Московский университет МВД России
имени В.Я. Кикотя
Московский областной филиал

Кафедра криминалистики

Лекция по дисциплине «Расследование преступлений в сфере компьютерной информации»

Тема 1-2
«Правовые основы и особенности расследования отдельных видов преступлений в сфере компьютерной информации. Планирование и организация деятельности следователя на этапе возбуждения уголовного дела»

План лекции

Вопрос 1. Правовая основа деятельности следователя по противодействию преступлениям в сфере компьютерной информации. Уголовно-правовая характеристика преступлений в сфере компьютерной информации.

Вопрос 2. Криминалистическая характеристика преступлений в сфере компьютерной информации.

Вопрос 3. Особенности возбуждения уголовного дела и организация начального этапа расследования преступлений в сфере компьютерной информации

Вопрос 4.

ВОПРОС 1.
Правовая основа деятельности следователя по противодействию преступлениям в сфере компьютерной информации. Уголовно-правовая характеристика преступлений в сфере компьютерной информации

Уголовная ответственность за преступления в сфере компьютерной информации предусмотрена **главой 28 УК РФ:**

ст. 272. 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. 274.1 Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»

Непосредственный объект - общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ, системы ЭВМ или их сети.

Предмет - **компьютерная информация**, которая с уголовно-правовых позиций *характеризуется следующими обязательными признаками*:

- **всегда является интеллектуальной собственностью;**
- **не обладает натуральными физическими параметрами (вещными свойствами);**
- **охраняется законом;**
- **содержится на машинном носителе, в ЭВМ, системе ЭВМ или их сети.**

Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»

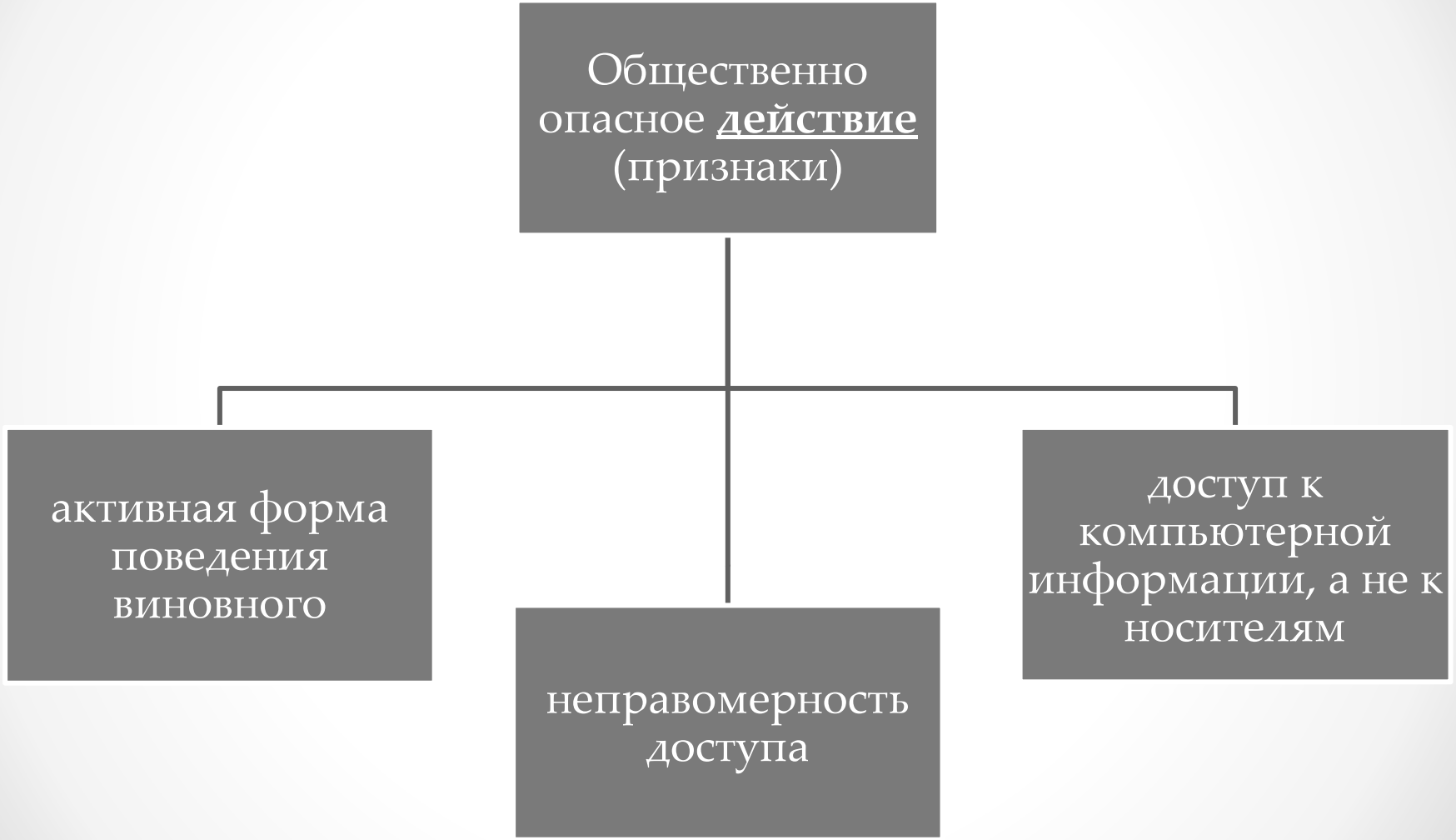
Объективная сторона преступления: неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло *уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети*.

Обязательные признаки неправомерного доступа к компьютерной информации (с его объективной стороны):

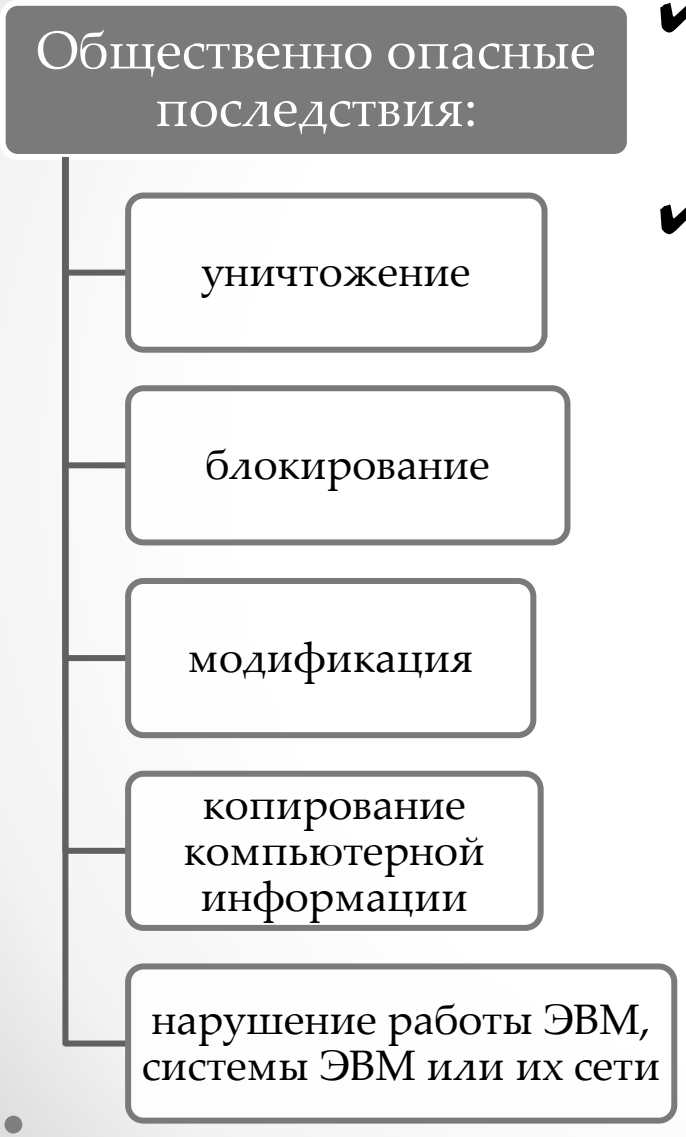
- 1) общественно опасное **действие**;
- 2) общественно опасные **последствия** ;
- 3) **причинная связь** между совершенным деянием и наступившими последствиями.

Отсутствие хотя бы одного из перечисленных признаков означает и отсутствие уголовной ответственности по ст. 272 УК РФ.

Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»



Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»



- ✔ необходимо установить факт переноса указанной информации на другой машинный носитель;
- ✔ несанкционированное **ознакомление** с охраняемой законом компьютерной информацией может выступать в качестве приготовления или покушения на совершение иного умышленного преступления, например незаконного получения и разглашения сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ), шпионажа (ст. 276 УК РФ) и др. В этом случае **дополнительной квалификации по ст. 272 УК РФ не требуется**.

Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»

Нарушение работы ЭВМ, системы ЭВМ или их сети - сбой в работе ЭВМ, системы ЭВМ или их сети, препятствующий нормальному функционированию вычислительной техники при условии сохранения ее физической целостности и требований обязательного восстановления.

В случае, когда неправомерный доступ к компьютерной информации приводит к серьезным повреждениям компьютерной техники и тем самым причиняет **значительный ущерб** собственнику или владельцу, действия виновного, наряду со ст. 272 УК РФ, подлежат **дополнительной квалификации** по ст. 167 УК РФ (умышленное уничтожение или повреждение имущества).

Преступление окончено с момента наступления общественно опасных последствий (материальный состав).

Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»

Вина – необходимый признак субъективной стороны каждого преступления. Мотив и цель совершения неправомерного доступа к компьютерной информации законодатель отнес к числу факультативных признаков.

Как правило, побуждающим фактором к совершению неправомерного доступа к охраняемой законом компьютерной информации является корысть, что, естественно, повышает степень общественной опасности указанного преступления.

Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»

Согласно ст. 20 УК РФ субъектом преступления, предусмотренного ч. 1 ст. 272 УК РФ, может быть любое физическое лицо, достигшее к моменту преступной деятельности 16-летнего возраста.

Составы, смежные со ст. 272 УК РФ

преступления в сфере компьютерной информации: ***создание, использование и распространение вредоносных программ для ЭВМ*** (ст. 273 УК РФ); ***нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети*** (ст. 274 УК РФ);

иные противоправные деяния, предметом посягательства которых может являться компьютерная информация, содержащаяся на машинном носителе, в ЭВМ, системе ЭВМ или их сети: ***нарушение неприкосновенности частной жизни*** (ст. 137 УК РФ), ***нарушение авторских и смежных прав*** (ст. 146 УК РФ), ***незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну*** (ст. 183 УК РФ), и некоторые другие.

Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»

Непосредственный объект преступления - общественные отношения по безопасному использованию ЭВМ, ее программному обеспечению и информационному содержанию.

Предметом преступного посягательства при создании, использовании и распространении вредоносных программ для ЭВМ является компьютерная информация.

Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»

С объективной стороны преступление предусматривает совершение хотя бы одного из следующих действий:

- создание вредоносных программ для ЭВМ;
- внесение изменений в существующие программы для ЭВМ;
- использование вредоносных программ для ЭВМ;
- распространение вредоносных программ для ЭВМ.

Совершить преступление, предусмотренное ст. 273 УК РФ, путем бездействия невозможно.

Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»

Создание вредоносной программы - комплекс операций, состоящих из подготовки исходных данных, предназначенных для управления конкретными компонентами системы обработки данных, в целях, указанных в диспозиции ст. 273 УК РФ. Эта деятельность включает:

- постановку задачи, определение среды существования и цели программы;
- выбор средств и языков реализации программы;
- наладка программы;
- запуск и работу программы.

Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»

Вредоносность или полезность соответствующих программ для ЭВМ определяется в связи с тем, предполагает ли их действие:

- **предварительное уведомление собственника компьютерной информации или другого законного пользователя о характере действия программы,**
- **получение его согласия на реализацию программой своего назначения.**

Нарушение одного из этих требований делает программу вредоносной.

При расследовании уголовных дел по ст. 273 УК РФ признак вредоносности программы устанавливается экспертом при проведении компьютерных судебных экспертиз с учетом выполненных функций определенной программы.

Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»

Внесение изменений в существующие программы – это несанкционированная законным пользователем или собственником программы ее модификация (переработка программы путем изменения, добавления или удаления ее отдельных фрагментов) до такого состояния, когда эта программа способна выполнять новые, изначально не запланированные функции и приводить к последствиям, предусмотренным ч.1 ст. 273 УК РФ.

Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»

Использование вредоносной программы - ее непосредственный выпуск в свет, распространение и иные действия по ее введению в хозяйственный оборот (в том числе в модифицированной форме).

Уголовная ответственность возникает уже в результате создания программы, независимо от того, использовалась программа или нет.

Использованием машинного носителя с вредоносной программой - всякое его употребление с целью использования записанной на нем программы для ЭВМ.

Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»

Распространение программы для ЭВМ – предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей.

Распространение вредоносных программ может осуществляться непосредственно путем их копирования на компьютер потерпевшего, например с дискеты, диска, флеш-карты, а также опосредованно, путем передачи по электронной почте, по линии связи законного пользователя через компьютерную сеть.

Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»

Состав преступления - усеченный.

Не стоит отождествлять понятия вредоносная программа и так называемый компьютерный вирус. «Программы-вирусы» обладают таким обязательным свойством как самовоспроизведение.

Часто создание, использование и распространение вредоносных программ для ЭВМ выступает в качестве способа совершения иного умышленного преступления, например: ***мошенничество*** *(ст. 159 УК РФ);* ***причинение имущественного ущерба путем обмана или злоупотребления доверием*** *(ст. 165 УК РФ);* ***незаконное получение сведений, составляющих коммерческую или банковскую тайну*** *(ст. 183 УК РФ) и др. В этом случае содеянное надлежит квалифицировать по совокупности совершенных преступлений.*

Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»

Субъективная сторона - вина в форме прямого или косвенного умысла.

Факультативными признаками субъективной стороны являются мотивы совершения анализируемого деяния, которыми чаще всего бывают корысть либо хулиганские побуждения, чувство мести, не исключено совершение их с целью сокрытия другого преступления и т.д.

Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»

Субъектом анализируемого состава преступления может быть любое физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста.

Ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»

Часть 2 ст. 273 УК РФ в качестве квалифицирующего признака преступления предусматривает наступление тяжких последствий.

К тяжким последствиям относят: дезорганизацию работы конкретного юридического лица, причинение крупного материального ущерба и т.п.

Специфика квалифицированного состава преступления заключается в том, что оно совершается **с двумя формами вины**, то есть характеризуется ***умыслом*** относительно факта создания, использования или распространения вредоносной программы для ЭВМ и ***неосторожностью*** (легкомыслием либо небрежностью) относительно наступления тяжких последствий.

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

Родовой объект: совокупность общественных отношений, составляющих содержание общественной безопасности и общественного порядка.

Видовой объект: совокупность общественных отношений в части правомерного и безопасного использования компьютерной информации и информационных ресурсов.

Непосредственный объект: общественные отношения в сфере соблюдения установленных правил, обеспечивающих нормальную эксплуатацию ЭВМ, системы ЭВМ или их сети.

Дополнительный объект: факультативный.

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

Диспозиция ст. 274 носит бланкетный характер. В ней же содержится прямое указание на предмет преступного посягательства – *компьютерная информация*.

Объективная сторона преступного нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети состоит из общественно опасного деяния в виде действия или бездействия, наступивших последствий этого деяния, а также причинной связи между ними.

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

Объективная сторона выражается **в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети. Под таковыми правилами понимаются**:

- техническая документация на приобретаемые компьютеры;
- конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка;
- требования по сертификации компьютерных сетей и оборудования;
- должностные инструкции конкретных сотрудников;
- правила пользования компьютерными сетями.

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

Нарушения правил эксплуатации ЭВМ:

физические (неправильное подключение периферийного оборудования, отсутствие устройств бесперебойного питания, нарушение теплового режима в помещении, неправильное подключение ЭВМ к источникам питания, нерегулярное техническое обслуживание, использование несертифицированных средств защиты, самодельных узлов и приборов и пр.)

интеллектуальные (невыполнение процедуры резервного копирования, несанкционированная замена программного обеспечения, параметров настройки системы ЭВМ или компьютерной сети и пр.).

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

Ответственность по ст. 274 УК РФ наступает только в том случае, если преступные последствия, альтернативно отраженные в ее диспозиции, явились именно необходимым следствием, закономерно вызванным неправомерным доступом лица к охраняемой законом компьютерной информации, а не наступили в силу иных причин.

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

Существенный вред - *утрата важной информации, перебои в производственной деятельности, необходимость сложного или длительного ремонта средств вычислительной техники, их переналадки, длительный разрыв связи между ЭВМ*, объединенными в компьютерную сеть, причинение значительного материального ущерба законному пользователю или владельцу информации, а также морального вреда личности путем разглашения сведений конфиденциального характера, составляющих личную, семейную, нотариальную, адвокатскую, врачебную тайну.

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

Под указанными в ч. 2 ст. 274 УК РФ тяжкими последствиями *нарушения правил эксплуатации ЭВМ понимаются безвозвратная утрата особо ценной информации, выход из строя важных технических средств (в том числе оборонного значения, авианавигационной техники), повлекшие аварии, катастрофы, гибель людей.*

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

Субъективную сторону преступления, предусмотренного ч. 1 ст. 274 УК РФ, составляет вина в виде прямого или косвенного умысла. Мотив и цель имеют факультативное значение.

Преступление, предусмотренное ч. 2 ст. 274, совершается *с двойной формой вины*: **умышленной** (в виде прямого или косвенного умысла) по отношению к нарушению правил эксплуатации ЭВМ, их системы или сети и **неосторожной** по отношению к наступившим тяжким последствиям.

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

Субъект анализируемого преступления – **специальный**. Им может быть любое физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста, на которое в силу закона, иного нормативного акта возложена обязанность соблюдения правил эксплуатации ЭВМ.

Закон не требует, чтобы это лицо занимало определенную должность и др. Главное, чтобы оно имело доступ к ЭВМ и было ознакомлено с правилами эксплуатации ЭВМ.

ВОПРОС 2.
Криминалистическая характеристика преступлений в сфере компьютерной информации

Первичное *обнаружение признаков неправомерных действий с компьютерной информацией* посторонними лицами осуществляется, как правило, *пользователями, работающими с конкретными ЭВМ*.

Признаки воздействия на информацию:

1. Изменения структуры файловой системы, а именно:

- переименование папок и файлов, появление новых файлов и папок;
- изменения размеров и содержимого файлов, изменения стандартных реквизитов, присущих данному файлу.

2. Изменения в заданных ранее настройках компьютера, в том числе: картинки и цвета экрана при включении; изменение порядка взаимодействия с периферийными, невозможность работы с имеющимися устройствами и др.

Признаки воздействия на информацию:

3. Необычные проявления в работе ЭВМ:

- замедленная или неправильная загрузка операционной системы;
- замедление реакции машины на ввод с клавиатуры;
- замедление работы машины с дисковыми устройствами (загрузка и запись информации);
- неадекватные реакции ЭВМ на команды пользователя;
- появление на экране нестандартных символов и т.п.

Криминалистическая характеристика преступлений в сфере компьютерной информации

Преступления в сфере компьютерной информации в большинстве случаев **совершаются лицами, имеющими высшее или среднетехническое образование**. По возрастной классификации компьютерных преступников делят на две возрастные категории: первая категория в возрасте от 16 до 20 лет, а вторая в возрасте от 21 года и старше.

Криминалистическая характеристика преступлений в сфере компьютерной информации

Категории лиц, совершающих преступления в сфере компьютерной информации:

- лица, осуществляющие неправомерный доступ к компьютерной информации в группе по предварительному сговору или организованной группой;
- лица, осуществляющие неправомерный доступ к компьютерной информации с использованием своего служебного положения;
- лица, имеющие доступ к ЭВМ, но осуществляющие неправомерный доступ к компьютерной информации или нарушающие правила эксплуатации ЭВМ;
- лица, создающие, использующие и распространяющие вредоносные программы.

Криминалистическая характеристика преступлений в сфере компьютерной информации

Это могут также быть:

лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного *фанатизма* и *изобретательности*;

лица, страдающие *новым видом психических заболеваний* – информационными болезнями или компьютерными фобиями;

профессиональные компьютерные преступники с ярко выраженными корыстными целями.

Криминалистическая характеристика преступлений в сфере компьютерной информации

Хакеры - лица, проникающие в память чужих компьютеров, к сетям передачи данных. При этом преследуются разнообразные цели: от любопытства и удовлетворения тщеславия до получения конкретной выгоды.

Одним из основных внешне поведенческих признаков хакерства является безразличие ко всему, что не имеет непосредственного отношения к работе с компьютером.

У хакеров атрофирована установка на конечный результат, их не интересует полезность и возможность передачи продукта их деятельности в общественное пользование.

Криминалистическая характеристика преступлений в сфере компьютерной информации

Крэкеры – «компьютерные террористы», создающие программы-вирусы и специализирующиеся на проникновении в компьютерные сети и системы с целью овладения конфиденциальной информацией.

Являясь программистами очень высокого класса, в отличие от хакеров, могут стереть или изменить данные в соответствии со своими интересами. В социальном плане крэкеры инфантильны, безответственны.

Мотивами поступков крэкеров могут быть мщение за какую-то нанесенную им обиду, попытка дезорганизовать вычислительные системы своих конкурентов или авторская защита программных продуктов от несанкционированного копирования и распространения.

Криминалистическая характеристика преступлений в сфере компьютерной информации

Общие признаки для указанных подгрупп:

- завышенная оценка своих профессиональных и, как следствие, интеллектуальных способностей;
- использование специфического жаргона не только в кругу специалистов, но и при повседневном общении;
- отсутствие интереса к проблемам повседневной жизни и др.

Особенности, свидетельствующие о совершении компьютерного преступления лицами, входящими в них:

- отсутствие целеустремленной, продуманной подготовки к преступлению;
- оригинальность способа совершения преступления;
- непринятие мер к сокрытию преступления.

Основные способы совершения данных видов преступлений

1. Компьютерный терминал подключается 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.

Основные способы совершения данных видов преступлений

2. К линии связи законного пользователя подключается путем случайного подбора номера абонента компьютерной системы.

Метод «интеллектуального перебора» (подбор предполагаемого пароля, исходя из заранее определенных тематических групп его принадлежности). В этом случае программе-«взломщику» передаются некоторые исходные данные о личности автора пароля.

Основные способы совершения данных видов преступлений

3. К линии связи законного пользователя подключаются, дожидаясь сигнала, обозначающего конец работы, перехватывают его на себя и осуществляют доступ к системе.

4. Несанкционированный доступ к компьютерной системе осуществляется путем нахождения слабых мест в ее защите.

Основные способы совершения данных видов преступлений

5. Производится поиск уязвимых мест компьютерной системы, определяются участки, имеющие ошибку или неудачную логику программного строения.

6. Лицом в найденной «бреши» программа «разрывается», и туда он дополнительно вводит одну или несколько команд.

Основные способы совершения данных видов преступлений

7. Действия лиц направлены на изменение или введение новых данных, которые осуществляются, как правило, при вводе-выводе информации.

8. Незаконное создание копии ключевой дискеты, модификацию кода системы защиты, моделирование обращения к ключевой дискете, снятие системы защиты из памяти ЭВМ и т.п.

Основные способы совершения данных видов преступлений

9. В чужое программное обеспечение тайно вводятся специально созданные программы, которые, попадая в информационно-вычислительные системы, начинают выполнять новые, не запланированные законным владельцем функции, с одновременным сохранением прежней ее работоспособности.

Разновидностями такого способа является внедрение в программы вредоносных программ для ЭВМ, способных 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.

Следовая картина

Следами могут являться какие-либо рукописные записи, распечатки и т.п., свидетельствующие о приготовлении и совершении преступления.

Следы остаются и на самой вычислительной технике (следы пальцев рук, микрочастицы на клавиатуре, дисководах, принтере и т.д.), а также на магнитных носителях и CD-ROM дисках.

Следы могут оставаться и при опосредованном (удаленном) доступе через компьютерные сети, например, через Интернет. Система определяет электронный адрес, используемое программное обеспечение и его версию.

При доступе в сеть обычно вводится адрес электронной почты, реальное имя провайдер для контроля обращений на его сервер, и это также позволяет идентифицировать личность того, кто проникает в сеть.

Криминалистическая характеристика преступлений в сфере компьютерной информации

Орудия преступлений в сфере компьютерной информации - средства компьютерной техники, в том числе и специальное программное обеспечение.

- *к орудиям непосредственного доступа* можно отнести машинные носители информации (накопитель на жестком магнитном диске (винчестер, HDD), перепрограммируемые карты памяти (флеш-карты и другие устройства));
- *к орудиям опосредованного (удаленного) доступа* относится сетевое оборудование (при неправомерном доступе из локальных сетей), а также средства доступа в удаленные сети (средства телефонной связи, модемы).

Криминалистическая характеристика преступлений в сфере компьютерной информации

Способы сокрытия рассматриваемых преступлений:

- при непосредственном доступе сокрытие следов сводится к *воссозданию обстановки*, предшествующей совершению преступления, то есть *уничтожению оставленных следов* (следов пальцев рук, микрочастиц и пр.);
- при опосредованном (удаленном) доступе сокрытие заключается в самом способе совершения преступления, который *затрудняет обнаружение неправомерного доступа*, распространения вредоносных программ. Это достигается применением чужих паролей, идентификационных средств доступа и т.д.

Факторы, способствующие совершению преступлений в сфере компьютерной информации

автоматизация межмашинного обмена информацией, в том числе на больших расстояниях;

низкий уровень прикладного программного обеспечения;

наличие возможности несанкционированного доступа или модификации компьютерной информации;

концентрация компьютерной информации различного назначения и принадлежности в единых базах данных;

Факторы, способствующие совершению преступлений в сфере компьютерной информации

отсутствие надлежащего контроля за доступом к информации;

небрежность пользователей ЭВМ, несоблюдение мер предосторожности;

постоянное увеличение потоков информации, накапливаемой, хранимой и обрабатываемой при помощи компьютеров и других средств автоматизации;

широкий круг пользователей, имеющих доступ к накопителям компьютерной информации, и др.;

высокая степень латентности данного вида преступлений.

Причины и условия высокого уровня латентности преступлений в сфере компьютерной информации

противоправные деяния совершаются по небрежности в силу неосведомленности самого пользователя-правонарушителя об их преступном характере;

потерпевшая сторона не сообщает о противоправном деянии в правоохранительные органы в силу собственной незаинтересованности;

в некоторых противоправных деяниях нет явно выраженной потерпевшей стороны;

противоправные деяния в силу их специфики известны узкому кругу лиц;

отсутствие должного уровня специального образования сотрудников правоохранительных органов, в результате высокий уровень нераскрытых (неполно раскрытых) преступлений в сфере компьютерной информации.

ВОПРОС 3.
Особенности возбуждения уголовного дела и организация начального этапа расследования преступлений в сфере компьютерной информации

Наиболее распространенные **поводы для возбуждения уголовных дел** по ст. 272 УК РФ являются:

- заявление о преступлении в числе которых можно выделить: заявленные должностными лицами от лица организаций и заявления граждан;
- сообщение о совершенном или готовящемся преступлении, полученное из иных источников, а именно: непосредственное обнаружение органом дознания, следователем сведений, указывающих на признаки преступления оформленное рапортом об обнаружении признаков преступления в соответствии со ст. 143 УПК РФ и сообщения о преступлении, распространенные в средствах массовой информации.

При проверке сообщения о преступлении и решении вопроса о возбуждении уголовного дела по ст. 272 УК РФ возможны следующие проверочные ситуации:

1. *Факт неправомерного доступа к компьютерной информации обнаружен законным пользователем этой информации, лицо, совершившее это, не установлено, однако существуют данные, позволяющие установить его*. Это наиболее распространенная проверочная ситуация.

При проверке сообщения о преступлении и решении вопроса о возбуждении уголовного дела по ст. 272 УК РФ возможны следующие проверочные ситуации:

2. *Неправомерный доступ обнаружен при реализации компьютерной информации незаконным пользователем (например, при осуществлении передачи логина и пароля выхода в Интернет)*. Сюда же относится ситуация, когда неправомерный доступ обнаружен в результате того, что лицо, осуществляющее такой доступ, застигнуто на месте преступления.

При проверке сообщения о преступлении и решении вопроса о возбуждении уголовного дела по ст. 272 УК РФ возможны следующие проверочные ситуации:

3. *Имел место неправомерный доступ к компьютерной информации (в наличии иные сведения об этом), однако лицо, его совершившее, не установлено и на этапе проверки сообщения о преступлении нет возможности установить его.*

В стадии возбуждения уголовного дела могут быть истребованы следующие документы и материалы:

1) журнал сбоев в работе компьютерной сети, выхода отдельных компьютеров или технических устройств из строя;

2) журнал учета рабочего времени операторов ЭВМ или компьютеров сети;

3) документы о проведенных в течение дня операциях, например банковских, результаты антивирусных проверок, проверок контрольных сумм файлов и т.п.;

4) физические носители информации и программное обеспечение ЭВМ;

В стадии возбуждения уголовного дела могут быть истребованы следующие документы и материалы:

5) системный блок и выносные накопители информации;

6) информация (в виде файлов) о попытках незаконного использования компьютера, несанкционированного подключения к сети;

7) список лиц, которые имеют право доступа к той или иной компьютерной информации и список паролей, под которыми идентифицированы в компьютере;

8) технические средства опознания пользователей (магнитные карты, ключи блокировки и пр.).

Основные ситуации, в ходе которых выявляются преступления, связанные с созданием, использованием и распространением вредоносных программ:

- в ходе взаимодействия пользователей с компьютерной системой (при эксплуатации программного обеспечения и др.);
- при приобретении программных средств и файлов данных (на машинных носителях информации в торговых точках, по электронной почте и т.д.);
- в ходе оперативных мероприятий, проводимых правоохранительными органами (проверочная закупка, снятие информации с технических каналов связи, оперативный эксперимент и т.д.);
- в ходе расследования иных преступлений в сфере компьютерной информации;
- в ходе расследования преступлений иных видов.

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

Наиболее сложен для изучения является этап возбуждения уголовного дела по признакам преступления, предусмотренного ст. 274 УК РФ, что связано с малым объемом практики расследования данных уголовных дел.

Необходимо знать пути возможного выявления данных преступлений:

- выявление нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети пользователями или собственниками;
- выявление преступлений в ходе расследования иных видов преступлений.

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

У лиц, работавших на ЭВМ и обслуживавших компьютерное оборудование подлежат выяснению следующие вопросы:

- 1. Круг обязанностей лиц, работавших с ЭВМ либо ее оборудованием, какими правилами они установлены.
- 2. Какая конкретно работа на ЭВМ и в каком порядке выполнялась, когда произошло уничтожение, блокирование, изменение компьютерной информации или наступили иные вредные последствия.
- 3. Какие неполадки в компьютерной системе обнаружились при работе на ЭВМ, не было ли при этом каких-либо сбоев, чреватых причинением существенного вреда.

Ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

Продолжение:

- 4. Какие, по его мнению, конкретно правила работы с компьютером были в данной ситуации нарушены.
- 5. Каким образом должны фиксироваться факты уничтожения, блокирования или модификации компьютерной информации в случае нарушения определенных правил эксплуатации ЭВМ.
- 6. Связаны ли уничтожение, блокирование, модификация информации с нарушением правил эксплуатации ЭВМ и каких именно либо они явились следствием непредвиденных обстоятельств.

Особенности подготовительного этапа осмотра места происшествия

После принятия решения о производстве ОМП следователь должен совершить следующие действия:

- 1. принять меры по обеспечению охраны места происшествия до своего прибытия;
- 2. принять меры к предотвращению или ослаблению вредных последствий компьютерного преступления;
- 3. обеспечить к моменту своего прибытия присутствие лиц, которые могут дать необходимую информацию о происшествии;
- 4. обеспечить присутствие специалистов на инструктаже следственно-оперативной группы;

Особенности подготовительного этапа осмотра места происшествия

Продолжение:

- 5. поручить специалистам проверить готовность программно-технических средств.
- 6. проконсультироваться со специалистами самому и обязать специалистов проинструктировать всех лиц, участвующих в осмотре места происшествия о порядке работы на месте происшествия.
- 7. обеспечить участие понятых.

По прибытии на место происшествия следователь должен:

1. Удалить с места происшествия всех посторонних лиц и предупредить появление таких лиц.

2. Выявить лиц, побывавших на месте происшествия до приезда СОГ, а также установить изменения, внесенные ими в обстановку.

3. Собрать путем беседы с сотрудниками потерпевшей организации либо с потерпевшими физическими лицами предварительные сведения.

4. Оценить возможность доступа посторонних лиц в помещения, в которых находятся критичные к несанкционированному доступу электронные устройства.

По прибытии на место происшествия следователь должен:

5. Выяснить порядок протоколирования доступа к информации, а так же каким образом и кем ведется администрирование сети.

6. Определить, соединены ли находящиеся в помещении компьютеры в локальную вычислительную сеть, и установить, имеются ли соединения компьютера с оборудованием или вычислительной техникой вне осматриваемого помещения.

7. Установить наименование используемого телекоммуникационного оборудования, его характеристики; наименование используемых средств электронной почты.

8. Определить, запущены ли программы на ЭВМ, и какие именно.

Особенности рабочего этапа осмотра места происшествия (правила)

1. Запрещено производить какие-либо действия с машинными носителями информации и компьютерной информацией, содержащейся на них, если результат таких действий заранее не известен.

2. Необходимо ограничить использование в ходе следственного действия или отказаться от применения технико-криминалистических средств, принцип работы которых основан на использовании магнитных полей, электромагнитного, рентгеновского, ультрафиолетового и иных излучений.

Особенности рабочего этапа осмотра места происшествия (правила)

3. Соблюдать осторожности при работе с порошками и химическими реактивами, использующимися для выявления и фиксации следов и посторонних наложений, не допускать их попадания на рабочие поверхности машинных носителей информации, в разъемы, устройства работы со съемными машинными носителями информации и т.д.

4. Использовать при фиксации характеристик и процесса функционирования компьютерных систем специальную терминологию.

Особенности рабочего этапа осмотра места происшествия (правила)

5. Использовать при осмотре компьютерной информации, хранящейся на машинном носителе, общих правил осмотра и описания: от общего к частному, от каталогов к отдельным файлам, от общих характеристик свойств файла к его конкретному содержанию.

6. Проводить максимально подробную фиксацию внешнего вида элементов компьютерной системы, информации, имеющейся на машинных носителях, и содержания компьютерной информации, следуя правилу относимости информации к расследуемому преступлению.

Особенности рабочего этапа осмотра места происшествия (правила)

7. Использовать в ходе проведения осмотров средств компьютерной техники сертифицированного программного обеспечения и аппаратно-технических средств.

8. Изыматься должны только те средства компьютерной техники, на которых содержится или может содержаться криминалистически значимая информация.

Особенности рабочего этапа осмотра места происшествия

- При осмотре места происшествия следует применять ***концентрический способ*** (от периферии к центру, где находится самый важный объект (объекты) – сетевой сервер (серверы) предприятия).
- Специалистом производится подключение своего ноутбука к сети или ЭВМ пострадавшего для проведения *антивирусного тестирования системы*.
- Специалист проводит тестирование персональных компьютеров и сети на предмет обнаружения вредоносных программ.
- С целью получения образцов для последующего сравнительного исследования (файлов) необходимо произвести полное ***резервное копирование файлов*** сетевой среды на внешние носители информации.

Особенности рабочего этапа осмотра места происшествия

Определенные в результате тестирования зараженные файлы не должны «вылечиваться». Факты обнаружения вредоносных программ только фиксируются, а зараженные файлы в дальнейшем будут переданы эксперту для дальнейшего исследования с целью установления:

- групповой принадлежности обнаруженных вирусов;
- распространенности в сетевых средах других организаций;
- вредоносных последствий использования;
- оценки даты их написания и степени квалификации лица, создавшего и (или) внедрившего данный программный код.

Особенности производства допроса при расследовании преступлений в сфере компьютерной информации

- ✔ свидетелями чаще всего выступают лица с высшим образованием, обладающие высоким интеллектом, в совершенстве владеющие специальной терминологией;
- ✔ может быть приглашен специалист в области вычислительной техники (необходимо предварительное согласование с ним формулировок задаваемых вопросов).

Особенности производства допроса при расследовании преступлений в сфере компьютерной информации

Основными тактическими задачами допроса потерпевших и свидетелей при расследовании дел рассматриваемой категории являются:

- выявление элементов состава преступления в наблюдавшихся ими действиях,
- установление обстоятельств, места и времени совершения значимых для расследования действий, способа и мотивов его совершения и сопутствующих обстоятельств,

Особенности производства допроса при расследовании преступлений в сфере компьютерной информации

Продолжение:

- признаков внешности лиц, участвовавших в нем,
- определение предмета преступного посягательства,
- размера причиненного ущерба,
- детальные признаки похищенного,
- установление свидетелей и лиц, причастных к совершению преступления.

Для решения указанных задач в процессе допроса свидетеля необходимо выяснить:

1. Не проявлял ли *кто-либо интереса* к компьютерной информации, программному обеспечению, компьютерной технике данного предприятия, организации, учреждения, фирмы или компании?

2. Не появлялись ли в помещении, где расположена компьютерная техника, *посторонние лица*, не зафиксированы ли случаи работы сотрудников с информацией, не относящейся к их компетенции?

3. Не было ли *сбоев в работе программ*, хищений носителей информации и отдельных компьютерных устройств?

Для решения указанных задач в процессе допроса свидетеля необходимо выяснить:

4. Зафиксированы ли *сбои* в работе компьютерного оборудования, электронных сетей, средств защиты компьютерной информации?

5. Как часто *проверяются* программы на наличие вирусов, каковы результаты последних проверок?

6. Как часто *обновляется* программное обеспечение, каким путем, где и кем оно приобретается?

7. Каким путем, где и кем *приобретается* компьютерная техника, как осуществляется ее *ремонт и модернизация*?

Для решения указанных задач в процессе допроса свидетеля необходимо выяснить:

8. Каков на данном объекте *порядок работы с информацией*, как она поступает, обрабатывается и передается по каналам связи?

9. Кто еще является *абонентом* компьютерной сети, к которой подключены компьютеры данного предприятия, организации, учреждения или фирмы, каким образом осуществляется доступ в сеть, кто из пользователей имеет право на работу в сети, каковы их полномочия?

10. Как осуществляется *защита компьютерной информации*, применяемые средства и методы защиты и др.?

Для решения указанных задач в процессе допроса свидетеля необходимо выяснить:

11. Могли ли возникшие последствия стать результатом *неосторожного* действия лица или неисправности работы ЭВМ, системы ЭВМ, сбоев программного обеспечения и т.п.?

12. Каков *характер изменений* информации?

13. Кто является *собственником* (владельцем или законным пользователем) скопированной (уничтоженной, модифицированной, блокированной) информации и др.?

Особенности допроса

В процессе допросов **операторов ЭВМ** следует выяснить:

- правила ведения журналов операторов, порядок приема-сдачи смен, режим работы операторов, порядок идентификации операторов;
- правила эксплуатации, хранения, уничтожения компьютерных распечаток (листингов), категорию лиц, имеющих к ним доступ;
- порядок доступа в помещение, где находится компьютерная техника, категорию работников, допущенных к работе с ней, и др.

Особенности допроса

В процессе допроса **программистов** выясняется:

- перечень используемого программного обеспечения и его классификации (лицензионное, собственное), пароли защиты программ, отдельных устройств компьютера, частота их смен;
- технические характеристики компьютерной сети, кто является администратором сети; порядок приобретения и сопровождения программного обеспечения;
- наличие в рабочих программах специальных файлов-протоколов, регистрирующих вхождение компьютеров пользователей, каково их содержание и др.

Особенности допроса

У **сотрудника, отвечающего за информационную безопасность**, *или* **администратора компьютерной сети** выясняется:

- наличие специальных технических средств защиты информации;
- порядок доступа пользователей в компьютерную сеть;
- порядок идентификации пользователей компьютеров, распорядок рабочего дня пользователей компьютерной сети;
- порядок доступа сотрудников к компьютерной технике во внерабочее время, порядок присвоения и смены паролей пользователей;
- характеристика мер по защите информации.

Особенности допроса

У **сотрудников, занимающихся техническим обслуживанием вычислительной техники,** выясняется:

- перечень и технические характеристики средств компьютерной техники, установленных в организации, а также перечень защитных технических средств, периодичность технического обслуживания, проведения профилактических и ремонтных работ;
- сведения о произошедших в последнее время случаях выхода аппаратуры из строя;
- случаи незаконного подключения к телефонным линиям связи, установка какого-либо дополнительного электрооборудования.

Особенности допроса

У начальника вычислительного центра или руководителей предприятия (организации) следует выяснить:

- действуют ли в учреждении специальные службы по эксплуатации сетей и службы безопасности, их состав и обязанности;
- сертифицированы ли программы системной защиты;
- организационную структуру вычислительного центра;;
- действуют ли внутриведомственные правила эксплуатации ЭВМ и сети, каков порядок ознакомления с ними и контроля за их исполнением;
- какие сотрудники учреждения (организации) были уволены в течение интересующего периода времени и по каким мотивам;
- были ли ранее случаи незаконного проникновения в помещение и несанкционированного доступа к компьютерной информации, вирусных атак и др.

Особенности допроса

У руководителя организации, работника юридического отдела или иного лица, уполномоченного представлять интересы потерпевшего юридического лица выясняется:

- стаж работы в должности;
- основания для представления интересов организации в правоохранительных органах;
- откуда стало известно о произошедшем;
- излагаются обстоятельства, ставшие известными представителю потерпевшего;
- выясняются лица, могущие разъяснить следователю технические вопросы, возникающие при расследовании уголовного дела;
- правовая регламентация статуса информации, подвергшейся воздействию в результате преступления.

Особенности допроса очевидцев преступления

Должно быть выяснено:

- 1. При каких обстоятельствах свидетель наблюдал преступников (процесс совершения преступления)?
- 2. В чем состоял способ совершения преступления?
- 3. Какую роль выполнял каждый из соучастников неправомерного доступа к компьютерной информации?
- 4. Знает ли свидетель, какую цель преследовал обвиняемый, совершая неправомерный доступ к компьютерной информации?
- 5. Имели ли место подобные проявления ранее, если да, то как на них реагировали руководители предприятия, организации, учреждения, фирмы, компании?
- 6. Как свидетель характеризует обвиняемого и его окружение?
- 7. Что способствовало совершению преступления?