Компьютерные преступления. Ответственность за совершение компьютерных преступлений

Основные пути выявления преступлений

- - в ходе взаимодействия пользователей с компьютерной системой (при эксплуатации программного обеспечения, обмене информацией, использовании данных, проведении проверок и т. д.);
- - в результате проведения регулярных проверочных мероприятий сотрудниками службы безопасности или специалистами по защите информации, состоящими в штате пользователя или провайдера;
- - в ходе встреч оперативных сотрудников с лицами, оказывающими содействие органам, осуществляющим ОРД;
- - в ходе проведения бухгалтерских и иных ревизий;
- - в ходе оперативно-розыскных мероприятий, проводимых правоохранительными органами (проверочная закупка, снятие информации с технических каналов связи, оперативный эксперимент, наведение справок и т.д.);
- - случайно;
- - в ходе расследования преступлений в сфере компьютерной информации;
- - в ходе расследования преступлений иных видов.

Компьютерная информация имеет специфику:

Очень объемна и быстро обрабатываема;

Очень легко и, как правило, бесследно уничтожаема;

Обезличена: между ней и ее разработчиком нет жесткой связи;

Легко передается по каналам связи компьютерных сетей на любое расстояние.

Может создаваться, изменяться, копироваться, применяться только с помощью ПЭВМ при наличии соответствующих устройств чтения машинных носителей информации

Основные причины и условия, способствующие совершению преступлений :

отсутствие контроля за доступом сотрудников, не имеющими полномочий, к АРМ компьютерной сети;

халатность при выполнении требований по использованию СВТ;

низкий уровень прикладного сетевого ПО;

несовершенство парольной защиты, идентификации и аутентификации пользователей;

отсутствие должностного лица, отвечающего за режим безопасности информации в части защиты от НСД;

отсутствие инструкций (контрактов) с сотрудниками по вопросам неразглашения государственной, коммерческой и служебной тайны

отсутствие системы допуска по категориям персонала конфиденциальной информации, в том числе находящейся в электронном виде;

наиболее типичные преступные цели

- подделка счетов и платежных ведомостей;
- приписка сверхурочных часов работы;
- фальсификация платежных документов;
- хищение наличных и безналичных денежных средств;
- вторичное получение уже произведенных выплат;
- перечисление денежных средств на фиктивные счета;
- легализация преступных доходов (путем их дробления и перевода на заранее открытые законные счета с последующим их снятием и многократной конвертацией);
- совершение покупок с фиктивной оплатой (фальсифицированной или похищенной электронной кредитной карточкой);
- незаконные валютные операции;
- незаконное получение кредитов;
- незаконные манипуляции с недвижимостью;
- получение незаконных льгот и услуг;
- продажа конфиденциальной информации;
- хищение материальных ценностей, товаров и услуг, топливно-сырьевых и энергетических ресурсов и т.п.

Кодификатор компьютерных преступлений

В 1991 году кодификатор Генерального Секретариата Интерпола был интегрирован в АС поиска и в настоящее время доступен подразделениям Национальных Центральных Бюро «Интерпола» более чем 100 стран.

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.

QA-Несанкционированный доступ и перехват

QAH -«компьютерный абордаж» (хакинг): несанкционированный доступ в компьютер или компьютерную сеть.

QAI - перехват: несанкционированный перехват информации при помощи технических средств, несанкционированные обращения в компьютерную систему или сеть как из нее, так и внутри компьютерной системы или сети.

QAT - кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты.

QAZ - прочие виды несанкционированного доступа и перехвата.

QD—Изменение компьютерных данных

QDL —логическая бомба: неправомерное изменение компьютерных данных путем внедрения логической бомбы.

QDT - троянский конь: неправомерное изменение компьютерных данных путем внедрения троянского коня.

QDV - вирус: изменение компьютерных данных или программ без права на то, путем внедрения или распространения компьютерного вируса.

QDW - червь: несанкционированное изменение компьютерных данных или программ путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть.

QDZ - прочие виды изменения данных.

QF-Компьютерное мошенничество

QFC - компьютерные мошенничества с банкоматами: 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 с игровыми автоматами: мошенничества и хищения, связанные с игровыми автоматами.

QFM - мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них путем манипуляции программами.

QFP - компьютерные мошенничества с платежными средствами: мошенничества и хищения, связанные с платежными средствами.

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

QFZ - прочие компьютерные мошенничества.

QR —Незаконное копирование

QRG/QRS - незаконное копирование, распространение или опубликование программного обеспечения.

QRT - незаконное копирование топографии полупроводниковых изделий.

QRZ - прочее незаконное копирование.

QS - Компьютерный саботаж

QSH - саботаж с использованием аппаратного обеспечения. **QSS** - компьютерный саботаж программы. **QSZ** - прочие виды саботажа. **QZ**—Прочие компьютерные преступления **QZB** - электронные доски объявлений (BBS). **QZE** - хищение информации, представляющей коммерческую тайну (компьютерный шпионаж). **QZS** - использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера. **QZZ** - прочие компьютерные преступления.

Компьютерные преступления. Ответственность за совершение компьютерных преступлений

компьютерные преступления
(список компьютерных преступлений рекомендованный Комитетом министров Европейского Совета)

A. Компьютерное мошенничество

B. Подделка компьютерной информации

C. Повреждение данных ЭВМ или программ ЭВМ

D. Компьютерный саботаж

E. Несанкциониро-ванный доступ

Минимальный список нарушений

F. Несанкцинированный перехват данных

H. Несанкциониро-ванное воспроизве-дение схем

G. Несанкционированное использование защищенных компьютерных программ

Необязательный Список нарушений

Компьютерный шпионаж

Неразрешенное использование ЭВМ

Изменение данных ЭВМ или программ ЭВМ

Неразрешенное использование защищенной программы ЭВМ

Собственно хакеры

1 группа- **молодежь в возрасте 11—15 лет;**
2 группа- **лица в возрасте 16—25 лет;**
3 группа- **лица в возрасте 26—45 лет**

"Классические " хакеры взлом, для демонстрации своих возможностей

Наемные хакеры

Информационные брокеры делают хакерам заказы на кражу информации, с целью перепродажи

Фрикеры

Метахакеры отслеживают работу хакеров и пользуются результатами их труда

Хакеры-кардеры незаконные операции с кредитными картами

собственно фрикеры бесплатные звонки прослушивание переговоров и перехват сообщений

Кракеры взлом ПАК защиты с целью получения информации, нанесения ущерба

Фрикеры-кардеры подделка карточек с энергонезависимой памятью и смарт-карт

Сетевые кракеры (киберкракеры) вход в АС с использованием уязвимых мест ПО

- **Кардинг** — мошеннические операции с кредитными картами либо банковскими чеками

- Собственно кардинг по схемам кражи денег делится на две категории:

- реальный — создаются физические дубликаты кредитных карт, и деньги потом снимаются с банкомата или в магазине;

- чисто сетевой — все операции проходят в Интернете.

Источники получения информации для изготовления кредитных карт

- **Покупка** информации у другого кардера
- **Фишинг** или, говоря иначе, поддельные сайты, липовая наживка.
- **Взлом интернет-магазина** хакером или подкуп сотрудника данного магазина с целью получения нужной информации.
- С этими данными кардеры легко снимают наличные с чужих счетов.

УК РФ

(ст. 272 УК) Неправомерный доступ к компьютерной информации

(ст. 273) Создание, использование и распространение вредоносных программ для ЭВМ

(ст. 274) Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

(ст.283)) Разглашение гос. тайны
(ст.284) Утрата документов, содержащих гос. тайну

(ст. 183)) Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну

(**ст. 138**) Нарушение тайны переписки, переговоров, почтовых сообщений

Статья 276. Шпионаж

Кодекс РФ об административных правонарушениях

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Статья 13.12. Нарушение правил защиты информации

Статья 13.13. Незаконная деятельность в области защиты информации

Статья 13.14. Разглашение информации с ограниченным доступом

Трудовой кодекс РФ

Статья 89. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя

Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

Временные методические рекомендации по порядку реализации в Гостехкомиссии России Кодекса РФ об административных правонарушениях

28 глава УК -"Преступления в сфере компьютерной информации":

Статья 272 защищает право владельца на неприкосновенность информации в системе.

Преступное деяние должно состоять в НСД к охраняемой законом компьютерной информации, и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств позволяющих преодолеть установленные системы защиты; незаконного применения действующих паролей или маскировка под видом законного пользователя для проникновения в компьютер, хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

Часть 1 лишение свободы **до двух лет**.

Часть 2 - совершение его группой лиц либо с использованием своего служебного положения, - лишение свободы **до пяти лет**.

Статья 273 **защищает права владельца компьютерной системы на неприкосновенность находящейся в ней информации.**

Под созданием вредоносных программам понимаются программы специально разработанные для нарушения нормального функционирования компьютерных программ. Достаточен сам факт создания программ или внесение изменений в существующие программы, заведомо приводящих к негативным последствиям, перечисленным в статье.

Наличие исходных текстов вирусных программ уже является основанием для привлечения к ответственности.

Часть 1 - лишение свободы до **трех лет**.

Часть 2 - предусматривает наступление тяжких последствий по неосторожности. Лицо сознает, что создает вредоносную программу, использует, либо распространяет такую программу или ее носители и либо предвидит возможность наступления тяжких последствий, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение, либо не предвидит этих последствий, хотя при необходимой внимательности и предусмотрительности должно и могло их предусмотреть.

- лишение свободы до **семи лет**

Статья ст. 274. защищает интерес владельца вычисли-тельной системы относительно ее правильной эксплуатации.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред,

Часть 1 -наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок **до пяти лет**, либо обязательными работами на срок от **ста восьмидесяти до двухсот сорока часов**, либо ограничением свободы на срок **до двух лет**.

Часть 2 - То же деяние, повлекшее по неосторожности тяжкие последствия, -наказывается лишением свободы на срок до **четырех лет.**

Кодекс Российской Федерации об административных правонарушениях

- **Статья 13.11.** Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

- Предупреждение или наложение административного штрафа
- на граждан 3-5 МРОТ
- на должностных лиц – 5-10 МРОТ

  на юридических лиц – 50-100 МРОТ

Кодекс Российской Федерации об административных правонарушениях

Статья 13.12. Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области ЗИ (за исключением информации, составляющей гос. тайну),

2. Использование несертифицированных информационных систем, баз и БД, СЗИ , если они подлежат обязательной сертификации (за исключением СЗИ, составляющей гос. тайну),

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и ЗИ, составляющей гос. тайну, созданием средств, предназначенных для защиты информации, составляющей гос. тайну, осуществлением мероприятий и (или) оказанием услуг по ЗИ, составляющей гос.тайну,

4. Использование несертифицированных средств, предназначенных для ЗИ, составляющей гос. тайну,

Должностные лица Гостехкомиссии России имеют право назначать административные наказания в виде административного штрафа:

ч. 1 ст.13.12: на граждан - о т **3** до **5** минимальных размером оплаты труда (МРОТ); на должностных лиц – от **5** до 10 МРОТ; на юридических лиц - от **50** до**100** МРОТ;

ч.**2 ст.13.12:** на граждан - в размере от **5** до **10** МРОТ; на должностных лиц - от **10** до **20** МРОТ; на юридических лиц - от **100** до **200** МРОТ;

ч. 3 ст. 13.12: - на должностных лиц - в размере от **20** до **30** МРОТ; на юридических лиц - от **150** до **200** МРОТ;

ч. 4 ст.13.12: на должностных лиц - в размере от **30** до **40** МРОТ; на юридических лиц - от **200** до **300** МРОТ;

Статья 13.13. Незаконная деятельность в области защиты информации

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна),

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну без лицензии,

Должностные лица Гостехкомиссии России имеют право назначать административные наказания в виде административного штрафа:

ч.1 ст. 13.13: на граждан - в размере от **5** до **10** МРОТ; на должностных лиц - от **20** до **30** МРОТ с конфискацией средств защиты информации или без таковой; на юридических лиц - от **100** до **200** МРОТ;

ч.2 ст. 13.13: на должностных лиц - в размере от **40** до **50** МРОТ; на юридических лиц - от **300** до **400** МРОТ.

Статья 13.14. Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен федеральным законом

Административный штраф:

на граждан – 5-10 МРОТ,

на должностных лиц – 40-50 МРОТ

Статья 283. Разглашение государственной тайны

Часть 1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены -

наказывается арестом на срок от **4** до **6 месяцев** либо лишением свободы на срок до **4 лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Часть 2.. То же деяние, повлекшее по неосторожности тяжкие последствия, -

наказывается лишением свободы на срок от **3** до **7 лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Тяжесть последствий определяется органами следствия и судом в зависимости от обстоятельств совершения преступления (важности разглашенных сведений, адресата, к которому они попали, использования этих сведений адресатом, ущерба от разглашения и т.д.

Статья 284. Утрата документов, содержащих государственную тайну

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, -

наказывается ограничением свободы на срок до **3 лет**, либо арестом на срок от **4** до **6 месяцев**, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Между утратой документов, установленных правил обращения с ними и наступлением тяжких последствий должна обязательно устанавливаться причинная связь.

Основанием для возбуждения уголовного дела служат:

- Заявление о преступлении, поступившее от потерпевшего - от представителя юридического лица или от гражданина (физического лица) - 40%.
- Непосредственное обнаружение признаков преступления органом дознания - 43%:
- - в результате проверки сообщения о совершенном или готовящемся преступлении, поступившего из оперативных источников - 48%;
- - в ходе проведения специальных оперативно-технических мероприятий - 11%;
- - по материалам контрольно-ревизионных и иных документальных проверок - 28%;
- - при задержании лица (лиц) на месте совершения преступления с поличным - 13%.
- Непосредственное обнаружение признаков преступления следователем или прокурором при расследовании уголовных дел о преступлениях других видов - 9%.

При проведении расследования необходимо доказать факт

что компьютерная информация, к которой произведен НСД, охраняется законами РФ

что несанкционированными действиями нарушены права собственника информации

что злоумышленником были осуществлены определенные неправомерные действия

осуществлено НСД к средствам компьютерной техники, либо попытка получения такого доступа

использования злоумышленником полученных денежных средств в своих целях

Залог успешного расследования:

- оперативность действий;

методически правильный подхода к процессу расследования;

умения организовать силы и средства, которыми располагают органы, ведущие борьбу с преступностью

- запоздалое начало уголовного процесса может привести к быстрой, по сравнению с другими видами преступлений:

- утрате важных доказательств,
- безнаказанности преступников,
- увеличению сроков предварительного расследования
- другим негативным последствиям

При решении вопроса о возбуждении уголовного дела допускается ряд тактических просчетов и ошибок:

- Низкое качество проводимой проверки сообщения о преступлении ;
- материалы о преступлении без достаточных оснований и с нарушением всех установленных УПК сроков оседают в органе дознания;
- заявления о преступлениях рассматриваемой категории регистрируются с большим опозданием, а иногда и вовсе не регистрируются.
- успех расследования преступления в обеспечивают:
- быстрота и решительность действий следователя в самые первые часы производства по делу,
- организованное взаимодействие со специализированным органом дознания - отделом "К" Управления специальных технических мероприятий (УСТМ) УВД (ГУВД, МВД) области (края, республики),
- Исключительно важное значение при расследовании преступлений выделенной группы имеют наличие и консультации со специалистами.

Первоначальные следственные действия

Произвести видеозапись, чтобы задокументировать конфигурацию АРМ и рабочего места.

Организовать хранения результатов съемки.

Произвести осмотр, обыскобыск на рабочем месте с целью обнаружения и выемки носителей информации и документов, имеющих отношение к НСД и изменению ПО; принимая при этом меры к обеспечению сохранности информации

Заактировать данные действия.

Произвести опрос специалистов отвечающих за защиту информации, эксплуатацию и ремонт СВТ, сопровождающих системное и прикладное ПО.

Результаты опроса оформить в виде объяснительных записок.

Произвести исследование:

- ✔журналов приложений, безопасности, системы (вход и выход в АРМ ЛВС, действия пользователей - кто что и когда уничтожал и с какого АРМ),
- ✔детальный анализ сбойных ситуаций,
- ✔ контрольных чисел файлов;
- ✔ всего программного обеспечения ЭВМ

Произвести архивацию журналов.

Заактировать данные действия.