков, $L = K \cdot 512$. В свою очередь каждый блок $M2, i=1,2, \dots, K$, разбивают на 16 массивов по 32 бита

$$X[0], X[1], \dots, X[k], k=0, 1, \dots, 15.$$

Для записи промежуточных значений в 128 бит при вычислении хэшфункции используются буфер H , который состоит из четырех переменных a, b, c и d размером в 32 бита каждая. Эти переменные соответственно инициализируются ранее определенными константами A, B, C и D .

Преобразуются блоки $Mi, i = 1, 2, \dots, K$, в 512 бит в профиль Hi длиной в 128 бит. Напомним, что блок Mi разбит на 16 частей (массивов) по 32 бита $X[0], X[1], \dots, X[k], k=0, 1, \dots, 15$.

Основные этапы алгоритма SHA-1 при сжатии исходного текста

Добавление битов заполнителя. Сообщение дополняется так, чтобы его общая длина в битах была сравнима со значением 448 по модулю 512, т.е. длина равна $448 \bmod 512$. Операция дополнения выполняется всегда, даже если сообщение уже оказывается требуемой длины. Поэтому число добавляемых битов должно быть от 1 до 512. Структура битов заполнителя следующая: первый бит равен 1, а все остальные равны 0.

К сообщению из шага 1 добавляется значение длины. К результату шага 1 добавляется 64-битовое значение длины исходного сообщения, т.е. длины сообщения до шага 1.

Результат шага 2 разбивается на блоки по 512 бит: $M_1, M_2, \dots, M_K$, где K есть число таких блоков, $L = K \times 512$. В свою очередь каждый блок M_i разбивают на 16 частей (массивов) по 32 бита $X[0], X[1], \dots, X[k]$, $k = 0, 1, \dots, 15$.

Для записи промежуточных значений в 160 бит при вычислении хэшфункции используются буфер H , который состоит из пяти переменных a, b, c, d и e размером в 32

бита каждая. Эти переменные соответственно инициализируются ранее определенными константами A, B, C, D и E .

Обработка сообщения происходит 512-битовыми блоками. Логiku модуля функции сжатия алгоритма можно представить в виде следующего цикла

$H_i = H_{i-1} + N$

Цикл от $t=0$ до $t=79$ шаг 1 Начало цикла

$H = (a \lll 5) + ft(b, c, d) + e + W_t + K_t \quad e = d \quad d = c \quad c = b \lll 30$

$b = a$

$a = H$ Конец цикла

$H_{i+1} = H_i + N$

Здесь:

$ft(b, c, d)$, W_t , K_t – функции, 32-битовые блоки и константы, которые определялись ранее. Отметим, что W_t формируется из текущего входного блока M_i .

H_i – промежуточные значения результата вычисления хэш-функции. $+$ – операция сложения по модулю 232.

3. Исследование логов веб-сервера

Текст, предназначенный для шифрования, разбивается на блоки длиной по 64 бит.

Полученные блоки в дальнейшем будем называть начальными данными.

В ключевое устройство

$X_0, X_1, \dots, X_7$

записывается сгенерированный ключ длиной в 256 бит по 32 бита в каждый

$X_i, i = 1, 2, \dots, 7$, то есть

$X_0 = (w_{32}, \dots, w_1),$

$X_1 = (w_{64}, \dots, w_{33}),$

...

$X_7 = (w_{256}, \dots, w_{225}).$

Очередной блок начальных данных T_i длиной в 64 бит

$T_i(a_1, a_2, \dots, a_{32}, b_1, b_2, \dots, b_{32})$

засылается в накопители N_1 и N_2 по следующей схеме

$N_1 = (a_{32}, \dots, a_1), N_2 = (b_{32}, \dots, b_1).$

Содержимое N_1 суммируем по модулю 232 с содержимым X_0 , результат засылается в N_1 .

Результат суммирования преобразовывается в блоке подстановки K .

Результат 5 шага преобразуется в регистре сдвига R . Происходит циклический сдвиг на 11 бит в сторону старших разрядов.

Результат сдвига суммируется по модулю 2 со значением в накопителе N_2 . Содержимое N_1 пересылается в N_2 , а результат 7 шага записывается в N_1 .

Процесс шифрования с четвертого по восьмой шаг алгоритма повторяется еще 31 раз в следующем порядке использования частей ключа (с учетом проделанного преобразования с

частью ключа X_0):

1-й раунд шифрования из 8 шагов;

$X_0, X_1, \dots, X_7$ 2-й раунд шифрования из 8 шагов; $X_0, X_1, \dots, X_7$ 3-й раунд шифрования из 8 шагов; $X_0, X_1, \dots, X_7$

4-й раунд шифрования из 8 шагов

$X_7, X_6, \dots, X_0$

Результат последнего 32 шага шифрования, т.е. результат 8 шага алгоритма, сохраняется в накопителе N_2 , а в N_1 сохраняется результат 31 шага.

Результат шифрования текущего блока T_i содержится в накопителях N_1 с 1-го по 32 разряд и N_2 с 1-го по 32 разряд.

Далее процесс шифрования в режиме простой замены продолжается с третьего шага до тех пор, пока не исчерпаются блоки с начальными данными.

Схема алгоритма: режим гаммирования

Текст, предназначенный для шифрования, разбивается на блоки длиной по 64 бит.

Полученные блоки в дальнейшем будем называть начальными данными.

В ключевое устройство

$X_0, X_1, \dots, X_7$

записывается сгенерированный ключ длиной в 256 бит по 32 бита в каждый

$X_i, i = 1, 2, \dots, 7$, то есть

$X_0 = (w_{32}, \dots, w_1)$,

$X_1 = (w_{64}, \dots, w_{33})$,

...

$X_7 = (w_{256}, \dots, w_{225})$.

Генератором последовательности случайных чисел формируется двоичная последовательность длиной в 64 бита (синхропосылка)

$S(s_1, s_2, \dots, s_{32}, s_{33}, s_{34}, \dots, s_{64})$

и засылается в накопители N_1 и N_2 по следующей схеме

$N_1 = (s_{32}, \dots, s_1)$

$N_2 = (s_{64}, \dots, s_{33})$.

Содержимое N_1 и N_2 шифруется в режиме простой замены.

Содержимое накопителей N_1 и N_2 , в которых находится результат шифрования, переписываются соответственно в накопители N_3 и N_4 .

Содержимое накопителя N_4 суммируется по модулю $(2^{32}-1)$ с накопителем N_6 , в котором хранится стандартная константа

$C_2 = 000000001000000001000000001000000001$.

Результат суммирования записывается в накопитель N_4 . Содержимое накопителя N_3 суммируется по модулю 232 с накопителем N_5 , в котором хранится стандартная константа $C_1 = 100000000100000000100000000100000000$.

Результат суммирования записывается в накопителя N_3 . Содержимое накопителя N_3 переписывается в N_1 .

Содержимое накопителя N_4 переписывается в N_2 . Содержимое N_1 и N_2 шифруется в режиме простой замены. Результат 10 шага образует текущий блок гаммы Γ .

Текущий блок гаммы суммируется по модулю 2 с текущим блоком заданного текста.

Результат суммирования формирует результат шифрования в режиме гаммирования.

Далее процесс шифрования в режиме гаммирования продолжается с четвертого шага до тех пор, пока не исчерпаются блоки с начальными данными.

Схема алгоритма: режим гаммирования с обратной связью

Текст, предназначенный для шифрования, разбивается на блоки длиной по 64 бит.

Полученные блоки в дальнейшем будем называть начальными данными.

В ключевое устройство

$X_0, X_1, \dots, X_7$

записывается сгенерированный ключ длиной в 256 бит по 32 бита в каждый

$X_i, i = 1, 2, \dots, 7$, то есть

$X_0 = (w_{32}, \dots, w_1),$

$X_1 = (w_{64}, \dots, w_{33}),$

...

$X_7 = (w_{256}, \dots, w_{225}).$

Генератором последовательности случайных чисел формируется двоичная последовательность длиной в 64 бита (синхропосылка)

$S(s_1, s_2, \dots, s_{32}, s_{33}, s_{34}, \dots, s_{64})$

и засылается в накопители N_1 и N_2 по следующей схеме

$N_1 = (s_{32}, \dots, s_1),$

$N_2 = (s_{64}, \dots, s_{33}).$

Содержимое N_1 и N_2 шифруется в режиме простой замены. Результат четвертого шага образует текущий блок гаммы Γ .

Текущий блок гаммы суммируется по модулю 2 с текущим блоком заданного текста.

Результат суммирования формирует зашифрованный блок

C по следующему правилу

$C(c_1, c_2, \dots, c_{32}, c_{33}, c_{34}, \dots, c_{64})$

в режиме гаммирования с обратной связью.

7. Зашифрованный блок C является исходным состоянием накопителей N_1 и N_2 для выработки следующего блока гаммы. Последовательность битов

$c_1, c_2, \dots, c_{32}, c_{33}, c_{34}, \dots, c_{64}$

засылаются в накопители N_1 и N_2 по следующей схеме

$N_1 = (c_{32}, \dots, c_1),$

$N_2 = (c_{64}, \dots, c_{33}).$

7. Далее процесс повторяется с четвертого шага, пока не исчерпаются блоки с начальными данными.

Схема алгоритма: режим выработки имитовставки

Текст, предназначенный для шифрования, разбивается на блоки длиной по 64 бит.

Полученные блоки в дальнейшем будем называть начальными данными.

В ключевое устройство

$X_0, X_1, \dots, X_7$

записывается сгенерированный ключ длиной в 256 бит по 32 бита в каждый

$X_i, i = 1, 2, \dots, 7$, то есть

$X_0 = (w_{32}, \dots, w_1),$

$X_1 = (w_{64}, \dots, w_{33}),$

...

$X_7 = (w_{256}, \dots, w_{225}).$

Очередной блок начальных данных T_i длиной в 64 бит

$T_i(a_1, a_2, \dots, a_{32}, b_1, b_2, \dots, b_{32})$

засылаются в накопители N_1 и N_2 по следующей схеме

$N_1 = (a_{32}, \dots, a_1), N_2 = (b_{32}, \dots, b_1).$

Содержимое N_1 и N_2 подвергается преобразованию, которое соответствует первым шестнадцати циклам алгоритма в режиме простой замены.

Полученное после шестнадцати циклов содержимое накопителей в N_1 и N_2

суммируются по модулю 2 со вторым блоком открытых данных.

Результат суммирования заносится в накопители N_1 и N_2 и повторяется алгоритм с четвертого шага, только суммирование в шаге 5 происходит со следующим блоком открытого текста и т.д., пока не исчерпается исходное сообщение.

После завершения режима работы выбирается отрезок длиной в 1 бит. Значения параметра l определяется действующими криптографическими требованиями. При этом учитывается, что вероятность навязывания ложных данных равна 2^{-l} .

Практическое занятие № 16. Компьютерная криминалистика

1. Установление принадлежности и расположения IP-адреса

Натуральное число p , больше единицы называется простым, если оно делится нацело только на единицу и на себя.

Теорема (Эвклид). Множество простых чисел бесконечно.

Обозначим через $\pi(x)$ функцию, которая равна числу простых чисел p в интервале $1 < x \leq p$. Российский математик П.Л. Чебышев в 1850г. показал, что имеет место

Простые числа являются важным понятием в криптографии. Многие современные криптографические системы строятся на базе простого числа. Поэтому алгоритмы генерации простых чисел и проверки на простоту сформированного числа в настоящее время являются важными инструментами при создании криптографической системы.

Заметим, что существует около 10151 простых чисел длиной от 1 до 512 бит включительно [5]. Для чисел, близких n , вероятность произвольно выбранному числу оказаться простым числом, равна $(1 / \ln n)$. При случайном выборе двух простых чисел в диапазоне от 1 до 151 бита вероятность совпадения этих чисел ничтожно мала.

Пусть даны два целых числа a и b . Говорят, что число a делит b , если существует такое целое число d , что $b=ad$. Число a в этом случае называют делителем b . Для факта, что a делит b , принято обозначение $a|b$. Справедливы следующие свойства делимости:

если $a|b$ и c – любое число, то $a|(bc)$; если $a|b$ и $b|c$, то $a|c$;

если $a|b$ и $a|c$, то $a|(b \pm c)$.

Здесь уместно сделать замечание, что важную роль в арифметике целых чисел имеет теорема о делении.

Теорема о делении. Для любых целых чисел a и b , $b > 0$, существуют, и притом единственные, целые числа q и r , такие, что

$$a = bq + r, 0 \leq r < b.$$

Определение. Натуральное число p , $p > 1$, называется составным, если число p имеет по крайней мере один положительный делитель, отличный от единицы и p .

Если число p составное, то справедлива следующая теорема.

Теорема. Для любого составного числа наименьший отличный от единицы положительный делитель является простым числом.

Одним из основных утверждений арифметики является факт, что любое натуральное число p можно единственным образом представить в виде произведения простых чисел. Например,

$$4290 = 3 \cdot 2 \cdot 5 \cdot 11 \cdot 13,$$

В общем случае каноническим разложением целого числа a называется представление в виде $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$,

где p_i , $i = 1, 2, \dots, k$, – простые числа. Например, $133100 = 2^2 \cdot 5^2 \cdot 11 \cdot 13$.

Заметим, что, вообще говоря, представление большого числа в канонической записи, т.е. в виде произведения простых сомножителей, является трудной и очень важной задачей в криптографии. Определение. Общим делителем целых чисел

$a_1, a_2, \dots, a_k$

называется любое целое число d , такое, что

$$d|a_1, d|a_2, \dots, d|a_k.$$

Определение. Наибольшим общим делителем (НОД) целых чисел $a_1, a_2, \dots, a_k$ называется такой положительный общий делитель этих чисел, который делится на любой другой делитель этих чисел.

Если d – наибольший общий делитель для чисел a и b , то для него вводится обозначение $(a, b) = d$.

Теорема. Если натуральное число p не делится ни на одно простое число

$$d \leq p,$$

то число p – простое.

Определение. Числа $a_1, a_2, \dots, a_k$ называются взаимно простыми, если наибольший общий делитель этих чисел равен 1.

Определение. Числа $a_1, a_2, \dots, a_k$ называются попарно взаимно простыми, если $(a_i, a_j) = 1, i \neq j, 1 \leq i \leq k, 1 \leq j \leq k$.

Если числа попарно взаимно простые, то все они взаимно простые.

Пример.

Числа 15, 21, 77 – взаимно простые, но эти числа не являются попарно взаимно простыми, потому что $(15, 21) = 3$.

Числа 34, 53, 99, 115 – попарно взаимно простые числа.

Алгоритм Евклида

Для двух целых чисел a и b существует сравнительно быстрый метод вычисления наибольшего общего делителя. Упомянутый метод вычисления наибольшего общего делителя называется алгоритмом Евклида. Приведем схему работы этого алгоритма.

Делим число a на число b , получаем
 $a = bq_0 + r_1$;

Делим число b на число r_1 , имеем
 $b = r_1q_1 + r_2$;

Делим число r_1 на число r_2 , запишем
 $r_1 = r_2q_2 + r_3$;

Делим число r_2 на число r_3 , получаем
 $r_2 = r_3q_3 + r_4$; $r_{t-1} = r_tq_t + r_{t+1}$.

Если остаток от деления $r_{t+1} = 0$, то в этом случае наибольший общий делитель равен числу r_t и алгоритм вычисления наибольшего общего делителя завершается.

Кратко алгоритм Евклида можно сформулировать следующим образом.

Даны два целых числа a и b . Для определенности предположим, что $a > b$. Для поиска наибольшего общего делителя следует выполнить следующие операции.

Разделить a на b . Пусть остаток равен r , $0 < r \leq a$.

Если $r = 0$, то алгоритм завершается, наибольший общий делитель равен b . Положим $a = b$ и $b = r$.

Возвращаемся на шаг 1.

Пример. Найти наибольший общий делитель чисел $a = 1173$ и $b = 323$. Делим число 1173 на число 323, получаем

$$1173 = 323 \cdot 3 + 204;$$

Делим число 323 на число 204, получаем $323 = 204 \cdot 1 + 119$; Делим число 204 на число 119, получаем

$$204 = 119 \cdot 1 + 85;$$

$$\text{Делим число 119 на число 85, получаем } 119 = 85 \cdot 1 + 34;$$

$$\text{Делим число 85 на число 34, получаем } 85 = 34 \cdot 2 + 17;$$

$$\text{Делим число 34 на число 17, получаем } 34 = 17 \cdot 2 + 0;$$

Итак, в итоге получаем $(1173, 323) = 17$.

2. Установление принадлежности доменного имени

Теорема. Пусть d – наибольший общий делитель для a и b , т.е. $d = (a, b)$, где $a > b$.

Тогда существуют такие целые числа x и y , что

$$d = ax + by.$$

Иными словами наибольший общий делитель двух чисел можно представить в виде линейной комбинации этих чисел с целыми коэффициентами.

Схема расширенного алгоритма Евклида

Определить

$$a_0 = 1, a_1 = 0, b_0 = 0,$$

$$b_1 = 1, \alpha = a, \beta = b.$$

Пусть число q – частное от деления числа a на число b , а число r – остаток от деления этих чисел, т.е.

$$a = qb + r.$$

Если остаток от деления r равен нулю, то выполняем шаг 6.

Определяем

$$a = b, b = r, t = a_0, a_0 = a_1,$$

$$a_1 = t - a_1q, t = b_0, b_0 = b_1; b_1 = t - b_1q; \text{ Возвращаемся на шаг 2. 6. Определяем } x = x_0, y = y_0 \quad d = \alpha x + \beta y.$$

Пример. Дано $a = 1769$, $b = 551$. Используя расширенный алгоритм Эвклида, найти целые числа x и y такие, что

$$d = ax + by,$$

где d – наибольший общий делитель чисел a и b . I этап последовательности вычислений

Определить

$$a_0 = 1, a_1 = 0, b_0 = 0, b_1 = 1, \alpha = 1769, \beta = 551.$$

Частное от деления

$$q = a/b = 1769/551 = 3,$$

a остаток от деления $r = 116$.

Если остаток от деления r равен нулю, то выполняем шаг 6.

Определяем

$$a = 551, b = 116, t = a_0 = 1, a_0 = a_1 = 0, a_1 = t - a_1q = 1 - 0 \cdot 3 = 1$$

$$t = b_0 = 0, b_0 = b_1 = 1, b_1 = t - b_1q = -3;$$

В результате текущего шага получили следующие промежуточные значения параметров $a = 551, b = 116, a_0 = 0, a_1 = 1, b_0 = 1, b_1 = -3$.

Так как остаток от деления $r \neq 0$, то возвращаемся на шаг 2.

II этап последовательности вычислений

Значение параметров

$$a = 551, b = 116, a_0 = 0,$$

$$a_1 = 1, b_0 = 1, b_1 = -3.$$

$$\text{Частное от деления } q = a/b = 551/116 = 4,$$

$$-3,$$

a остаток от деления $r = 87$.

Если остаток от деления r равен нулю, то выполняем шаг 6.

Определяем

$$a = 116, b = 87, t = a_0 = 0, a_0 = a_1 = 1, a_1 = t - a_1q = 0 - 1 \cdot 4 = -4, t = b_0 = 1, b_0 = b_1 =$$

$$b_1 = t - b_1q = 1 - (-3) \cdot 4 = 13.$$

В результате текущего шага получили следующие промежуточные значения параметров

$$a = 116, b = 87, a_0 = 1, a_1 = -4, b_0 = -3, b_1 = 13.$$

Так как остаток от деления $r \neq 0$, то возвращаемся на шаг 2. III этап последовательности вычислений

Значение параметров

$$a = 116, b = 87, a_0 = 1, a_1 = -4, b_0 = -3, b_1 = 13.$$

Частное от деления $q = a/b = 116/87 = 1$, a остаток от деления $r = 29$. Если остаток от деления r равен нулю, то выполняем шаг 6.

Определяем

$$a = 87, b = 29, t = a_0 = 1, a_0 = a_1 = -4, a_1 = t - a_1q = 1 - (-4) \cdot 1 = 5; t = b_0 = -3, b_0 = b_1 = 13; b_1 = t - b_1q = -3 - (13) \cdot 1 = -16.$$

В результате текущего шага получили следующие промежуточные значения параметров $a = 87, b = 29, a_0 = -4, a_1 = 5, b_0 = 13, b_1 = -16$.

Так как остаток от деления $r \neq 0$, то возвращаемся на шаг 2.

IV этап последовательности вычислений

Значение параметров

$$a = 87, b = 29, a_0 = -4, a_1 = 5, b_0 = 13, b_1 = -16.$$

Частное от деления $q = a/b = 87/29 = 3$, а остаток от деления $r = 0$. Если остаток от деления r равен нулю, то выполняем шаг 6.

Определяем

$$a = 87, b = 29, \quad t = a_0 = -4, \quad a_0 = a_1 = 5, \quad a_1 = t - a_1q = -4 - 5 \cdot 3 = -19, \quad t = b_0 = 13, \quad b_0 = b_1 = -16,$$

$$b_1 = t - b_1q = 13 - (-16) \cdot 3 = 61.$$

В результате текущего шага получили следующие промежуточные значения параметров $a = 87, b = 29, a_0 = 5, a_1 = -19, b_0 = -16, b_1 = 61$.

Так как остаток от деления $r = 0$, то выполняем шаг 6. 6. Вычисляем наибольший общий делитель по формуле

$$d = \alpha x + \beta y, \text{ где}$$

$$x = x_0 = 5, y = y_0 = -16, \alpha = 1769, \beta = 551.$$

Подставляя значение параметров, получаем

$$d = \alpha x + \beta y = 1769 \cdot 5 - 551 \cdot 16 = 8845 - 8816 = 29.$$

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания
по выполнению самостоятельных работ
по дисциплине «ЭКСПЕРТИЗА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И
КОМПЬЮТЕРНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ»
для студентов специальности 10.05.01 Компьютерная безопасность
специализация «Информационно-аналитическая и техническая экспертиза
компьютерных систем»

Ставрополь
2026

Введение

Целью изучения дисциплины «Экспертиза вычислительной техники и компьютерных носителей информации» является формирование набора общекультурных и профессиональных компетенций по специальности 10. 05. 01 «Компьютерная безопасность», закрепление полученных теоретических знаний, привитие практические навыки по расследованию компьютерных преступлений.

Задачами дисциплины являются:

1. Развитие личности студента, направленное на фундаментализацию образования, формирование его научного мировоззрения и улучшение системного мышления;
2. Освоение системы знаний о методах расследований, необходимых для ориентации в профессии и успешном выполнении задач по обнаружению компьютерных преступлений;
3. Формирование у студентов способности и готовности к сознательному и ответственному действию в сфере отношений, урегулированных нормами права, в том числе обнаружению преступлений и оценке явлений и событий.

Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, практические занятия и самостоятельная работа (СРС).

На лекциях, лабораторных и практических занятиях раскрываются основные положения и понятия курса дисциплины.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к практическим занятиям, завести новую тетрадь для конспектирования лекций и семинарских занятий.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий. В конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и

приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы студентов по учебной дисциплине являются:

самостоятельное изучение учебного материала по заданным темам; подготовка к семинарским занятиям и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;

работа с нормативными документами; поиск информации в Интернет;

2) для закрепления и систематизации знаний:

работа с конспектом лекции (обработка текста); повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);

составление плана и тезисов ответа или графическое изображение структуры ответа;

составление таблиц для систематизации учебного материала; изучение нормативных документов;

ответы на контрольные вопросы; 3) для формирования умений: подготовка к практическим занятиям;

решение задач и практических заданий;

подготовка отчетов по практическим занятиям;

подготовка отчетов по лабораторным занятиям;

рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические занятия, лабораторные работы и контрольные вопросы) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к практическим и лабораторным занятиям.

2. Самостоятельное изучение тем лекций

№п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая	Интернет-ресурсы
1	Самостоятельное изучение руководящих документов по методам расследования правонарушений в области информационных технологий	1 - 3	3,4	1	-
2	Самостоятельное изучение методики расследования преступлений в сфере компьютерной информации	4 - 5	3,4	1	1

3	Самостоятельное изучение методов защиты информации от компьютерных преступлений	1 - 5		1	1
4	Самостоятельное изучение правовой ответственности за совершение компьютерных преступлений	1 - 3	1, 2	1	1
5	Самостоятельное изучение особенностей проведения компьютерно-технической экспертизы	2, 5	2, 4	1	1

3.1. Вопросы для собеседования по практическим занятиям

1. Краткие исторические сведения о преступлениях в области информационных технологий
2. Основные термины и определения
3. Состав компьютерного преступления
4. Виды компьютерных преступлений
5. Субъекты компьютерных преступлений
6. Элементы и признаки состава преступления
7. Объект компьютерных преступлений
8. Признаки объективной стороны компьютерного преступления
- Субъект состава компьютерного преступления
9. Субъективная сторона состава компьютерного преступления
10. Понятие и виды предварительного расследования и следственных действий
11. Понятие и виды следственных действий
12. Допрос свидетеля и потерпевшего. Следственный осмотр
13. Обыск и выемка
14. Назначение и производство экспертизы
15. Следственный эксперимент,
16. Допрос обвиняемого и подозреваемого
17. Особенности образования следов по делам о компьютерных преступлениях
18. Понятие и классификация следов компьютерных преступлений
19. Анализ следов компьютерных преступлений
20. Классификация компьютерных вирусов
21. Основные типы вредоносных объектов, воздействующих на компьютерную систему
22. Особенности начала расследования неправомерного доступа к компьютерной информации
23. Признаки несанкционированного доступа к компьютерной информации

24. Способы преступных манипуляций в сфере компьютерной информации
25. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
26. Создание, использование и распространение вредоносных программ для ЭВМ
27. Способы совершения компьютерных преступлений методом перехват и методом несанкционированного доступа
28. Способы совершения компьютерных преступлений методом манипулирования
29. Понятие и виды предварительного расследования и следственных действий
30. Понятие и виды следственных действий
31. Использование компьютера при совершении компьютерных преступлений
32. Следственный эксперимент, Допрос обвиняемого и подозреваемого
33. Общая характеристика преступлений в сфере компьютерной информации
34. Неправомерный доступ к компьютерной информации
35. Сущность и понятие прокурорского надзора в области компьютерных преступлений
36. Общие и специальные задачи прокурорского надзора в области компьютерных преступлений
37. Требования нормативно-правовая база по организации и проведению служебных расследований в сфере информационных технологий
38. Методы и средства, применяемые для проведения служебных расследований в сфере информационных технологий
39. Особенности применяемых методов и средств в области расследований компьютерных преступлений
40. Особенности документального оформления процедуры служебных расследований в сфере информационных технологий
41. Особенности следов от совершенных преступлений, связанных с НСД к компьютерной информации
42. Методические рекомендации по проведению служебных расследований по вопросам НСД к компьютерной информации
43. Особенности следов от совершенных преступлений, связанных с внедрением и распространением вредоносных компьютерных программ
44. Методические рекомендации по проведению служебных расследований по вопросам внедрения и распространения вредоносных компьютерных программ
46. Особенности следов от совершенных преступлений, связанных с нарушением правил эксплуатации средств обработки компьютерной информации
47. Методические рекомендации по проведению служебных расследований по вопросам нарушения правил эксплуатации средств обработки компьютерной информации

48. Меры и мероприятия, разрабатываемые в организациях в соответствии с требованием законодательства РФ

49. Меры и мероприятия, разрабатываемые в организациях, связанные с утечкой информации по техническим каналам

Список рекомендуемой литературы

5.1. Основная литература

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.

5.2. Дополнительная литература

1. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
4. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

5.3. Методическая литература

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине "Методы расследования правонарушений в области информационных технологий"

5.4. Интернет-ресурсы

1. Правовые справочно-поисковые системы («Гарант», «Консультант Плюс», «Техэксперт»).

5.5. Программное обеспечение: не требуется.