МИНИСТЕРСТВО ОБРАЗОВАНИЯ и НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

В.М. Алексеев

«Преступления в информационной сфере»

Учебно-методическое пособие для выполнения практических занятий
по части 1 дисциплины «Организационное и правовое обеспечение информационной безопасности»

Пенза 2024

ЦЕЛЬ И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

При проведении данного цикла практических занятий происходит закрепление и углубление знаний по правовому обеспечению информационной безопасности и выработка практических навыков деятельности специалиста по защите информации по экспертизе компьютерных преступлений.

Порядок проведения занятий:

При подготовке к занятию студенты изучают в соответствии с указаниями преподавателя необходимую литературу. Затем студенты, разбившись на бригады, выполняют задания и оформляют отчет.

Во время проведения занятия студенты защищают отчеты о выполнении практического занятия, делая доклад, и отвечая на вопросы преподавателя и других студентов группы. Отчет, доклад и ответы на вопросы оцениваются преподавателем. Отчеты подлежат размещению в специальном разделе ЭИОС по данной дисциплине.

Тема 1. Понятие и характеристика компьютерного преступления. Состав преступления. Психологический портрет компьютерного преступника

Изучаемые учебные вопросы:

- понятие компьютерного преступления в российском законодательстве;
- уголовно-правовая характеристика компьютерных преступлений;
- криминалистическая характеристика компьютерных преступлений.

Цель занятия: практическое занятие имеет целью закрепление знания студентами основных положений и правовых норм в области компьютерных преступлений

Содержание занятия:

Студенты:

- изучают положения статей 272,273,274 Уголовного Кодекса Российской Федерации в области информационной безопасности, а также- сведения по уголовно-правовому анализу указанных статей;
- выполняют контрольное задание,
- защищают отчет.

Понятие компьютерного преступления в российском законодательстве

Специалисты относят к компьютерным те преступления, у которых объектом преступного посягательства является информация , обрабатываемая и хранящаяся в компьютерных системах, а орудием посягательства служит компьютер.

В соответствии с классификацией Организации экономического и социального развития выделяются следующие группы компьютерных преступлений:

экономические преступления;

преступления против личных прав и частной сферы;

преступления против государственных и общественных интересов.

Экономические компьютерные преступления совершаются по корыстным мотивам и включают в себя компьютерное мошенничество, кражу программ, услуг и машинного времени, экономический шпионаж.

Компьютерным преступлением против личных прав и частной сферы является незаконный сбор данных о лице, разглашение персональных данных, врачебной тайны, незаконное получение информации о расходах.

Компьютерные преступления против государственных и общественных интересов включают преступления, направленные против государственной и общественной безопасности, угрожающие обороноспособности государства, злоупотребления с государственной автоматизированной системой «Выборы» и т.п.

Подходить к классификации компьютерных преступлений наиболее оправданно с позиций составов преступлений, которые могут быть отнесены к разряду компьютерных. Хотя состав компьютерных преступлений в настоящее время четко не определен, можно выделить ряд видов противоправных деяний, которые могут быть в него включены.

Перечислим некоторые основные виды преступлений, связанных с вмешательством в работу компьютеров:

1) *несанкционированный доступ в корыстных целях к информации, хранящейся в компьютере или информационно-вычислительной сети.* Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных. Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т.п.), оказываются беззащитны против этого приема. Самый простой путь его осуществления — получить коды и другие идентифицирующие шифры законных пользователей. Несанкционированный доступ может осуществляться и в результате системной поломки. Например, если некоторые файлы одного

пользователя остаются открытыми, то другие пользователи могут получить доступ к не принадлежащим им частям банка данных;

2) *разработка и распространение компьютерных вирусов*;

3) *ввод в программное обеспечение «логических бомб».* Это такие программы, которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему;

4) *халатная небрежность при разработке, создании и эксплуатации программно-вычислительных комплексов компьютерных сетей, приведшая к тяжким последствиям.* Особенностью компьютерных систем является то, что абсолютно безошибочных программ в принципе не бывает;

5) *подделка и фальсификация компьютерной информации.* Этот вид компьютерной преступности является одним из наиболее распространенных. Он является разновидностью несанкционированного доступа с той лишь разницей, что пользоваться им может сам разработчик, причем имеющий достаточно высокую квалификацию. Идея преступления состоит в подделке выходной информации с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К фальсификации информации можно отнести также подтасовку результатов выборов, референдумов и т. п. Если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы. Естественно, что подделка информации может преследовать и другие, в том числе корыстные, цели;

6) *хищение программного обеспечения.*;

7) *несанкционированное копирование, изменение или уничтожение информации.* При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны;

8) *несанкционированный просмотр или хищение информации из банков данных, баз данных и баз знаний.*

Парадоксальная особенность компьютерных преступлений состоит и в том, что трудно найти другой вид преступления, после совершения которого его жертва не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность на поприще компьютерного взлома, мало что утаивая от представителей правоохранительных органов. Психологически этот парадокс вполне объясним. Во-первых, жертва компьютерного преступления совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты своей репутации) существенно превосходят уже причиненный ущерб. И, во-вторых, преступник приобретает широкую известность в деловых и криминальных кругах, что в дальнейшем позволяет ему с выгодой использовать приобретенный опыт.

Понятие состава преступления

Состав преступления - это система обязательных объективных и субъективных элементов, образующих и структурирующих общественно опасное деяние, признаки которых описаны в диспозициях уголовно-правовых норм Общей и Особенной частей УК.

Как всякая система состав преступления охватывает целостное множество подсистем и элементов. Подсистем в составе четыре: объект, субъект, объективная и субъективная стороны (подсистемы) состава преступления. Отпадение хотя бы одного обязательного элемента, а тем более подсистемы приводит к распаду всей системы состава преступления, к его отсутствию в деянии лица.

Элементы состава преступления представляют собой компоненты состава. Они подразделяются на обязательные и факультативные (см. 2 данной главы). Первые образуют составы всех преступлений. Вторые - лишь некоторых. Признаки элементов составов преступлений определяют их специфику, позволяют отграничить один состав преступления от другого, а также размежевать преступления от непреступных правонарушений. Признаки элементов и подсистем составов преступлений представлены в диспозициях норм Общей и Особенной частей УК.

Статья 8 УК РФ устанавливает: "Основанием уголовной ответственности является совершение деяния, содержащего все признаки состава преступления, предусмотренного настоящим Кодексом". Определив главную функцию состава преступления - быть основанием уголовной ответственности, УК не раскрывает понятия состава. Его можно вывести только путем толкования ст. 8 и тех статей, которые употребляют термин "состав преступления".

О составе преступления, как содержащемся в деянии и служащим основанием уголовной ответственности, говорит и УПК. Например, ч. 2 ст. 5 устанавливает, что уголовное дело не возбуждается, а возбужденное подлежит прекращению "за отсутствием в деянии состава преступления". Статья 309 предписывает вынесение оправдательного приговора, "если в деянии подсудимого нет состава преступления". И УК и УПК говорят о составе как содержащемся в деянии. Как правило, УК оперирует понятиями не "состав преступления", а "преступление" или "деяние". Состав упоминается лишь в нормах о добровольном отказе и деятельном раскаянии, когда речь заходит об освобождении от уголовной ответственности, если в деянии не содержится "иного состава преступления". Например, в ч. 3 ст. 31 УК сказано, что "лицо, добровольно отказавшееся от доведения преступления до конца, подлежит уголовной ответственности лишь в том случае, если фактически совершенное им деяние содержит иной состав преступления". Примечание к ст. 206 УК о захвате заложника устанавливает: "Лицо, добровольно или по требованию властей освободившее заложника, освобождается от уголовной ответственности, если в его действиях не содержится иного состава преступления".

Состав преступления - это система обязательных объективных и субъективных элементов деяния, образующих его общественную опасность и структурированных по четырем подсистемам, признаки которых предусмотрены в диспозициях уголовно-правовых норм Общей и Особенной частей УК. Как система, т.е. целостное единство множества (а не просто совокупность), состав преступления слагается (составляется) из ряда взаимосвязанных подсистем и их элементов. Отсутствие хотя бы одной подсистемы или элемента состава преступления приводит к распаду системы, т.е. отсутствию состава преступления в целом.

Элементы" состава преступления - это компоненты, первичные слагаемые системы "состав преступления". Они входят в четыре подсистемы состава: объект, объективная сторона, субъект, субъективная сторона. Элементы состава бывают обязательными и факультативными

Подсистема "объект" как объект преступления и объект уголовно-правовой охраны включает в себя общественные отношения, социальные интересы. Их перечень дается в ст. 1 УК о его задачах, в наименованиях разделов и глав Особенной части Кодекса. Таковы интересы личности, ее здоровье, социальные права, политические и экономические интересы государства и общества, правопорядок в целом. Объект описывается помимо наименований глав и статей в Особенной части УК, также через характеристику предмета посягательства и ущерба. Ущерб представляет собой вредные, антисоциальные изменения в объектах посягательства и потому характер объекта и ущерба тесно взаимосвязаны. Например, диспозиция нормы о краже говорит о тайном похищении чужого имущества. Описание предмета кражи дает информацию об объекте кражи - чужой собственности. Заголовок гл. 21 "Преступления против собственности" прямо характеризует объект уголовно-правовой охраны. Наиболее общая характеристика объектов посягательства, принятая в УК 1996 г. - "охраняемые уголовным законом интересы". Конечно, в состав преступления входит не весь объект целиком, а лишь та его часть, которая подверглась вредным изменениям в результате посягательства. Сами по себе правоохраняемые интересы не могут быть подсистемами ни преступления, ни его состава.

Подсистема состава "объективная сторона" включает в себя элементы с описанными в диспозициях уголовного закона признаками деяния, т.е. действия и бездействия, посягающего на тот или иной объект и причиняющего ему вред (ущерб). К ней относятся также атрибуты внешних актов деяния - место, способ, обстановка, орудия совершения преступления.

Подсистема состава "субъект преступления" описывает такие признаки, как физические свойства лица, совершившего преступление - его возраст, психическое здоровье (вменяемость). В некоторых составах субъектом преступления выступает специальное лицо, например, должностное, военнослужащий.

Наконец, четвертая, последняя подсистема состава - "субъективная сторона" - включает такие элементы, как вина, мотив, цель, эмоциональное состояние (например, аффект).

Все четыре подсистемы с более чем дюжиной элементов состава преступления органически взаимосвязаны и взаимодействуют. Объект взаимодействует с объективной стороной состава через элемент в виде ущерба. Объективная сторона как акт поведения взаимодействует с субъектом преступления, ибо именно он совершает то или иное действие или бездействие, причиняющее вред объекту. Субъективная сторона взаимосвязана с объективной, ибо само поведение мотивированно и целенаправленно в изначальном психологическом его свойстве, а содержание объективной стороны входит в содержание вины-предвидения и психического отношения к конкретному деянию, его определенной общественной опасности.

Уголовно-правовая характеристика компьютерных преступлений

Глава 28 УК РФ определяет общественно опасные деяния, совершаемые с использованием средств компьютерной техники:

- ст.272 – Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации;
- ст.273 – Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;
- ст.274 – Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

УК РФ содержит понятие «компьютерная информация», под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

С точки зрения уголовно-правовой охраны под компьютерными преступлениями понимаются те предусмотренные уголовным законом общественно опасные деяния, в которых машинная информация является предметом преступного посягательства. В качестве орудия совершения преступления может выступать машинная информация, компьютер, компьютерная система или компьютерная сеть.

(Преступления, имеющие своим предметом только лишь аппаратно-технические средства ЭВМ (уничтожение, хищение) подпадают под

уголовные правонарушения, предусмотренные главой 21 УК РФ “Преступления против собственности”.)

Глава 28 УК РФ имеет своей целью охрану именно информационной безопасности и только в силу этого защиту и аппаратно-технических средств, которые являются материальными носителями информационных ресурсов. Последствия неправомерного использования информации могут быть самыми разнообразными: нарушение неприкосновенности интеллектуальной собственности, разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений нормальной деятельности предприятия, отрасли и т.д. Поэтому совершенно оправданно то, что преступления данного вида помещены в раздел «Преступления против общественной безопасности и общественного порядка».

Таким образом, общим объектом компьютерных преступлений выступает совокупность всех общественных отношений, охраняемых уголовным законом; родовым — общественная безопасность и общественный порядок; видовым — совокупность общественных отношений по правомерному и безопасному использованию информации; а непосредственный объект трактуется, исходя из названий и диспозиций конкретных статей. Чаще всего непосредственный объект основного состава компьютерного преступления сформулирован альтернативно, в квалифицированных составах количество их, естественно, увеличивается.

Машинная информация может являться и средством преступного посягательства, когда компьютерная техника используется с целью совершения другого противоправного посягательства на иной объект. Разработчики УК РФ сформулировали в главе 28 составы преступлений таким образом, что машинная информация в каждом случае является лишь объектом преступного посягательства.

Однако при использовании машинной информации в качестве средства совершения другого преступления отношения по ее охране страдают неизбежно, т.е. она сама становится предметом общественно опасного деяния. Невозможно противоправно воспользоваться информацией, хранящейся в ЭВМ, не нарушив при этом ее защиты, т.е. не совершив одного из действий, предусмотренных в Федеральном законе «Об информации, информационных технологиях и о защите информации». Таким образом, даже при совершении такого преступления, как электронное хищение денег, ответственность должна наступать по правилам идеальной совокупности преступлений.

Нельзя не признать, что уничтожение, блокирование, модификация и копирование информации не исключают совершения самостоятельных действий. В литературе указывается, что правильнее было бы рассматривать основанием уголовной ответственности за неправомерный доступ к компьютерной информации случаи, когда неправомерный доступ сопряжен с

уничтожением, блокированием и т. д., т. е. такому доступу следовало бы придать значение не только причины , но и необходимого условия[1].

В силу ч. 2 ст. 9 УК РФ временем совершения каждого из преступлений будет признаваться время окончания именно деяния независимо от времени наступления последствий. Сами же общественно опасные деяния чаще всего выступают в форме действий и лишь иногда — как бездействие. В одном случае такой признак объективной стороны состава преступления, как способ его совершения, сформулирован в качестве обязательного признака основного и квалифицированного составов. В остальных случаях этот признак, а также время, место, обстановка, орудия, средства совершения преступления могут быть учтены судом в качестве смягчающих или отягчающих обстоятельств.

Из всех признаков субъективной стороны значение будет иметь только один — вина. Для всех преступлений данного вида необходимо наличие вины в форме умысла, и лишь два квалифицированных состава преступлений предусматривают две ее формы: умысел по отношению к деянию и неосторожность в отношении наступивших общественно опасных последствий. Факультативные признаки субъективной стороны, так же как и в вопросе о стороне объективной, не будут иметь значения для квалификации преступления.

Мотивами совершения деяний чаще всего бывают корысть либо хулиганские побуждения, но могут быть и соображения интереса, чувство мести; не исключено совершение их с целью скрыть другое преступление и т.д. Естественно, что особую трудность вызывает проблема неосторожного причинения вреда, что связано с повышенной сложностью и скрытностью процессов, происходящих в компьютерных системах и сетях.

Субъект нескольких составов является специальным. В остальных случаях им может стать в принципе любой человек, особенно если учесть растущую компьютерную грамотность населения.

Общим объектом компьютерных преступлений выступает совокупность всех общественных отношений, охраняемых уголовными законами, родовым – общественная безопасность и общественный порядок, ведомым – совокупность общественных отношений по правомерному и безопасному использованию информации, а непосредственный объект трактуется, исходя из названий и диспозиций конкретных статей. Почти все составы преступлений главы 28 конструктивно сформулированы как материальные, поэтому предполагают не только совершение общественно опасного деяния, но и наступление общественно опасных последствий, а также установление причин и связи между этими двумя признаками. В силу ч.2 ст.9 УК РФ временем совершения каждого из преступлений будет признаваться время окончания именно деяния независимо от времени

---

[1] **Уголовное право: Особенная часть: Учебник / Под ред. И.Я.Козаченко. — М., 1997.**

наступления последствий. Сами общественно опасные деяния чаще всего выступают в форме действий, и лишь иногда как бездействие. В одном случае такой признак объективной стороны состава как способ его совершения сформулирован в качестве обязательного признака основного и квалифицированного составов. В остальных случаях это признак, а также время, место, обстановка, орудие, средства совершения преступления могут быть учтены судом в качестве смягчающих или отягчающих обстоятельств. Из всех признаков субъективной стороны значение будет иметь только один – вина. Для всех преступлений данного вида необходимо наличие вины в форме умысла, и лишь два квалифицированных состава преступления предусматривают две её формы: умысел по отношению к деянию и неосторожность в отношении наступивших общественно опасных отношений. Мотивами совершения деяний чаще всего являются корысть, хулиганские побуждения, но могут быть и соображения интереса, чувство мести, желание скрыть другое преступление. Естественно, что особую трудность вызывает проблема неосторожного причинения вреда, что связано с повышенной сложностью и скрытностью процессов, происходящих в компьютерных системах и сетях.

Субъект нескольких составов является специальным. В остальных случаях им может стать в принципе любой человек, особенно если учесть растущую компьютерную грамотность населения.

Рассмотрим уголовно-правовой анализ статей главы 28.

Статья 272 УК РФ Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, - наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех

лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

1. Общественная опасность преступлений в сфере компьютерной информации состоит в том, что неправомерный доступ к информации, повлекший ее уничтожение, блокирование, модификацию, копирование, нарушение работы ЭВМ, их систем и сетей, может нарушить деятельность различных систем автоматизированного контроля и управления объектами жизнеобеспечения, энергетики, обороны, транспорта, повлечь не только значительный материальный ущерб, но и причинение вреда здоровью людей, их гибель.

Преступность в сфере высоких технологий (киберпреступность) является серьезной угрозой национальной безопасности РФ. Она приобрела характер транснациональной организованной преступности, о чем отмечено в Бангкокской декларации по результатам XI Конгресса ООН 2005 г. В Конвенции о преступности в сфере компьютерной информации (Будапешт, 2001 г., с Дополнительным протоколом, в котором Россия не участвует) не только государства - члены Совета Европы, но и другие признали необходимость проведения в приоритетном порядке общей политики в сфере уголовного права, нацеленной на защиту общества от преступности в сфере компьютерной информации.

В целях обеспечения эффективной борьбы с рассматриваемыми преступлениями было принято Соглашение о сотрудничестве государств - участников СНГ в борьбе с преступлениями в сфере компьютерной информации (Минск, 2001 г.). В Соглашении определены основные термины:

а) преступление в сфере компьютерной информации - уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация;

б) компьютерная информация - информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи;

в) вредоносная программа - созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

г) неправомерный доступ - несанкционированное обращение к компьютерной информации.

Стороны признали в соответствии с национальным законодательством в качестве уголовно наказуемых следующие деяния, если они совершены умышленно:

а) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

б) создание, использование или распространение вредоносных программ;

в) 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 или тяжкие последствия;

г) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб.

2. Непосредственный объект преступления, предусмотренного ст. 272, - общественные отношения, обеспечивающие информационную безопасность, право собственника или иного законного владельца по реализации своих полномочий в установленных законом пределах на информацию, производство, владение, использование, распоряжение, защиту от неправомерного воздействия. Дополнительным объектом может выступать какая-либо тайна - государственная, коммерческая, банковская, личная, налоговая, врачебная, адвокатская, нотариальная, тайна исповеди и др.
Потерпевшим является собственник или иной законный владелец компьютерной информации, предметом преступления - охраняемая законом компьютерная информация.

3. Электронно-вычислительная машина (ЭВМ) - совокупность технических средств, создающая возможность проведения обработки информации и получения результата в необходимой форме, основные функциональные устройства которой выполнены на электронных компонентах. Под ЭВМ могут пониматься как компьютер, так и различные электронные устройства, отвечающие этим требованиям: устройства каналы связи, банкоматы, сотовые телефоны, кассовые аппараты и т.д.

Сетью ЭВМ признается совокупность компьютеров, а также средств и каналов связи, которые позволяют использовать информационные и вычислительные ресурсы каждого компьютера, включенного в сеть, независимо от его места нахождения.

Система ЭВМ - это совокупность взаимосвязанных и взаимодействующих как единое целое ЭВМ, обеспечивающих возможность выполнения единой задачи. Такой, например, является, государственная автоматизированная система (ГАС) "Выборы".

Под базой данных понимается объективная форма представления и организации совокупности данных (например, статей, расчетов), систематизированных таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ.

4. Согласно п. 1 ст. 2 Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" <1> под информацией понимаются сведения (сообщения, данные) независимо от формы их представления. Закон подробно регламентирует вопросы доступа, ограничения, распространения, предоставления, защиты, использования информации, информационно-телекоммуникационных сетей, ответственности за правонарушение в сфере информации, информационных технологий.

<1> СЗ РФ. 2006. N 31 (ч. I). Ст. 3448.

Информация делится на общедоступную и ограниченного доступа. Режим защиты информации, если иное не предусмотрено законом, определяет обладатель информации, который вправе ограничивать доступ к информации, обязан принимать меры по защите информации, если это установлено федеральным законом.

5. Информация признается объектом гражданских прав (ст. 128 ГК РФ). Вопросы правовой защиты информации определены в части четвертой ГК РФ, введенной в действие с 01.01.2008. В частности, в ст. 1225 ГК РФ в числе охраняемых результатов интеллектуальной деятельности и средств индивидуализации указаны программы для электронных вычислительных машин (программы для ЭВМ), базы данных.

В ст. 1261 ГК РФ указано, что авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы. В ней же дано понятие программы для ЭВМ, которой является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Статья 1262 ГК РФ определяет порядок и процедуру регистрации программ для ЭВМ и баз данных в федеральном органе исполнительной власти по интеллектуальной собственности. Предусмотрено, что программы для ЭВМ и базы данных, в которых содержатся сведения, составляющие государственную тайну, государственной регистрации не подлежат.

6. Компьютерная информация - это сведения, содержащиеся в оперативной памяти ЭВМ, на машинных носителях, подключенных к ЭВМ, или на съемных устройствах (жесткие магнитные диски (винчестеры), гибкие магнитные диски (дискеты), магнитооптические, оптические, лазерные и иные диски, ленты, карты памяти, компакт-диски и т.д.).

К охраняемой законом компьютерной информации относится любая информация, указанная в законе в связи с охраной вещных и обязательственных прав на ЭВМ и компьютерное оборудование, а также в связи с охраной тайны связи.

Она является информацией с ограниченным доступом и подразделяется на информацию, отнесенную к государственной тайне, и информацию конфиденциальную.

Конфиденциальность информации предполагает обязательное для выполнения лицом, получившим доступ к ней, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Согласно ч. 1 ст. 24 Конституции РФ сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Перечень сведений конфиденциального характера утвержден Указом Президента РФ от 06.03.97 N 188 <1>. К ним, в частности, относятся:

<1> СЗ РФ. 1997. N 10. Ст. 1127.

сведения о фактах, событиях и обстоятельствах частной жизни гражданина, сведения, составляющие тайну следствия и судопроизводства, сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20.08.2004 N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" <1> и другими нормативными правовыми актами РФ;

<1> СЗ РФ. 2004. N 34. Ст. 3534.

служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений);

сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна);

сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

7. Объективная сторона характеризуется неправомерным доступом к охраняемой законом компьютерной информации на любой стадии ее технологической обработки (сбор, перенос, формирование, ввод, передача и т.д.), что повлекло указанные в законе альтернативные последствия в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети.

Неправомерность предполагает завладение информацией не в установленном законом порядке, вопреки воле собственника или иного законного владельца (самовольное, без необходимого разрешения, согласия, с нарушением установленного порядка и т.д.).

Под доступом к информации понимается возможность получения информации и ее использования (приобретение и использование возможности просматривать, получать, вводить, изменять или уничтожать информацию либо влиять на процесс ее обработки, распоряжаться информацией). Способы доступа законодателем не определены, и они могут быть различными: хищение носителя информации, внедрение в чужую информационную систему, считывание, сканирование, перехват, взлом системы защиты с использованием специальных технических или программных средств, ввод ложной информации, ложного пароля, незаконное использование действующего пароля, кода и т.д.

8. Преступление имеет материальный состав, считается оконченным с момента наступления хотя бы одного из указанных в ч. 1 ст. 272 последствий в виде уничтожения, блокирования, модификации, копирования информации, нарушения работы ЭВМ, систем ЭВМ или их сети. Ознакомление с информацией при отсутствии последствий не образует состава преступления, предусмотренного ст. 272.

Уничтожение информации представляет собой ее удаление (полное или частичное) с соответствующего носителя, приведение ее в состояние, негодное для применения. Возможность владельца восстановить уничтоженную информацию не исключает ответственности. Если информация была не уничтожена, а лишь удалена, то в случае ее восстановления содеянное квалифицируется как покушение на уничтожение.

Блокирование информации заключается в создании различного рода временных или постоянных препятствий по правомерному доступу к ней, невозможности использования информации (полностью или частично) при ее полной сохранности.

Модификация информации - это ее любое изменение, не являющееся адаптацией, без согласия собственника или иного законного владельца (удаление, дополнение записей, перевод на другой язык, переработка и т.д.).

Копирование информации означает ее воспроизведение (перенос) с оригинала на другой носитель, ее дублирование без повреждения самой информации с возможностью дальнейшего использования по назначению, вывод информации на печатающее устройство и т.д.

Если при неправомерном доступе к информации виновный не только копирует, но и тиражирует информацию, то содеянное следует квалифицировать по совокупности ст. ст. 272 и 146 УК.

Нарушение работы ЭВМ, системы ЭВМ или их сети предполагает случаи уменьшения производительности, сбоев в работе, когда ЭВМ, их система или сеть не выполняют полностью или частично своих функций, например не выдают информацию вообще или выдают, но искаженную, неверную и т.п.

Если при нарушении работы ЭВМ, системы ЭВМ или их сети происходит их уничтожение или повреждение, то содеянное может квалифицироваться по совокупности ст. 272 и ст. 167 УК.

В случае, когда для неправомерного доступа к компьютерной информации лицо совершает хищение ЭВМ, содеянное охватывается ст. 272 и соответствующей статьей УК, предусматривающей ответственность за преступления против собственности в зависимости от формы хищения.

Совершение лицом какого-либо преступления с помощью полученной им при неправомерном доступе компьютерной информации подлежит самостоятельной юридической оценке. Например, хищение денег при неправомерном доступе к компьютерной информации может быть квалифицировано по совокупности ст. ст. 272 и 158 УК, поскольку совершается тайное хищение чужого имущества с использованием неправомерно полученной компьютерной информации.

9. Субъективная сторона характеризуется виной в форме умысла (прямого или косвенного).

10. Субъект преступления - лицо, достигшее возраста 16 лет.

11. В части 2 ст. 272 предусмотрены квалифицирующие признаки: деяние, совершенное группой лиц по предварительному сговору или организованной группой (ст. 35 УК) либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Использование служебного положения предполагает наличие специального субъекта. Им могут быть как должностное лицо, так и государственный и муниципальный служащий, не являющийся должностным лицом, а также иное лицо, использующее для совершения преступления (неправомерного доступа к компьютерной информации) свое служебное положение в организации, работником которой оно является, или в контролирующей организации.

Под лицами, имеющими доступ к ЭВМ, системе ЭВМ или их сети, понимаются любые лица, которые на законных основаниях (в соответствии со служебным положением, на основании разрешения, согласия владельца и т.п.) имеют право доступа к компьютерной системе, право получать компьютерную информацию, производить с ней определенные операции, осуществлять техническое обслуживание оборудования (операторы, программисты, абоненты системы ЭВМ и др.).

Статья 273 УК РФ Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет,

либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

1. Непосредственным объектом являются общественные отношения, обеспечивающие неприкосновенность, безопасное использование, владение и распоряжение содержащейся в ЭВМ, системах ЭВМ или их сети информации (программного обеспечения) от неправомерного воздействия. Предмет преступления - вредоносные программы для ЭВМ или машинные носители, содержащие такие программы.

Вредоносные программы - это специально созданные для ЭВМ различного рода программы с целью нарушения нормального функционирования компьютерных программ в соответствии с их документацией для достижения указанных в законе преступных результатов - заведомо приводящие к несанкционированным уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети (компьютерные вирусы, программы-сканеры, патчеры, управления информацией, эмуляторы электронных средств защиты и т.д.).

Вирусная программа как опасная разновидность вредоносной программы обладает способностью самораспространения, прохождения через коммуникационные сети компьютерных систем, "заражения" других ЭВМ и систем. Программы-сканеры предназначены для поиска каналов доступа (портов) к ЭВМ или их системе и несанкционированного проникновения с целью копирования информации с ЭВМ или на ЭВМ вредоносной программы. С помощью программ-эмуляторов осуществляется доступ к объектам, защита которых обеспечивается ЭВМ. Программы-патчеры используются для модификации программ, определенных производителем, устранения установленных им ограничений по защите

авторских прав от незаконного копирования; программы-генераторы - для управления потоками компьютерной информации.

2. Объективная сторона характеризуется созданием программ для ЭВМ или внесением изменений в существующие программы, заведомо приводящих к несанкционированным уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использованием либо распространением таких программ или машинных носителей с такими программами.

Создание вредоносной программы означает любую деятельность, направленную на разработку совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств, при условии, что ранее такая программа не существовала, с целью уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Создание вредоносной программы следует считать оконченным с момента, когда она приобрела окончательный вариант.

Использование вредоносной программы означает введение ее в оборот, непосредственное использование по назначению вредоносных качеств программы для несанкционированных уничтожения, блокирования, модификации, копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети.

Распространение вредоносной программы означает предоставление доступа, передачу носителя другим лицам, в том числе копирование или дозволение копирования программы на носитель другого лица, любым путем, включая продажу, дарение, обмен, прокат, сдачу внаем, предоставление взаймы (например, размещение на сайтах, в сети Интернет и т.д.).

Внесение изменений предполагает переработку, модификацию ранее созданной и существующей программы, в результате чего она становится вредоносной и может быть использована для указанных в ч. 1 ст. 273 целей.
Несанкционированные уничтожение, блокирование, модификация либо копирование информации означают достижение этого результата без разрешения собственника или иного законного владельца ЭВМ или иного законного основания.

Состав преступления формальный, преступление считается оконченным с момента создания, изменения, использования или распространения вредоносной программы, создающей угрозу указанных в законе последствий. Для наступления уголовной ответственности достаточно того, что программа была создана с целью достижения хотя бы одного из таких последствий.

3. Субъективная сторона характеризуется виной в виде прямого умысла.

4. Субъект преступления - лицо, достигшее возраста 16 лет.

5. В ч. 2 ст. 273 предусмотрен квалифицированный вид состава - совершение деяния, повлекшего по неосторожности тяжкие последствия.

Тяжкие последствия - оценочный признак, устанавливается по конкретному делу с учетом всех обстоятельств. Таковы могут быть, например, причинение по неосторожности смерти человека, тяжкого вреда здоровью, самоубийство потерпевшего, причинение особо крупного имущественного ущерба, возникновение аварии на транспорте, катастрофы, разрушений средств связи, коммуникаций, утрата секретной информации и т.д.

Субъективная сторона характеризуется двумя формами вины - умыслом в совершенных действиях и неосторожность к наступившим тяжким последствиям.

Статья 274 УК РФ Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, - наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок

1. Непосредственным объектом признаются общественные отношения, обеспечивающие правильную и безопасную эксплуатацию ЭВМ, системы ЭВМ или их сети. Предмет преступления - охраняемая законом компьютерная информация.
2. Объективная сторона характеризуется нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшим уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.

Под правилами эксплуатации ЭВМ, системы ЭВМ или их сети (компьютерной системы) понимаются правила, определяющие порядок работы с ЭВМ (нормативные акты, инструкции, правила, техническое описание, положение, приказы и т.д.), установленные компетентным государственным органом, или технические правила, установленные соответствующими лицами (изготовителями ЭВМ, разработчиками компьютерных программ, их законными владельцами и др.). Например, Федеральный закон от 07.07.2003 N 126-ФЗ "О связи" <1> устанавливает правовые основы деятельности в области связи на территории РФ и на находящихся под ее юрисдикцией территориях, определяет полномочия органов государственной власти в области связи, а также права и

обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

<1> СЗ РФ. 2003. N 28. Ст. 2895.

Существенный вред - понятие оценочное, зависит от конкретных значимых для дела обстоятельств, например от важности и ценности информации для гражданина, общества, государства, от размера материального ущерба в результате уничтожения информации, от объема повреждения, блокирования, модификации ЭВМ, системы ЭВМ или их сети и т.д.

Состав преступления материальный, считается оконченным с момента причинения существенного вреда.

3. Субъективная сторона характеризуется виной в форме умысла (прямого или косвенного).

4. Субъект преступления специальный - лицо, достигшее возраста 16 лет, имеющее доступ к ЭВМ, системе ЭВМ или их сети.

5. В части 2 ст. 274 предусмотрен квалифицированный вид состава - совершение деяния, повлекшего по неосторожности тяжкие последствия. Данное понятие оценочное, но в любом случае вред должен быть выше существенного, указанного в ч. 1 ст. 274 УК.

6. Субъективная сторона характеризуется двумя формами вины

Криминалистическая характеристика преступлений в сфере компьютерной информации

Одним из следствий массовой компьютеризации в России явились преступления в сфере компьютерной информации. Интеграция современных информационных технологий практически во все области человеческой деятельности привела к тому, что с помощью компьютерных средств и систем совершаются «традиционные» преступления (например, присвоение, кража, мошенничество, фальшивомонетничество, лжепредпринимательство и др.). Компьютерные технологии используются с целью: фальсификации платежных документов; хищения наличных и безналичных денежных средств путем перечисления на фиктивные счета; отмывания денег; вторичного получения уже произведенных выплат; совершения покупок с использованием фальсифицированных или похищенных электронных платежных средств; продажи секретной информации и проч.

Преступления, сопряженные с использованием компьютерных технологий, представляют серьезную угрозу для любой располагающей компьютерной техникой организации. При этом наряду с высокой степенью риска ей наносится и значительный материальный ущерб: вывод из строя электронно-вычислительной системы в результате возникновения нештатной технической ситуации или преступления может привести даже самый

крупный банк к полному разорению за четверо суток, а более мелкое учреждение — за сутки.

Преступления, совершаемые с использованием компьютерных средств и систем, принято называть **компьютерными преступлениями.** Эта дефиниция должна употребляться не в уголовно-правовом аспекте, где это только затрудняет квалификацию деяния, а в криминалистическом, поскольку связана не с квалификацией, а именно со способом совершения и сокрытия преступления и, соответственно, с методикой его раскрытия и расследования.

Компьютерная информация применительно к процессу доказывания может быть определена как фактические данные, обработанные компьютерной системой и (или) передающиеся по телекоммуникационным каналам, а также доступные для восприятия, на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения уголовного или гражданского дела. Источниками компьютерной информации служат:

- машинная распечатка;
- накопители на магнитных, оптических и иных носителях;
- база данных (фонд) оперативной памяти ЭВМ или постоянного запоминающего устройства.

Для совершения компьютерных преступлений злоумышленники используют:

- подбор паролей, ключей и другой идентификационной или аутентификационной информации;
- подмену IP-адресов пакетов, передаваемых по Интернету или другой глобальной сети, так, что они выглядят поступившими изнутри сети, где каждый узел доверяет адресной информации другого;
- инициирование отказа в обслуживании — воздействие на сеть или отдельные ее части с целью нарушения порядка штатного функционирования;
- прослушивание и расшифровку трафика с целью сбора передаваемых паролей, ключей и другой идентификационной или аутентификационной информации;
- сканирование с использованием программ, последовательно перебирающих возможные точки входа в систему (например, номера TCP-портов или телефонные номера) с целью установления путей и возможностей проникновения;
- подмену, навязывание, уничтожение, переупорядочивание или изменение содержимого данных (сообщений), передаваемых по сети, и др.

Известны следующие способы совершения компьютерных преступлений:

а) методы перехвата: подключение к компьютерным сетям; поиск данных, оставленных пользователем после работы с компьютером (физический поиск — осмотр содержимого мусорных корзин и сбор оставленных за ненадобностью распечаток, деловой переписки и т. п.; электронный поиск —

последние из сохраненных данных обычно не стираются после завершения работы), для обнаружения паролей, имен пользователей и проч.;

б) методы несанкционированного доступа: подключение к линии законного пользователя через Интернет, через слабые места в защите системы, при системной поломке либо под видом законного пользователя (физический вариант — пользователь выходит ненадолго, оставляя терминал в активном режиме). Системы, не обладающие средствами аутентичной идентификации (по отпечаткам пальцев, голосу и т. п.), оказываются без защиты против этого приема. Простейший путь — получение идентифицирующих шифров законных пользователей либо использование особой программы, применяемой в компьютерных центрах при сбоях в работе ЭВМ;

в) методы манипуляции:

- подмена данных — изменение или введение новых данных осуществляется, как правило, при вводе или выводе информации с ЭВМ;
- манипуляции с пультом управления компьютера — механическое воздействие на технические средства машины, что создает возможность манипулирования данными;
- «троянский конь» — тайный ввод в чужую программу команд, позволяющих, не изменяя работоспособность программы, осуществить определенные функции. Этим способом преступники обычно отчисляют на свой счет определенную сумму с каждой операции. Вариантом является «салями», когда отчисляемые суммы малы и их потери практически незаметны (например, по 10 центов с операции), а накопление осуществляется за счет большого количества операций;
- «бомба» — тайное встраивание в программу набора команд, которые должны сработать (или срабатывать каждый раз) при определенных условиях либо в определенные моменты времени (например, вирус «Чернобыль», который активизируется 26 апреля — в день аварии на Чернобыльской АЭС);
- моделирование процессов, в которые преступники хотят вмешаться, и планируемые методы совершения и сокрытия посягательства для оптимизации способа преступления. Одним из вариантов является реверсивная модель, когда создается модель конкретной системы, в которую вводятся реальные исходные данные и учитываются планируемые действия. Из полученных правильных результатов подбираются правдоподобные желательные. Затем путем прогона модели назад, к началу, выясняют результаты и устанавливают, какие манипуляции с исходными данными нужно проводить. Таких операций может быть несколько. После этого остается только осуществить задуманное.

Как правило, компьютерные преступления совершаются с помощью того или иного сочетания приемов.

Типичные следственные ситуации при расследовании преступлений в сфере компьютерной информации.

Типичные следственные ситуации по данной категории преступлений можно классифицировать по различным основаниям.

По источнику информации выделяют ситуации, когда:

- преступление обнаружено самим пользователем;
- преступление обнаружено в ходе оперативно-розыскной деятельности;
- преступление обнаружено в ходе прокурорских проверок;
- преступление выявлено при проведении ревизии;
- преступление обнаружено в ходе производства следственных действий по другому уголовному делу.

Наименьшим объемом информации характеризуется первая ситуация, наибольшим - последняя.

Вообще в зависимости от объема информации, имеющейся в распоряжении следствия, можно выделить такие ситуации, как:

- отсутствует информация о способе, мотивах, личности злоумышленника, известны только последствия преступного деяния, т.е. преступный результат (например, дезорганизация компьютерной сети банка), механизм преступления неизвестен;

- - известны способ, мотивы и последствия преступного деяния, но неизвестна личность злоумышленника или же он известен, но скрылся, механизм преступления в полном объеме неясен (например, произошел несанкционированный доступ к файлам законного пользователя через Интернет, через слабые места в защите компьютерной системы);

- имеется информация и о способе, и о мотивах, и о личности злоумышленника, т.е. в условиях очевидности — характер и его обстоятельства известны (например, какой вирус и каким способом введен в компьютерную сеть) и выявлены потерпевшим собственными силами, преступник известен и задержан (явился с повинной);

В наименее благоприятной ситуации необходимо установить механизм преступления.

В третьем случае необходимо установить, имелась ли причинно-следственная связь между несанкционированным проникновением в компьютерную систему и наступившими последствиями (сбоями в работе, занесением компьютерного вируса и проч.), определить размеры ущерба.

Во втором случае первоочередной задачей наряду с указанными выше являются розыск и задержание преступника.

В зависимости от имеющейся у следствия информации проводится предварительная проверка, в ходе которой должны быть получены: документы, обусловливающие права потерпевшего на компьютерную технику или компьютерную информацию, подвергшуюся атаке; документы, отражающие неправомерно совершенную операцию.

В первых двух ситуациях целесообразно строить расследование по следующей схеме: опрос заявителя и свидетелей - осмотр места

происшествия с участием специалистов - проведение ОРМ для установления причин преступления, выявления злоумышленников - допрос свидетелей и потерпевших - выемка и изучение компьютерной техники и документации - задержание злоумышленника - допрос подозреваемого - обыски по месту жительства и работы - назначение и производство судебных экспертиз.

В третьей (максимально информативной) ситуации схема может быть несколько иная: изучение материалов предварительной проверки и возбуждение уголовного дела - осмотр места происшествия - задержание злоумышленника - допрос подозреваемого - обыски по месту жительства и работы подозреваемого - допросы потерпевших и свидетелей - выемка компьютерной техники и документации - назначение экспертиз.

Психологический портрет

В расследовании преступлений со скрытой мотивацией каких-либо «материальных» следов для поимки преступника обнаружить обычно не удается, либо они не пригодны для идентификации личности. В помощь сотрудникам правоохранительных органов приходит методика построения психологического портрета неустановленного лица, совершившего преступление. Использование этой методики позволяет решить ряд задач, а именно: определение круга подозреваемых, прогнозирование поведения преступника, построение наиболее оптимальной тактики допроса, оправдание невиновного лица и т.д.

Психологический портрет преступника можно определить как документ, к которому предъявляются определенные требования относительно содержания и формы систематизации информации о преступнике в портрете. Кроме того, необходимо учитывать, что в содержании этого документа должны быть указаны не только психологические признаки, но и любые иные сведения, основанные на анализе поведения личности преступника. Это может быть пол, возраст, социально-демографические признаки. Составление психологического портрета преступника предполагает решение определенных задач, имеющих прикладное значение в рамках деятельности правоохранительных органов. В связи с этим, его содержание не должно быть абстрактным. В зависимости от того, какие задачи ставятся для создания психологического портрета преступника, в юридической психологии выделяют его различные виды:

I. По основанию его предназначения: 1) Розыскной (используется при расследовании преступлений); 2) Прогностический (используется для прогнозирования поведения преступника, например, при освобождении заложников); 3) Следственный (используется для построения эффективной тактики проведения следственных действий); 4) Пенитенциарный (предназначен для организации исправительно-воспитательных воздействий); 5) Постпенитенциарный (предназначен для оценки

эффективности мер воздействия применявшихся к конкретному лицу и прогнозирование поведения после освобождения из мест лишения свободы.

II. В зависимости от содержания и определенности исходной информации о виновном можно выделить: 1) Психологический портрет известного преступника; 2) Психологический портрет неизвестного преступника. Для них существенно различен характер и качество источников информации. Так, при составление психологического портрета известного преступника, можно изучить биографию, взять интервью у него или у его родственников, что поможет сделать психологический портрет более точным; в то время как при составлении психологического портрета неизвестного преступника приходится делать выводы только на основании осмотра места происшествия, результата экспертиз, показаний свидетелей, изучения личности потерпевшего.

III. По количественному признаку объекта отображения: 1) Психологический портрет преступной группы; Психологический портрет преступника.

Для составления психологического портрета необходимо понимать, какой перечень он должен содержать. Наиболее полезным для следствия видятся следующие данные: 1) индивидуальные признаки личности – привычки, склонности, навыки; 2) возраст; 3) район места жительства; 4) район места работы, службы, учебы; 5) частные характеристики места вероятного обитания; 6) уровень образования и профессиональной квалификации; 7) род занятий; 8) особенности происхождения (родительской семьи) и личной истории жизни; 9) семейное положение; 10 наличие детей; 11) отношение к отдельным видам деятельности – к службе в армии, спорту, медицине, работе с людьми и пр.; 12) наличие прошлой судимости; 13) наличие психической, а также иной патологии; 14) антропологические и динамические характеристики лица (тип внешности, телосложение, пантомимика и др.). 9 Помимо указанных могут быть приведены и другие данные.

Методика составления психологического портрета преступника изучается и тщетно разрабатывается отечественными и зарубежными исследователями. Непосредственным объектом данной методики являются поведенческие особенности преступника в контексте ситуации, общим же объектом будет само событие преступления. Предмет метода «портретирования» - способ или система способов анализа следов и обстоятельств происшествия. Алгоритм метода составления психологического портрета преступника включает в себя четыре последовательных этапа его разработки и содержит в себе три уровня анализа следов. Выделяют следующие уровни анализа: 1) Криминалистический, в которой по объективной стороне преступления восстанавливается «внешняя» картина преступления. На самом общем уровне делаются предположения о мотиве и цели преступления. 2) Поведенческий, в котором выявляют индивидуальные признаки в действиях преступника. 3) Диагностический, в котором индивидуальные признаки

связывают с другими признаками его личности и психологическими свойствами.

Этапы разработки психологического портрета преступника:

1) Составление криминалистической информационной модели события преступления;

2) Ситуационное моделирование;

3) Психологическая интерпретация поведения преступника;

4) Оформление выводной информации о признаках личности преступника в психологическом портрете. На первом этапе по следам на месте происшествия и его обстоятельствам, воссоздается внешний ряд действий преступника и ситуации преступления. Здесь собирается и анализируется информация о событии происшествия, содержащаяся в возможных ее носителях. Такими «носителями» могут выступить: само место преступления; показания свидетелей; информация о личности жертвы; объект преступления; заключения экспертиз. Исследователями в данной области выделено четыре ключевых вида сведений:

1) способ преступления (орудие и средства);

2) обстановка места происшествия (пространственно-объектно-временные характеристики);

3) Объект преступления, как носитель конкретных качеств;

4) Лица, косвенно связанные с преступлением.

На основе собранных данных в полном объеме выявляется внешняя сторона преступления, субъективная сторона - представлена весьма обобщено. Хотелось бы отметить, что первый этап крайне важен в силу того, что психические явления должны исследоваться на основе объективных показателей их признаков, проявившихся во вне. Второй этап заключается в том, что будут подвергнуты анализу данные, полученные на первом этапе, в целях моделирования поведения преступника. Сам же блок «ситуационное моделирование» включает в себя:

1) моделирование ситуации;

2) моделирование жертвы и ее поведения;

3) реконструкция (моделирование) психологической структуры преступной деятельности. Наиболее сложным на этом этапе является реконструкция психологической структуры преступной деятельности. Здесь каждая структурная единица: действие, цепочка действий, деятельность в целом, имеет свою познавательную функцию, поэтому их четкое различение необходимо в целях установления данных о субъективной стороне преступления.

Вообще, на втором этапе разработки психологического портрета эксперты в этой области воссоздают поведение преступника как единую систему, системообразующим принципом которой выступает личность преступника в ее субъективном отношении к другим элементам системы. Данное отношение находит свое внешнее проявление в «индивидуальности действия». По мнению Х. Хекхаузена, действие детерминировано не ситуацией, а личностью. Третий этап заключается в интерпретации

выявленных элементов поведения преступника в целях описания его личностных особенностей, свойств и признаков, опираясь на существующие социально-психологические закономерности. Этот этап выступает высшим уровнем анализа преступного события. Четвертый последний этап – это оформление полученных данных в документе, который будет передан правоохранительным органам, целью которого является помощь в поимках лица, совершившего преступление. Данный документ должен состоять из пяти разделов. В первом разделе дается психологический анализ совершенного преступления от момента предкриминальной ситуации до момента оставления преступником места происшествия. Данный раздел решает задачу обоснования выводных данных о личности преступника, исходя из выявляемого смысла отдельных поступков и криминального поведения в целом. Здесь же объясняется мотив и значение действий преступника, которые непонятны правоохранительным органам. Во втором разделе указывается психологический диагноз, квалифицирующий личность преступника. Третий раздел должен содержать поисковый психологический портрет, и решать задачу обобщения и оптимизации выводной информации о признаках преступника. На основании этой части данного документа правоохранительные органы выдвигают розыскные версии. Поэтому его содержание должно непосредственно указывать на признаки виновного лица, пригодные для целей его розыска. Четвертый раздел содержит в себе идентификационный психологический портрет преступника, в котором даны опорные психологические и социальные признаки лица, пригодные для его идентификации на стадии подозреваемого. Хотелось бы отметить, что третий и четвертый раздел тесно взаимосвязаны и постоянно взаимодействуют друг с другом в процессе психологического анализа преступления. Идентификационный портрет служит вспомогательным материалом, он может выступать косвенным доказательством принадлежности преступлений одному и тому лицу, что позволит на стадии предварительного следствия объединить уголовные дела. К сожалению, в силу разных причин, начиная с кооперации между правоохранительными органами, заканчивая человеческими факторами, на территории России не сразу удается установить принадлежность нескольких преступлений к одному субъекту, что осложняет поимку виновного лица. Помимо всего прочего, идентификационный портрет, после соответствующей переработки и уточнения его содержания, может эффективно использоваться органами следствия в процессе задержания, допроса и иных следственных действий. Последним, пятым разделом в документе может явиться вероятностный прогноз на совершение нового преступления тем же лицом, с указанием на временные и пространственные параметры.

Личность преступника отличается целым рядом особенностей:

- четко формулирует любую профессиональную задачу, но часто характеризуется хаотическим поведением в быту;
- обладает развитым формально-логическим мышлением, которое зачастую подводит в реальной жизни;

- стремится к точности, четкости и однозначности в языке, постоянно задает уточняющие вопросы и переспрашивает, что вызывает раздражение собеседника;
- постоянно использует компьютерный жаргон, малопонятный непосвященным.

Отечественные правонарушители в сфере компьютерной информации могут быть разделены на две возрастные группы: первая — 14-20 лет, вторая — с 21 года и старше.

Представители первой возрастной группы — это старшие школьники или студенты младших курсов высших или средних специальных учебных заведений, которые активно ищут пути самовыражения и находят их, погружаясь в виртуальный мир компьютерных сетей. При этом чаще всего ими движет скорее любопытство и желание проверить свои силы, нежели корыстные мотивы. К числу особенностей, указывающих на совершение компьютерного преступления лицами рассматриваемой категории, можно отнести: отсутствие целеустремленной, продуманной подготовки к преступлению; оригинальность способа; непринятие мер к сокрытию преступления; факты немотивированного озорства.

Компьютерные преступники, входящие во вторую возрастную группу, — это уже вполне сформировавшиеся личности, обладающие высокими профессиональными и устойчивыми преступными навыками, а также определенным жизненным опытом. Совершаемые ими деяния носят осознанный корыстный характер, при этом, как правило, предпринимаются меры по противодействию раскрытию преступления. Преступления, которые носят серийный, многоэпизодный характер, обязательно сопровождаются действиями по сокрытию. Это обычно высококвалифицированные специалисты с высшим математическим, инженерно-техническим или экономическим образованием, входящие в организованные преступные группы и сообщества, прекрасно оснащенные технически (нередко специальной оперативной техникой). Особую опасность с точки зрения совершения преступлений в сфере компьютерной информации представляют профессионалы в области новых информационных технологий. На долю этой группы приходится большинство особо опасных должностных преступлений, совершаемых с использованием средств компьютерной техники, присвоений денежных средств в особо крупных размерах, мошенничества и проч.

Среди мотивов и целей совершения посягательств можно выделить:

- корыстные (присвоение денежных средств и имущества);
- политические (шпионаж, деяния, направленные на подрыв финансовой и денежно-кредитной политики, валютной системы страны);
- исследовательский интерес;
- хулиганские побуждения и озорство;
- месть и иные побуждения.

Сведения о потерпевшей стороне. Потерпевших можно подразделить на три основные группы: собственники компьютерной системы; клиенты, пользующиеся их услугами; иные лица.

Потерпевший, особенно относящийся к первой группе, часто неохотно сообщает (или вовсе не сообщает) правоохранительным органам о преступных фактах в сфере движения компьютерной информации по следующим причинам:

- из-за некомпетентности сотрудников правоохранительных органов в данном вопросе;
- боязни, что убытки от расследования превысят размер причиненного ущерба и к тому же будет подорван авторитет фирмы;
- боязни раскрытия в ходе судебного разбирательства системы безопасности организации;
- боязни выявления собственных незаконных действий; боязни должностных лиц, что одним из итогов расследования станут выводы об их профессиональной непригодности (некомпетентности);
- из-за правовой неграмотности;
- из-за непонимания истинной ценности имеющейся информации.

Контрольные вопросы и задания

Контрольные вопросы

1. Какие деяния относятся к преступлениям в сфере компьютерной информации?
2. Что понимается под неправомерным доступом к компьютерной информации согласно УК Российской Федерации?
3. Какова ответственность за неправомерный доступ к компьютерной информации согласно УК Российской Федерации?
4. Каковы правовые последствия создания, использования и распространения вредоносных программ для ЭВМ?
5. Каковы правовые последствия нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети?
6. Что понимается под терминами: блокирование, модификация, копирование компьютерной информации, в чём состоит нарушение работы ЭВМ, системы ЭВМ или их сети?
7. Какова ответственность за компьютерные преступления?

Задания

1. Установить наличие состава преступления и квалифицировать его в соответствии с УК РФ на основе описания совершенного деяния в сфере компьютерной информации. Описать непосредственный объект, обязательные признаки объективной стороны, субъекта, последствия, санкции и т.п.
2. Идентифицировать следственную ситуацию и выбрать схему расследования.
3. Сформулировать возможные цели, мотивы и характеристику преступника. Разработать психологический портрет компьютерного преступника.

4. Подготовить и защитить отчет о выполнении задания.

Литература

1. Уголовный Кодекс Российской Федерации
2. ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации.-М. 2013: http://genproc.gov.ru/documents/nauka/execution/document-104550/
3. http://5fan.ru/wievjob.php?id=44475
4. **http://www.studylaw.narod.ru/kursup1/kursup1_6_1.htm**

Тема 2 Тактика обнаружения, изъятия и фиксации компьютерной информации при производстве следственных действий. Осмотр места происшествия. Обыск

Осмотр места происшествия по делам о расследовании многих преступлений – неотложное следственное действие, которое в соответствии со ст. 178 УПК РФ производится для «обнаружения следов преступления и других вещественных доказательств, выяснения обстановки происшествия, а равно иных обстоятельств, имеющих значение для дела». Отсюда задачами осмотра являются:

1) изучение и фиксация обстановки места происшествия с целью выяснения характера и механизма происшествия;

2) обнаружение и изъятие следов преступления, которые в дальнейшем могут служить вещественными доказательствами по делу;

3) выявление признаков, характеризующих лиц, участвовавших в совершении преступления (их число; примерный возраст; физические данные; наличие у них определенных привычек, навыков, психических отклонений, а также осведомленности о жизненном укладе, распорядке работы потерпевшего);

4) фиксация особенностей, присущих потерпевшему и иным объектам посягательства;

5) установление обстоятельств, отражающих объективную сторону преступления: время и способ его совершения; действия преступника на месте происшествия; последствия преступления; наличие причинной связи между действиями преступника и наступившими последствиями

6) выявление признаков, указывающих на мотивы и цели совершения преступления;

7) выявление обстоятельств, способствующих совершению преступления.

Выполнение задач осмотра места происшествия помогает получить исходные данные для раскрытия преступления, розыска и изобличения преступника.

Тактика осмотра места происшествия. В криминалистической литературе по тактике осмотра места происшествия обстоятельно разработаны вопросы, относящиеся условно говоря, к технической стороне проведения этого следственного действия, позволяющего уже на изначальной общей стадии осмотра, решать задачу по построению версии о содержании и характере происшедшего на основе общей обстановочной картины места происшествия и видовых, не расчлененных следов. Анализ материала позволяет сделать вывод о том, что входе осмотра места происшествия процессы восприятия сочетаются с процессами мысленного моделирования, которое проходит ряд этапов:

1) Установление картины совершенного преступления в целом (по видовым следам);

2) Установление всех непосредственно воспринимаемых материальных следов преступных действий;

3) Мысленное восстановление следователем каждого из совершенных действий;

4) Мысленное восстановление картины совершенного преступления в целом. В результате реконструкции события преступления происходит уточнение мотива и цели через смысловое объяснение каждого из действий, связанных с совершением расследуемого преступления. В соответствии со ст. 166 и ст. 180 УПК РФ, в протоколах описываются все действия следователя, а также все обнаруженное при осмотре в той последовательности, в какой производился осмотр, и в том виде, в каком обнаруженное наблюдалось в момент осмотра. Таким образом, в протоколах отражается простая «инвентаризация следов», вне определения их структурной принадлежности и характера действий преступника. Это представляется наилучшим решением законодателя, так избегается субъективизм в данном следственном действии. Кроме того, разработчик психологического портрета преступника будет объективно рассматривать те или иные «следы», делая свои выводы, которые могут быть отличны от выводов следователя.

Действия следователя при получении сообщения о преступлении

Получив сообщение о преступлении, следователь должен:

1) выяснить, что случилось; где; когда; кто и когда обнаружил происшествие; кто из сотрудников органов внутренних дел или должностных лиц находится на месте происшествия;

2) дать указание сотрудникам органов внутренних дел, находящимся на месте происшествия или в районе его расположения, организовать охрану места происшествия;

3) вызвать для участия в осмотре сотрудника органа дознания и в необходимых случаях кинолога с собакой;

4) пригласить для участия в осмотре соответствующих специалистов (например, по делам о взрывах – специалиста по взрывному делу;

при наличии на месте происшествия трупа – специалиста в области судебной медицины или иного врача), а также специалиста-криминалиста с соответствующей техникой;

5) дать задание специалисту-криминалисту проверить **состояние** техники;

6) предложить сотрудникам органа дознания, находящегося в районе расположения места происшествия, пригласить понятых, не заинтересованных в исходе дела;

7) сообщить начальнику следственного отдела или прокурору о предстоящем выезде, согласовав с ними состав следственно-оперативной группы и обеспечение ее транспортными средствами для выезда на место происшествия.

Действия следователя по прибытию на **место происшествия**

Прибыв на место происшествия, следователь

1) принимает меры для оказания помощи потерпевшему;

2) оказывает содействие в организации тушения пожара, спасения ценного имущества и т.п.;

3) проверяет, как осуществляется охрана места происшествия и защита следов преступления;

4) обеспечивает удаление с места происшествия посторонних;

5) путем опроса работников внутренних дел и должностных лиц, находящихся на месте происшествия, а также очевидцев получает информацию о происшествии, о том, какие изменения внесены в обстановку происшествия с момента его обнаружения;

6) в соответствии со ст. 133^1, ст. 139 и 135 УПК разъясняет специалисту и понятым их права и обязанности и в случае необходимости предупреждает понятых о неразглашении ими сведений, полученных при осмотре места происшествия, а специалиста – об ответственности за отказ и уклонение от выполнения своих обязанностей;

7) принимает меры, направленные на улучшение условий осмотра (например, обеспечение осмотра искусственным освещением; оборудование рабочего места для составления протокола осмотра);

8) при осмотре больших территорий, нескольких помещений **к их** осмотру могут дополнительно привлечь другого следователя.

Действия следователя при осмотре места происшествия

После подготовки к осмотру необходимо:

1) произвести обзор места происшествия для определения границ участка, подлежащего осмотру, и способа последовательного изучения обстановки на месте происшествия. Границы осмотра места происшествия охватывают место, где произошло событие и вследствие этого возможно обнаружение следов или предметов, связанных с ним; пути прихода преступника на место происшествия или ухода с него; место засады, где преступник ожидал жертву; иные помещения или участки местности, которые также могут быть носителями следов преступления. К методам осмотра относятся приемы и способы его проведения:

сплошной и выборочный;

концентрический **(от** периферии к центру) и эксцентрический (от центра к периферии);

линейный (фронтальный);

статический и динамический;

2) поручить специалисту-криминалисту произвести ориентирующую и обзорную фотосъемку места происшествия; помощнику следователя составить черновик схемы (плана) расположения видимых с одной точки объектов обстановки происшествия;

3) дать задания сотрудникам органов дознания о проведении неотложных оперативных мероприятий;

4) если для осмотра приглашен кинолог с собакой, обеспечить возможность ее применения;

5) после производства обзора приступить к детальному осмотру места происшествия, применяя один или несколько выбранных методов осмотра; при этом необходимо учитывать следующее:

– в первую очередь осматривать, фиксировать и изымать предметы со следами, которые могут исчезнуть или легко видоизмениться (например, предметы, возможно, содержащие запаховые следы; пищевые продукты со следами зубов или пальцев рук, возможные предметы–носители микрочастиц и др.);

– учитывать изменения, которые могли внести в обстановку места происшествия до прибытия следователя лица, оказавшиеся первыми **на** месте происшествия: работники органов внутренних дел, должностные лица предприятия или учреждения, где совершено преступление, пожарные и др.;

– обращать внимание на наличие негативных обстоятельств;

– выдвигать и по возможности проверять версии, возникшие в ходе осмотра;

6) если это необходимо, прерывать долго длящиеся осмотры, отмечая время начала и окончания перерыва в часах и минутах;

7) в соответствии со ст. 182 УПК составить протокол осмотра места происшествия, а также план и схему. Изъять и упаковать следы и вещественные доказательства.

Основные вопросы, подлежащие установлению при осмотре

При осмотре места происшествия необходимо стремиться выяснить следующее:

1) Какое именно событие произошло на месте происшествия?

2) Время совершения исследуемого события.

3) Объект преступного посягательства.

4) Имеются ли жертвы происшествия и кто именно.

5) Сведения о преступниках: их количество, пол, возраст, антропологические данные, пути их прихода на место происшествия и ухода с него. Для установления этих данных детально изучается весь комплекс оставшихся на месте происшествия следов совершенного преступления.

6) Как долго находились преступники на месте происшествия? Такие данные могут быть получены в результате моделирования события происшествия с учетом способа его совершения.

7) Как вели себя на месте происшествия преступник и жертва? Какие действия и в какой последовательности совершали? Для ответа на этот вопрос также изучаются все обнаруженные следы.

8) Какие орудия, инструменты и иные средства использовались при совершении преступления?

9) Что похищено при совершении корыстных преступлений? Могло ли быть похищенное унесено с места происшествия или его увезли на каком-либо транспорте? Не спрятаны ли похищенное или его часть неподалеку от места происшествия?

10) Какой вид транспорта использовался преступниками для прибытия на место происшествия и убытия с него?

11) Предпринимали ли преступники меры для сокрытия следов своего пребывания на месте происшествия и какие именно?

12) Каковы мотивы и цели совершения преступления?

Виды осмотра места происшествия

При расследовании может возникнуть необходимость в производстве дополнительного или повторного осмотра:

1) дополнительный осмотр назначается, если при первоначальном осмотре отдельные объекты, расположенные на месте происшествия, о которых стало известно, например из допросов очевидцев преступления, не осматривались или осмотрены недостаточно детально. От дополнительного осмотра места происшествия следует отличать осмотр отдельных участков со следами, относящимися к происшествию, обнаруженными при прочесывании местности. Он осуществляется позже первичного осмотра для поиска на большой территории, прилегающей к месту происшествия, предметов со следами преступления пли авиакатастроф, крушений поездов. Этот осмотр проводится силами общественности или воинскими подразделениями. При обнаружении таковых осматривается участок местности, на которой они найдены, и прилегающая к ним территория. Результаты осмотра оформляются либо отдельным протоколом, либо вносятся в протокол осмотра места происшествия, когда последний осуществляется одновременно с прочесыванием местности;

2) повторный осмотр требуется в случаях проведения первоначального осмотра в неблагоприятных погодных условиях, в связи с чем важные для дела обстоятельства не могли быть установлены, или есть основания полагать, что первоначальный осмотр произведен недоброкачественно, например вследствие отсутствия соответствующего специалиста.

При подготовке к производству дополнительного или повторного осмотров места происшествия следует изучить протокол первичного осмотра и приложения к нему; ознакомиться с собранными по делу доказательствами; по возможности пригласить для участия в осмотре тех понятых и

специалистов, которые участвовали в первоначальном осмотре места происшествия.

Протокол осмотра места происшествия

Процессуальное значение протокола и требования, предъявляемые к его составлению следующие:

1. В соответствии со ст. 69 и 87 У ПК протокол осмотра места происшествия служит источником доказательств, поэтому при его составлении необходимо руководствоваться требованиями ст. 141,142 и 182 УПК.

2. Статья 141 УПК определяет момент составления протокола: «в ходе следственного действия или непосредственно после его окончания».

3. Согласно ст. 141 УПК в протоколе осмотра места происшествия должны быть обязательные реквизиты, отсутствие одного из которых является нарушением закона, что может иметь отрицательные последствия при оценке протокола в суде, особенно в тех случаях, если они не могут быть восполнены допросами участников осмотра.

4. Статья 182 УПК предусматривает порядок составления описательной части протокола.

5. Статья 141 УПК устанавливает порядок использования при осмотре научно-технических средств и отражения их применения в протоколе осмотра, а также дает перечень необходимых приложений к протоколу.

6. Статьи 133 и 141 УПК регламентируют процесс уведомления участников осмотра о применении технических средств и ознакомления участников осмотра с содержанием протокола, а также порядок реализации их прав.

Вводная часть протокола

Обязательными элементами этой части протокола являются:

1) место и дата производства осмотра;

2) должность, фамилия, инициалы лица, производившего осмотр и составившего протокол;

3) основания производства осмотра (согласно ст. 178 УПК);

4) характер происшествия, расположение места осмотра;

5) время начала и окончания осмотра;

6) фамилия, имя и отчество каждого участника осмотра; занимаемая должность представителей учреждений и предприятий; адреса понятых;

7) отметка о разъяснении понятым их прав и обязанностей;

8) отметка о разъяснении специалистам их прав и обязанностей;

предупреждении об ответственности за отказ или уклонение от выполнения своих обязанностей, а также наличие подписи, удостоверяющей это предупреждение;

9) условия проведения осмотра (освещение, метеорологические или иные условия, влияющие на проведение осмотра);

10) отметка об уведомлении лиц, участвующих в производстве осмотра, о применении в ходе осмотра конкретных технических средств.

Отсутствие в протоколе одного из требований, предусмотренных ст. 133, 135, 141, 142, 178, 179, 180, 182 УПК РСФСР, должно быть восполнено

немедленно при обнаружении этого факта после отъезда группы с места происшествия путем проведения допросов участников осмотра или производства повторного осмотра места происшествия.

Описательная часть протокола

В целях выполнения процессуальных требований ст. 141 и 182 УПК в протоколе следует:

1) «описывать все действия следователя, а равно все обнаруженное при осмотре... в той последовательности, как производился осмотр, и в том виде, в каком обнаруженное наблюдалось в момент осмотра...»

При описании действий следователя и обнаруженных на месте происшествия предметов и следов необходимо:

а) избегать употребления длинных фраз, неопределенных выражений типа «недалеко», «вблизи» и т.п.; местных выражений и большого количества специальных терминов; использования синонимов при описании одного объекта;

6) последовательно и четко излагать свои мысли;

в) подробно описывать предметы и видимые следы, относящиеся к преступлению;

г) при описании этих объектов индивидуализировать предметы и следы, чтобы в дальнейшем исключить возможность их фальсификации, а в случае их утраты – основные параметры и признаки объектов остались бы зафиксированными в протоколе;

2) отразить наступившие в ходе осмотра различные обстоятельства (например, изменения погодных условий)»;

3) отметить, какие технические средства применялись для измерения, фотосъемки, видеозаписи; для выявления, изготовления слепков и других видов фиксации следов, условия их применения, полученные результаты.

Заключительная часть протокола

В конце протокола отмечаются:

1) время окончания осмотра;

2) объекты, обнаруженные, зафиксированные и изъятые при осмотре; описывается их упаковка, куда они направлены или кому переданы

для хранения;

3) заявления специалиста, «связанные с обнаружением, закреплением и изъятием доказательств» (ст. 131 УПК);

4) замечания понятых «по поводу произведенных действий» в ходе осмотра (ст. 135 УПК);

5) замечания иных участников осмотра (ст. 141 УПК);

6) прилагаемые к протоколу осмотра планы, схемы, фотографические негативы и снимки, слепки и оттиски следов, аудио- и видеокассеты (материалы), изготовленные при производстве осмотра.

Одним из самых важных следственных действий на первоначальном этапе расследования компьютерных преступлений является осмотр места происшествия. К проведению осмотра необходимо привлекать специалистов. Первейшей задачей осмотра является определение местонахождения всех

компьютеров, объединенных в систему или сеть. Местоположение компьютеров фиксируется в протоколе и отмечается в составленной схеме. В схеме также фиксируется "иерархия" соединений (одноранговая сеть, компьютеры-администраторы и компьютеры-пользователи и т.д.). Определяются способы объединения (локальная сеть, прямое подключение и т.д.). Выявляются способ связи компьютеров (сетевой кабель связи, контакт через ИК-порты, контакт через выход в Интернет и т.д.), аппаратура, используемая для связи компьютеров, нахождение на момент осмотра. Проверяется нахождение компьютера "в сети" или индивидуальная работа, а также конкретный домен или компьютер, с которым осуществляется контакт. Исследуются кабельные соединения сети на предмет проверки их целостности и определения посторонних включений. Выясняется политика администрирования сети (с какого терминала осуществляется управление). Дальнейший осмотр отдельных персональных компьютеров желательно начинать с компьютера-сервера (администратора сети).

При осмотре персональных компьютеров фиксируется выведенная на дисплей информация (желательно не только описать ее, но и сфотографировать), определяется работающая на момент начала осмотра программа (работающие программы). Выполнение программы должно быть остановлено и зафиксирован результат остановки выполняемой программы. Осматриваются и описываются в протоколе (а также могут быть сфотографированы) подключенные к компьютеру внешние устройства (внешние модемы, сканеры, принтеры, web-камеры и т.д.). Определяются тип и модель компьютера и периферийных устройств, проверяется возможное использование внешних накопителей (внешних винчестеров, "флэшек"). Проверяется наличие в дисководах дискет и дисков. При наличии принтера желательно распечатать "дерево каталогов" (перечень каталогов, содержащихся в компьютере). Некоторые авторы предлагают обязательный запуск при осмотре компьютера антивирусных программ, однако нам представляется, что такая проверка не всегда возможна: проверка антивирусными программами пользователя необязательно даст необходимый результат, поскольку у пользователя могут быть устаревшие антивирусные базы; запуск программы с переносного диска серьезно замедляет антивирусную проверку; большой объем винчестера и большое количество файлов на винчестере приведут к слишком продолжительной проверке; вирусы зачастую в первую очередь поражают системную область диска и антивирусные программы. Поэтому нам кажутся возможными осмотр компьютера без антивирусной проверки и последующая загрузка со "спасательной" дискеты. Информация, содержащаяся на компьютере, может быть скопирована на переносные винчестеры. В любом случае копируются на носители системные файлы и файлы протокола (log-файлы). Обязательно проверяются базы программ online- и offline-сетевого общения (электронная почта, mail-агенты, ICQ и т.д.).

Проверяется наличие классических трасологических следов (микрочастиц, следов рук и т.д.). Наиболее вероятные места обнаружения

данных следов - клавиши включения и перезагрузки компьютера, кнопки периферийных устройств, клавиатура, розетки, кнопки дисководов и выдвижения дискет, передняя поверхность системного блока, мышь и т.д.

В протоколе фиксируются все манипуляции, произведенные с компьютерными устройствами.

Проверяется возможность отключения компьютера без повреждения обрабатываемых файлов. При отключении компьютеров сети в первую очередь отключается компьютер администратора.

Перед изъятием должен быть решен вопрос об изъятии компьютера целиком или изъятии только жесткого диска компьютера с сохранением на нем данных оперативной памяти. Изымать компьютер целиком (и системный блок, и монитор, и периферийные устройства) желательно, когда исследованию должен быть подвергнут весь компьютер; когда на компьютере установлено уникальное аппаратное обеспечение, с которым связано программное обеспечение (работа компьютера возможна только при его определенной комплектации); когда пользователем установлен пароль на вход (имеется в виду пароль в BIOS); на месте производства следственного действия нет возможности копирования информации жесткого диска и в некоторых иных случаях. При упаковке компьютерной техники фиксируется схема соединений, опечатываются кнопки и разъемы. Каждое устройство упаковывается отдельно в фиксированном положении во избежание повреждений.

Кроме компьютерных устройств, осматриваются и изымаются носители информации: диски, дискеты, съемные винчестеры, "флэшки" и т.д. Описываются их тип, модель, внешний вид, наличие фирменных обозначений, содержащаяся информация, наличие следов пальцев на поверхности носителя. Каждый носитель упаковывается отдельно.

Следует отметить, что любую компьютерную технику и носители следует оберегать от влажности, воздействия высоких или низких температур, электромагнитных полей и т.д.

Осмотр документов (источников и носителей криминалистически значимой компьютерной информации, документации, различных записей, даже на клочках бумаги) может иметь значение для успешного достижения цели. На начальном этапе следователь получает общее представление о документе, выясняя следующие обстоятельства:

что представляет собой документ;

у кого и где он хранится; внешний вид документа и его реквизиты; происхождение документа, от кого поступил адресату. При осмотре документа — вещественного доказательства следователь доступными ему средствами решает вопрос о его подлинности, изучая содержание и форму документа, материал и его отдельные части, подписи, оттиски печатей и штампов и др.

При осмотре электронных документов определяются их местонахождение (конкретный носитель и "адрес" на носителе, атрибуты файла (архивный, скрытый, системный и т.д.), формат (doc, rtf, html, txt и т.д.), объем файла,

время создания и изменения. Далее включается соответствующая программная оболочка (WordPad, Word и т.д.), в которой и открывается файл. В открытом документе изучается содержащаяся информация (по критериям, аналогичным исследованию письменной речи).

Обыск

Обыск - это следственное действие, содержанием которого является принудительное обследование помещений, участков местности, отдельных граждан, их одежды и вещей в целях обнаружения и изъятия источников доказательственной и ориентирующей информации (орудий преступления, предметов и ценностей или иных веществ, добытых преступным путем или могущих иметь значение для дела), а также обнаружения разыскиваемых лиц и трупов или сведений о их местонахождении.

По последовательности различают обыск первоначальный (первичный) и повторный. Как правило, повторный проводится, когда возникают сомнения в полноте и тщательности ранее проведенного обыска, либо, когда поступает информация о месте нахождения искомых предметов, не обнаруженных при первичном обыске, или относимости к делу определенного объекта, обнаруженного, но не изъятого при первоначальном обыске.

Принято различать в зависимости от специфики подлежащего обыску объекта:

- обыск помещений;
- личный обыск;
- обыск местности (необходимо отметить, что участки местности, не входящие в чье-либо правомерное владение, не обыскиваются; в случае необходимости отыскать на этих участках какие-либо объекты проводится следственный осмотр);
- обыск транспортных средств.

Задачи, цели и общие положения проведения обыска

Конкретные цели обыска определяются следователем в зависимости от обстоятельств расследуемого преступления и собранных данных.

Исходя из того, что обыск как следственное действие, носит ярко выраженный поисковый характер, а следователю, иных оперативным работникам необходимо найти орудия преступления, предметы и ценности, как правило спрятанные, укрытые обвиняемым, можно сформулировать его основные задачи:

1. Обнаружение и изъятие объектов, которые могут иметь доказательственное значение по делу (речь идет прежде всего о предметах, специально предназначенных для совершения преступления; предметах общего обихода, использовавшихся в преступных целях; о предметах и ценностях, добытых преступным путем и т.д. Большое значение по делу может иметь обнаружение документов, в том числе личных писем, служебной переписки, черновых записей, просмотр бухгалтерской

документации и т. п., а также имеющих отношение к делу фото-, видеоматериалов, магнитных записей). По делам о преступлениях против личности, например, нередко важные сведения содержат частная переписка обыскиваемого, записные книжки, дневники и т.д. Обнаруженные при обыске документы могут дать материал для характеристики личности обыскиваемого, установления его связей, намерений. Подлежат изъятию и документы, указывающие на местонахождение имущества (аккредитивы, сберегательные книжки, кредитные пластиковые карточки и т.п.) или на факт владения обыскиваемым определенным имуществом (сохранные квитанции, расписки, кассовые чеки, фабричные ярлыки, паспорта, гарантийные свидетельства, различная документация имущественного характера, заверенная нотариусом и т.п.).

2. Обнаружение и изъятие предметов, документов и веществ, хранящихся без надлежащего разрешения, запрещенных в гражданском обороте или изъятых из него (этими объектами могут быть радиоактивные вещества; наркотики, а также любая разновидность наркотиков или исходных компонентов для их синтетического изготовления и ядовитые материалы; незаконнохранящееся оружие и боеприпасы к нему и т.д.).

3. Обнаружение разыскиваемых лиц либо трупов, а также любых материалов, облегчающих их розыск. Это касается как непосредственного обнаружения лица, скрывающегося, например, в жилом помещении, или трупа, захороненного на приусадебном участке, в подвале, сарае и т. п., так и обнаружения материалов, указывающих на возможное местонахождение разыскиваемого лица или скрываемого трупа.

4. Обнаружение ценностей, других предметов или документов, наличие которых позволяет выдвинуть версию о совершении других преступлений помимо расследуемого, обусловившего проведение обыска.

Основанием для производства обыска должны быть достоверные данные процессуального характера или данные, полученные из непроцессуальных источников, в том числе в результате проведения определенных оперативно-розыскных мероприятий. Действующий УПК РФ конкретизирует основания производства данного следственного действия. Необходимо наличие достаточных данных для того, чтобы полагать, что в каком-либо месте или у какого-либо лица могут находиться орудия преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела.

Проводящие данное следственное действие сотрудники должны досконально ориентироваться в процессуальных вопросах проведения обыска. Общими для всех обыскивающих являются следующие положения:

* обыск производится на основании постановления следователя (оно должно быть мотивировано (ч. 2 ст. 182 УПК РФ), содержать указание, возможно в общей форме, что или кто будет отыскиваться при обыске, фактические его основания и указание места его проведения);

* при производстве обыска обязательно участие понятых;

* до начала обыска следователь предъявляет постановление о его производстве, а в случаях, когда обыск производится в жилище, - судебное

решение, разрешающее его производство (в этом судебном заседании вправе участвовать следователь и прокурор для обоснования ходатайства);

* при обыске должно быть обеспечено присутствие лица, у которого производится обыск, либо совершеннолетних членов его семьи;

* с разрешения следователя при обыске могут присутствовать защитник, а также адвокат того лица, в помещении которого производится обыск;

* производство обыска в ночное время (с 22 до 6 часов), кроме случаев, не терпящих отлагательств, не допускается;

* следователь должен принимать меры к тому, чтобы не были оглашены выявленные в ходе обыска обстоятельства частной жизни обыскиваемых и других лиц;

* все помещения, не используемые на законных основаниях для постоянного или временного проживания, могут подвергаться обыску на основании постановления следователя (офисы, рабочие кабинеты, магазины, ларьки и.т.д.);

* следователь вправе вскрывать любые запертые помещения, если владелец отказывается добровольно открыть их, избегая при этом не вызываемого необходимостью повреждения запоров, дверей и иных предметов;

* следователь вправе запретить лицам, присутствующим на месте, где производится обыск, покидать его, а также общаться друг с другом и иными лицами до окончания обыска;

* следователь вправе подвергнуть личному обыску лиц, находящихся в помещении или ином месте, в котором производится обыск (при наличие оснований полагать, что они скрывают на себе предметы или документы, которые могут иметь значение для уголовного дела);

* изымаются все обнаруженные предметы и документы, изъятые из оборота;

* все изымаемое предъявляется понятым и другим лицам, присутствующим при обыске, подробно описывается в протоколе обыска или прилагаемой к нему описи, а в случае необходимости упаковывается и опечатывается следователем на месте производства обыска, удостоверяется их подписями;

* в протоколе должно быть указано, где и при каких обстоятельствах были обнаружены изымаемые объекты, выданы они добровольно или изъяты принудительно;

* в протоколе помимо точного указания количества и индивидуальных признаков изымаемых объектов требуется указать их точную меру, вес и по возможности стоимость;

* если в ходе обыска были предприняты попытки уничтожить или спрятать подлежащее изъятию, то об этом делается соответствующая запись в протоколе и указываются принятые меры;

* копии протокола и прилагаемой к нему описи изъятого имущества или имущества, на которое был наложен арест, вручается обыскиваемым,

если обыск производился в помещении организации, то копия вручается ее представителю (ч. 15 ст. 182 УПК РФ).

В случае отказа владельца добровольно открыть запертые помещения и иные хранилища следователь вправе их вскрыть. При этом он должен стараться не причинять каких-либо излишних повреждений имуществу. Владельцу целесообразно разъяснить неправильность его поведения и ознакомить с содержанием ч. 6 ст. 182 УПК РФ. Для вскрытия хранилищ может быть привлечен специалист.

В случае отсутствия обыскиваемого или членов его семьи на месте обыска следователь:

1. принимает меры к их вызову, не называя истинной причины (можно направить сотрудника уголовного розыска с поручением доставить обыскиваемого к месту обыска);

2. дожидается обыскиваемого или членов его семьи либо оставляет кого-либо из сотрудников, поручив им немедленно сообщить о прибытии указанных лиц;

3. если помещение не закрыто, начинает обыск в присутствии представителей жилищно-эксплуатационной организации или любого официального лица, имеющего отношение к данному помещению в связи с исполнением своих служебных обязанностей;

4. установив, что обыскиваемый или члены его семьи куда-то скрылись или выехали, вскрывает запертое помещение и проводит обыск в присутствии представителей жилищного управления или местных органов управления (администрации).

Компьютеры и их комплектующие опечатываются путем наклеивания на разъемы листа бумаги и закрепления его краев на боковых стенках компьютера густым клеем или клейкой лентой, чтобы исключить возможность работы с ними в отсутствие владельца или эксперта. Магнитные носители упаковываются, хранятся и перевозятся в специальных экранированных контейнерах или в стандартных дискетных или иных алюминиевых футлярах заводского изготовления, исключающих разрушающее действие различных электромагнитных и магнитных полей и наводок, направленных излучений. Опечатываются только контейнеры или футляры. Пояснительные надписи могут наноситься только на специальные самоклеящиеся этикетки для дискет, причем сначала делается надпись, а потом этикетка наклеивается на предназначенный для этого участок на дискете. Если на дискете уже имеется этикетка с какой-либо надписью, проставляется только порядковый номер, а пояснительные надписи под этим номером делаются на отдельном листе, который вкладывается в коробку. Недопустимо приклеивать что-либо непосредственно к магнитным носителям, пропускать через них бечеву, пробивать отверстия, наносить подписи, пометки, печати и т.д.13

Как правило, изъятые в результате обыска компьютеры впоследствии направляются на компьютерно-техническую экспертизу. Результаты этой экспертизы зависят напрямую от сохранности информации на внутренних и

внешних магнитных носителях. Весьма важно в связи с этим соблюдать правила доставки компьютерной техники с места производства обыска в кабинет следователя для последующего направления на экспертизу.

Перевозка и хранение компьютерной техники должны осуществляться в условиях, исключающих ее повреждение. При перевозке и складировании недопустимо ставить компьютеры один на другой, размещать на них какие-либо другие предметы. Хранят компьютеры и комплектующие в сухом, отапливаемом помещении

Перед началом обыска принимаются меры к предотвращению повреждения или уничтожения информации:

- осуществляется контроль за бесперебойным электроснабжением ЭВМ в момент осмотра;
- удаляются все посторонние лица с территории, на которой производится обыск, и прекращается доступ на нее;
- оставшиеся на территории лица лишаются доступа к средствам вычислительной техники и к источникам электропитания;
- эвакуируются находящиеся на объекте взрывчатые, легковоспламеняющиеся, едкие вещества, посторонние источники излучения и другие предметы и аппаратура, способные привести к аварии ЭВМ.

Обыск целесообразно производить с участием специалиста в области судебной компьютерно-технической экспертизы и специалиста-криминалиста, поскольку на компьютерных средствах зачастую оказываются следы рук, а также обнаруживаются рукописные и печатные документы. Желательно в качестве понятых приглашать квалифицированных пользователей ЭВМ.

Не следует ограничиваться поиском информации только в компьютере; необходимо внимательно осмотреть имеющуюся документацию, вплоть до записей на клочках бумаги. Поэтому любые обнаруженные носители информации должны быть изъяты и изучены.

Производство обыска в помещениях, где находится много компьютерных устройств, работает множество людей, сопряжено со значительными трудностями. Для проведения такого объемного и крупномасштабного следственного действия зачастую необходимо привлечение большого количества работников правоохранительных органов, включая сотрудников силовых подразделений, поскольку лица, в отношении которых расследуется уголовное дело, часто оказывают серьезное сопротивление. Число участников такого объемного следственного действия достигает нескольких десятков, а подчас и сотен, поэтому главным элементом его проведения является четкая организация, инструктаж каждого участника о целях и задачах следственного действия.

Важнейшими условиями успеха в этом случае являются: собирание информации об объекте осмотра или обыска; составление плана осмотра или обыска с детальной регламентацией задач каждого участника; определение

состава следственно- оперативной группы; обеспечение оперативной группы необходимыми техническими средствами.

При подготовке к обыску необходимо определить: количество компьютеров и их типы; организацию электропитания и наличие автономных источников питания; используемые носители компьютерных данных; наличие локальной сети и выхода в другие сети с помощью модема, радиомодема или выделенных линий; используемое системное и прикладное программное обеспечение; наличие систем защиты информации, их типы; возможности использования средств экстренного уничтожения компьютерной информации; квалификацию пользователей, а также взаимоотношения в коллективе сотрудников, обслуживающих технику.

Полезно допросить (опросить) администратора системы (системного администратора) и выяснить: какие операционные системы установлены на каждом из компьютеров; какое используется программное обеспечение; какие применены системы защиты и шифрования; где хранятся общие файлы данных и резервные копии; каковы пароли супервизора и администраторов системы; какие зарегистрированы имена и пароли пользователей.

Для успешного проведения обыска особое значение имеет фактор внезапности. В противном случае подозреваемый (обвиняемый) может быстро уничтожить изобличающие его материалы, находящиеся в ЭВМ или на магнитных носителях. Если получены сведения о том, что компьютеры организованы в локальную сеть, по возможности следует установить местонахождение всех компьютерных устройств, подключенных к этой сети. При этом проводится групповой обыск одновременно во всех помещениях, где установлены компьютерные средства.

Рабочий этап обыска включает обзорную и детальную стадии. На обзорной стадии следователь корректирует и пополняет данные об объекте, фиксирует участки, требующие особого внимания. Следует обратить внимание на неподключенные разъемы на коаксиальном кабеле и свободные розетки (розетки для подключения компьютеров в локальную сеть, использующие витую пару). В этих местах, возможно, находились компьютеры или подключались портативные компьютеры, которые в момент проведения следственного действия могут находиться в другом месте или быть спрятаны. На этой стадии уточняется распределение объектов между участниками обыска.

На детальной стадии осуществляются непосредственный поиск, обнаружение и изъятие объектов обыска— компьютерных средств и криминалистически значимой компьютерной информации. Может быть использован как последовательный, так и выборочный методы обследования. При большом сосредоточении компьютерных устройств последовательный поиск занимает слишком много времени. Поэтому необходимо в первую очередь осматривать те компьютерные средства, которые выбраны на подготовительном этапе. Другой причиной выбора того или иного компьютерного средства является подозрительное поведение обыскиваемого, его неубедительные объяснения поданному устройству, файлу, программе,

несоответствие обнаруженных компьютерных средств или программ личности обыскиваемого.

Для сокрытия информации на компьютерах могут быть установлены специальные защитные программы, которые при определенных условиях автоматически производят полное или частичное стирание информации. Это высокая степень защищенности компьютерной информации. Низкая степень защищенности определяется наличием простого алгоритма ограничения доступа (например, данные защищены только паролем), получением достоверных данных о его преодолении.

Включать и выключать компьютеры, производить с ними какие-то манипуляции может только специалист, участвующий в производстве данного следственного действия. Если на объекте было отключено электроснабжение (например, в связи с пожаром или взрывом), до его включения следует проверить, всели компьютеры и периферийные устройства находятся в отключенном состоянии.

Если компьютер на момент начала обыска оказался включен, необходимо оценить информацию, отображенную на мониторе, и определить, какая программа выполняется в данный момент. В случае работы стандартного программного обеспечения нельзя приступать к каким-либо манипуляциям на входе без предварительного визуального осмотра технических средств. Экран монитора нужно сфотографировать, а также отключить все телефонные линии, подключенные к компьютеру.

В протоколе необходимо описать все соединения на задней стенке системного блока. Если это признано целесообразным, вскрывается кожух системного блока и визуально определяется конфигурация ЭВМ, описывается месторасположение электронных плат.

В случае если при осмотре аппаратных средств выявлены неизвестные участникам следственного действия устройства (платы расширения, нестандартные соединения и т. д.), компьютер необходимо сразу выключить. При этом следует не отключать тумблер блока питания, а вынимать вилку из розетки.

Затем следует промаркировать всю систему подключения до того, как провода будут отсоединены; промаркировать все порты и разъемы с тем, чтобы потом можно было осуществить точную реконструкцию расположения кабелей, плат расширения и других устройств. Если конфигурация процессора стандартна, следует корректно завершить работу исполняемой в данный момент программы либо дождаться завершения се работы для получения дополнительных, возможно искомых, данных.

Если для поиска информации задействуется программное обеспечение, не находящееся в компьютере, это необходимо отмстить в протоколе. Такие программы должны быть стандартны и лицензированы, а контроль за их работой нагляден.

Особого внимания требуют места хранения носителей информации. Если при внешнем осмотре компьютеров в их составе обнаружены устройства типа стримера, магнитооптического накопителя и им подобные, то

необходимо найти места хранения носителей информации к соответствующим накопителям. Кроме того, в организациях с развитой локальной сетью, как правило, производится регулярное архивирование информации на какой-либо носитель. Только после выполнения указанных выше мероприятий специалист, участвующий в следственном действии, может произвести изъятие носителей информации.

В протоколе следственного действия следователь описывает основные физические характеристики изымаемых устройств, их видимые индивидуальные признаки, конфигурацию компьютерных средств (их комплектацию); номера моделей и серийные номера каждого из устройств; инвентарные номера, присваиваемые бухгалтерией при постановке средства на баланс организации; иную информацию, имеющуюся на фабричных ярлыках фирмы-изготовителя.

Выемка электронных документов и иной информации из вычислительных сетей. Законодатель пока не предложил детальной регламентации этого процесса, поэтому если необходимо произвести выемку электронной почты из домашнего компьютера, то это можно сделать путем изъятия самого компьютерного средства или жесткого диска. Как правило, операторы связи (провайдеры, предоставляющие абоненту услуги телематических служб сети Интернет) не хранят на своих серверах электронную почту абонентов, т. е. речь идет о еще не полученной электронной почте. В договорах о предоставлении Интернет- услуг обычно предусмотрены обязательства провайдера предпринимать общепринятые в Интернете технические и организационные меры для обеспечения конфиденциальности информации, получаемой или отправляемой абонентом. Доступ третьим лицам к информации, получаемой или отправляемой абонентом, обеспечивается исключительно в соответствии с законодательством Российской Федерации.

Собирание криминалистически значимой информации в вычислительной сети имеет свои особенности. В первую очередь необходимо установить общее количество компьютеров и их распределение по другим помещениям, а также количество и тип используемых серверов и рабочих мест. Далее важно выяснить тип используемой сетевой операционной системы и состав прикладного программного обеспечения, используемого в вычислительной сети. Следует также установить факт наличия резервных копий данных и места их хранения. Особое внимание должно уделяться выявлению выхода в другие, в том числе и глобальные, сети; установлению возможностей использования коммуникационных средств для связи с удаленными пользователями, другими организациями (фирмами), частными лицами.

В это же время определяются принятые в организации мероприятия по защите информации и наличие выхода в Интернет. В случае использования телефонной линии для связи с другими сетями обеспечить отключение телефона; по возможности удалить из помещения все взрывчатые, едкие и легковоспламеняющиеся материалы.

Для обеспечения сохранности информации необходимо: предотвратить отключение энергоснабжения организации, обеспечив охрану распределительного щита;

- запретить работникам организации и прочим лицам производить какие-либо манипуляции с компьютерными средствами;
- предупредить всех участников следственного действия о недопустимости самостоятельных манипуляций с компьютерными средствами;
- точно установить местоположение серверов; определить местоположение компьютеров, подключенных к вычислительной сети (иногда помогает электропроводка: достаточно проследить трассы кабелей или специальных коробов для защиты кабелей).

Следственная группа должна иметь физическую возможность одновременно занять все помещения, в которых находятся компьютеры, входящие в сеть. Наличие средств удаленного доступа позволяет оперативно манипулировать информацией в сети любым компьютером, входящим в нее.

Для производства обыска по месту жительства и работы подозреваемого желательно привлечение соответствующего специалиста. Очень важно обеспечить внезапность обыска для воспрепятствования уничтожению информации. После проникновения на объект блокируется доступ пользователей к компьютерам. При обнаружении запущенных программ удаления информации или форматирования выход осуществляется экстренным отключением компьютера. Само изучение компьютерной техники осуществляется аналогично проведению осмотра. Следует учитывать, что подключенные к компьютеру периферийные устройства, а также несколько компьютеров, объединенных в систему или сеть, могут находиться в разных помещениях. При обыске очень важны обнаружение и изъятие не только компьютерной техники и носителей, но также и компьютерных распечаток, отрывочных записей на листах бумаги или в блокноте. При изучении данных записей могут быть обнаружены: план совершения преступления, записи о системе защиты "пораженного" объекта, попытки подбора паролей и имен пользователей и т.д. Обнаруживается и изымается "хакерское", нелицензионное программное обеспечение на дисках и дискетах. Важно также обнаружить телефонные счета (в настоящее время обслуживание доступа в Интернет выделяется в счете отдельной строкой, и по размеру счета можно определить объем использованного интернет-времени).

В ходе обыска следует также обращать внимание на специфическую литературу по программированию, взлому, созданию вредоносных программ и т.д.

Информация о времени доступа в сеть и времени, проведенном в сети, может быть получена путем проведения выемок журналов регистрации или истребования сведений у провайдера.

Завершающим этапом осмотра, обыска или выемки по делам, сопряженным с использованием компьютерных технологий, являются

фиксация и изъятие компьютерных средств. От того, как произведены изъятие, транспортировка и хранение этих объектов, часто зависит их доказательственное значение. Все изъятые системные блоки и другие устройства должны быть упакованы и опечатаны таким образом, чтобы исключить возможность их повреждения, включения в сеть и разборки. В протоколе должны быть точно отражены место, время и внешний вид изымаемых предметов и документов. При изъятии компьютеров и носителей данных их следует упаковывать и опечатывать.

Фиксация результатов обыска

Основным средством фиксации хода и результатов данного следственного действия является протокол. Вместе с тем, справедливо мнение о том, что многообразные способы фиксации, установленные законом, можно объединить в несколько групп. Следует выделить: 1) знаковую форму фиксации, 2) предметную форму, 3) наглядообразную форму. Каждая из них отличается специфическим способом закрепления фактических данных, соответствующим особенностям отображаемых следов. Под фиксацией доказательств следует понимать систему осуществляемых в соответствии с уголовно-процессуальным законом действий следователя, направленных на преобразование воспринятой им доказательственной информации в форму, обеспечивающую максимально полное сохранение и использование полученных данных в целях доказывания.

При проведении обыска наиболее целесообразно проводить именно видеозапись. Просмотр видеозаписи обыска позволяет выявить упущения ведущего его лица, отметить реакцию обыскиваемых на поставленные следователем вопросы. Применение видеотехники послужит сдерживающим фактором, предотвратит возможность незаконных действий или аморальных проявлений отдельных лиц.

С помощью видеозаписи фиксируется весь ход обыска. Но видеозапись является лишь приложением к протоколу любого следственного действия. Фотографирование, видеосъемка, звукозапись не могут заменить собой протокола, а считаются факультативными средствами фиксации. Тем не менее, они наглядно фиксируют беседу, интонации, вызванные различными причинами паузы в ответах обыскиваемых. Данные приложения к протоколу нагляднее и полнее отражают происходящее.

Место расположения тайников, сами сокрытые объекты, система действий по их извлечению по возможности должна быть зафиксирована на фото- или видеосъемку. Для наглядной фиксации их местонахождения могут быть составлены схемы или планы. Приложения к протоколу в соответствии с ч. 8 ст. 166 УПК РФ, фиксирующие то или иное обстоятельство, более адекватно и наглядно отражают определенные фрагменты, фактические данные, которые могут быть трудно передаваемы протоколированием и фиксируются в нем в общей форме. Необходимо отметить, что отсутствие записи в протоколе обыска об изготовленных или составленных приложениях приводит к фактической утрате данных доказательств.

Согласно пп. 13 и 14 ст. 182 УПК РФ «В протоколе должно быть указано, в каком месте и при каких обстоятельствах были обнаружены предметы, документы или ценности, выданы ли они добровольно или изъяты принудительно». Если не будет зафиксировано место их обнаружения (само по себе указывающее на то – укрывались ли предметы и документы либо хранились открыто) доказательственное значение результатов обыска может быть ослаблено, или вообще утрачено.15 «Если в ходе обыска были предприняты попытки уничтожить или спрятать подлежащие изъятию предметы, документы или ценности, то об этом в протоколе делается соответствующая запись и указываются принятые меры».
Протокол обыска подписывается всеми участники данного следственного действия, копия протокола выдается лицу, у которого он производился.

Контрольные вопросы и задания

Контрольные вопросы

1. Как производится осмотр места происшествия?
2. Каковы общие правила обращения с СВТ и их носителями в ходе производства следственных действий?
3. Как производится обыск?
4. Каковы общие правила обращения с СВТ и их носителями в ходе производства следственных действий?
5. Каковы особенности проведения следственных действий при проведении расследований компьютерных преступлений?

Задания

1. Составить отчет об осмотре заданного гипотетического места преступления.

2. Составить отчет об обыске заданного гипотетического места преступления.

Литература по теме

1. http://lawdiss.org.ua/books/a1711.doc.html

2. Подготовка и производство обыска и выемки // Криминалистика / Под ред. д-ра юрид. наук, проф. В.А. Образцова - М.: Юрист, 2001, с. 473.

3. Хрусталев В.Н. Трубицын Р.Ю. Участие специалиста-криминалиста в следственных действиях. - СПб.: Питер, 2003, с. 17.

Тема 3 Тактика обнаружения, изъятия и фиксации компьютерной информации при производстве следственных действий. Следственные версии. Последующие этапы расследования компьютерных преступлений

Цель и задачи практического занятия

Изучить методику проведения следственного эксперимента

Дать студентам знания содержании допросов (опросов) потерпевших, свидетелей, подозреваемых

Анализ отечественного и зарубежного опыта показывает, что можно выделить три типичные следственные ситуации.

1. Собственник информационной системы собственными силами выявил нарушения целостности конфиденциальности информации в системе, обнаружил виновное лицо и заявил об этом в правоохранительные органы.

2. Собственник самостоятельно выявил указанные нарушения в системе, однако не смог обнаружить виновное лицо и заявил об этом в правоохранительные органы.

3. Данные о нарушениях целостности конфиденциальности информации в информационной системе и виновном лице стали общеизвестны или непосредственно обнаружены органом дознания (например, в ходе проведения оперативно-розыскных мероприятий по другому делу).

При наличии заподозренного виновного лица первоначальная задача следствия заключается в сборе с помощью собственника информационной системы и процессуальной фиксации доказательств:

а) нарушения целостности и конфиденциальности информации в системе;

б) размера ущерба, причиненного нарушением целостности конфиденциальности информации;

в) причинной связи между действиями, образующими способ нарушения, и наступившими последствиями путем детализации способа нарушения целостности конфиденциальности информации в системе и характера совершенных виновным действий;

г) отношения виновного лица к совершенным действиям и наступившим последствиям.

При отсутствии заподозренного виновного лица первоначальная задача следствия заключается в сборе с помощью собственника информационной системы и процессуальной фиксации указанных выше доказательств, за исключением указанных в пункте «г».

Следует принять меры к розыску виновного и поиску его рабочего места, откуда осуществлялось вторжение в информационную систему.

Осуществляется поиск:

- места входа в данную информационную систему и способа входа в систему — вместе и с помощью должностных лиц собственника информационной системы;

- путей следования, через которые вошел в «атакованную» систему злоумышленник или проникли его программы — вместе и с помощью должностных лиц иных информационных и коммуникационных систем — до рабочего места злоумышленника.

Такое место, как указывалось, может быть как по месту его службы, так и дома, а также в иных местах, где установлена соответствующая аппаратура (например, студенческие вычислительные центры и др.).

При выдвижении версий совершения преступлений в сфере компьютерной информации необходимо учитывать, что они совершаются обычно группой из двух и более человек, хотя не исключена возможность работы преступника-одиночки. В таком случае он сам или, если действует группа, один из ее членов является либо сотрудником данного учреждения, либо имеет свободный доступ к компьютерам (представитель службы технической или программной поддержки, программист, работающий по контракту, и т.д.), умеет работать с вычислительной техникой, хорошо представляет, какая информация и где расположена в компьютере.

Интерес обычно представляет информация, содержащая государственную или коммерческую тайну (например, информация из базы данных о передвижении оружия, наркотиков и т.д.).

В основном, как правило, информация преступниками копируется на магнитный носитель, хотя не исключена возможность ее передачи по сетям телекоммуникации, распечатки на бумаге, кино-, фото-, видеосъемки изображения экрана и действий оператора или перехвата с помощью специальных технических средств. Копирование может осуществляться на портативный компьютер (Notebook) с подключением его как к локальной вычислительной сети, так и непосредственно к последовательному или параллельному порту конкретной ЭВМ с помощью специального кабеля.

Преступление обычно происходит в рабочее время и внешне не отличается от обычной работы в учреждении. Похищенная информация используется в дальнейшем самими преступниками для подготовки хищений или может быть продана заинтересованным лицам.

Учитывая конкретные обстоятельства, следователем могут быть выдвинуты и проверены следующие общие версии:

- преступление совершено сотрудником данного учреждения либо лицом, имеющим свободный доступ к компьютерной технике;

- преступление совершено сторонним лицом, входящим в круг родственников, друзей, знакомых сотрудников учреждений;

- преступление совершено группой лиц по предварительному сговору или организованной группой с участием сотрудника данного учреждения либо лица, имеющего свободный доступ к компьютерной технике и в совершенстве владеющего навыками работы с ней;

- преступление совершено лицом или группой лиц, не связанных с деятельностью учреждения и не представляющих ценность компьютерной информации.

Приведенный перечень следственных версий является общим и в зависимости от конкретной ситуации может быть расширен.

Последующие этапы расследования компьютерных преступлений

На последующем этапе расследования компьютерных преступлений могут быть проведены очные ставки, допросы обвиняемых, следственные эксперименты, экспертизы и иные процессуальные действия.

Очные ставки могут быть проведены между соучастниками компьютерного преступления или подозреваемыми (обвиняемыми) и свидетелями или потерпевшими при наличии в их показаниях существенных противоречий.

При **допросах подозреваемых и обвиняемых** необходимо учитывать данные криминалистической характеристики о личности предполагаемого преступника.

При первоначальном допросе, побуждая лицо к деятельному раскаянию, необходимо выяснить:

- какие изменения в работу компьютерных систем были внесены;
- какие вирусы использовались;
- есть ли, с точки зрения подозреваемого (обвиняемого), возможность быстро устранить или уменьшить вред, причиненный несанкционированным проникновением в систему; какие сведения и кому передавались.

При допросах свидетелей и потерпевших необходимо выяснить:

- назначение и функции компьютерной системы; кто имел доступ к ней и в помещения, где располагалась компьютерная техника;
- не появлялись ли там посторонние лица; какие средства защиты использовались; кто санкционировал доступ к информации (если она была закрытой) и кто реально был допущен;
- какой вред (имущественный, неимущественный) причинен преступлением и имеются ли способы его уменьшить.

С помощью следственного эксперимента могут быть проверены профессиональные навыки злоумышленника: способность "взломать" компьютер при удаленном доступе к нему или шифры и пароли доступа при работе на самом "взламываемом" терминале, создать "хакерскую" или вредоносную программу, возможность "взломать" компьютер определенным способом, возможность появления на экране "закрытой" информации вследствие ошибки, программной или администратора, сбоя в компьютерном оборудовании, возможность наступления определенных последствий при нарушении конкретных правил пользования компьютером и т.д. При проведении следственного эксперимента необходимо использовать компьютерную технику и программное обеспечение, аналогичные тем, которые стали объектами преступного посягательства или средствами

совершения преступления. С помощью следственного эксперимента может быть также проверена надежность средств защиты.

Контрольные вопросы и задания

Контрольные вопросы

1 Как выдвигаются следственные версии?

1 Каковы общие обстоятельства, подлежащие установлению при расследовании компьютерных преступлений в обязательном порядке?

2 Что выясняется на допросах?

4 Что проверяется при следственном эксперименте?

Задания

1 Составить отчет о выдвинутых следственных версиях заданного гипотетического преступления.

3. Составить отчет о проведении следственного эксперимента при расследовании заданного гипотетического преступления..

Литература по теме

1 http://bookzie.com/book_7_glava_17_Glava_4_UCHENIE_O_SLEDSTVENNOJ.html

2 http://www.bibliotekar.ru/criminalistika-1-2/85.htm

3 http://bookzie.com/book_7_glava_17_Glava_4_UCHENIE_O_SLEDSTVENNOJ.html

4 http://www.bibliotekar.ru/criminalistika-1-2/85.htm

Тема 4 Организационно-правовые задачи по преступлениям в информационной сфере.

Цель и задачи практического занятия

Дать студентам знания о решении практико-ориентированных задач по преступлениям в области компьютерной информации на основе фактов из реальной жизни.

Примеры задач и их решения.

Задача 1. Сотрудник МВД при проведении служебных совещаний, на которых обсуждались сведения, составляющие государственную тайну (далее - ССГТ), брал с собой смартфон. Им неоднократно фотографировались ССГТ, чтобы затем использовать эти сведения в служебной деятельности.

Контрольные вопросы и задания

Контрольные вопросы

Правомерно ли был им получен доступ к ССГТ? Соблюдал ли он правила ознакомления с ССГТ? Где он мог делать пометки со служебных совещаний?

Задание

Дайте анализ состава правонарушения.

Вариант решения. Сотрудник в своей деятельности нарушил внутренний приказ министра своего ведомства а также закон о ГТ, который предписывает при обработке ССГТ использовать только учтённые носители, которые хранятся и учитываются особым образом. Его действия имели предпосылку к ознакомлению с ССГТ неограниченного круга лиц. В ходе очередного совещания, его действия были замечены начальником подразделения и было начато служебное разбирательство по данному факту. В результате этого разбирательства, при осмотре устройства и дачи показаний было выяснено, что эти фотографии пересылались сотрудником в мессенджерах коллегам по работе и было обсуждение служебных вопросов. Действия сотрудника нарушают ст. 12 ФЗ № 5485-1, т.к. носитель сведений, составляющих ГТ не был учтен соответствующим 26 образом, на него не были нанесены реквизиты и его хранение и перемещение было бесконтрольным, что могло повлечь к разглашению сведений составляющих ГТ неограниченному кругу лиц. Действия должностного лица подпадают под действие ст. 283 УК РФ, ч.2 и предусматривают наказание в виде лишения свободы от 3 до 7 лет с лишением права занимать определенные должности на срок до 3 лет. Возможно, при дальнейшем разбирательстве будет установлена ответственность и по ст. 284 УК РФ, что предусматривает наказание в виде лишения свободы до 3 лет с лишением права занимать определенные должности на срок до 3 лет.

.

Задача 2. Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления

контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема - одного из элементов компьютерной системы.

Контрольные вопросы и задания

Контрольные вопросы

Подлежит ли привлечению к уголовной ответственности Шатурин?

Что понимается под информационно-телекоммуникационными сетями и оконечным оборудованием в смысле ст. 274 УК РФ? Какие виды оконечного оборудования возможны? Относится ли к оконечному оборудованию телефонный модем?

Задание

Дайте анализ состава правонарушения.

Вариант решения.

В деянии Шатурина можно усмотреть признаки состава преступления, предусмотренные ст. 274 УК РФ «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно телекоммуникационных сетей ». законодательная база для решения задачи – ст. 274 УК РФ, примечания к ст. 272 УК РФ

Родовым объектом данного преступления являются общественная безопасность и общественный порядок; видовым – отношения в сфере компьютерной безопасности. Непосредственный объект – это отношения, обеспечивающие правила эксплуатации хранения, обработки, передачи компьютерной информации и информационно-телекоммуникационных сетей. Объективная сторона преступления сконструирована в качестве материального состава. Обязательные условия наступления уголовной ответственности – причинение крупного ущерба. В деянии Шатурина усматриваются отдельные признаки объективной стороны деяния, в частности, нарушения правил эксплуатации информационно-телекоммуникационных сетей. Он также обладает признаками субъекта данного преступления – вменяем и достиг 16 лет. Субъективная сторона преступления характеризуется виной как в форме умысла, так и неосторожности. Однако, вопрос об уголовной ответственности Шатурина

зависит от того, в каком размере был причинен ущерб его деянием, так как состав преступления является материальным. Согласно 28 примечанию к ст. 22 УК РФ крупным ущербом в статьях данной главы признается ущерб сумма которого превышает один миллион рублей. Таким образом, Шатурин будет подлежать уголовной ответственности по ч. 1 ст. 274 УК РФ, если его деянием причинен ущерб на сумму свыше одного миллиона рублей.

Перечень заданий по теме 4

Номера студентов по списку группы в ЭИОС	**Задачи**
	Группа ПТв1
1-8	Начальник отдела новых разработок в военном НИИ ехал на доклад в вышестоящий орган управления. Для доклада им были взяты носители сведений, составляющие государственную тайну (далее – ССГТ), соответствующие грифу «Секретно». В процессе транспортировки носители были утеряны. Как были подготовлены документы к перевозке? Выделялась ли охрана, был ли проведён инструктаж перед убытием? Где и при каких обстоятельствах произошла утеря? Имел ли начальник отдела корыстный умысел?
9-15	При проведении комплексной проверки дочернего предприятия, комиссия из головного офиса отправляла сведения об основных направлениях деятельности к вышестоящим начальникам. Отправка происходила по каналам электронной почты без дополнительных мероприятий по защите информации. В результате конкурирующей фирме стали известны сведения, составляющие коммерческую тайну дочернего предприятия. Были ли выполнены мероприятия по защите коммерческой тайны? Были ли ознакомлены сотрудники предприятия 29 и члены комиссии с внутренними документами по обеспечению безопасности информации, составляющей КТ?
16-23	Сотрудник фирмы использовал в своей служебной деятельности документацию о устройстве станка, составляющую ноу-хау предприятия. Им она была получена от коллеги при переводе в отдел. При переходе из основного корпуса в технологический, по улице был 30 остановлен сотрудником подразделения информационной безопасности. Были ли эти сведения коммерческой тайной предприятия? Был ли ознакомлен сотрудник с перечнем сведений и с правилами работы с КТ?
24-30	За опубликование редакцией газеты "Лабинские вести" материалов, которые содержали персональные данные несовершеннолетней гражданки, а именно фамилии, имени, сведений о школе, в которой обучается несовершеннолетняя, без ее согласия и согласия ее законного представителя, а также ряда других статей с персональными данными несовершеннолетних, Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций вынесло письменное предупреждение о недопустимости распространения через средство массовой информации сведений, составляющих специально охраняемую законом тайну, главному редактору СМИ газеты "Лабинские вести". Однако, главный редактор не отреагировала на это предупреждение и продолжала публиковать персональные данные граждан без их согласия. Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций обратилось в Краснодарский краевой суд с исковым заявлением о прекращении деятельности газеты "Лабинские вести". Оцените ситуацию и разрешите спор с точки зрения норм права.
	Группа ПТ1
1-8	Гражданин обратился в районный суд Санкт-Петербурга с исковым заявлением к ЗАО

	"Издательский дом "Комсомольская правда" о признании незаконным распространение газетой "Комсомольская правда" персональных данных, а также его личного изображения. Кроме того, гражданин просил взыскать с редакции газеты компенсацию морального вреда и опубликовать в ближайшем планируемом выпуске газеты "Комсомольская правда" опровержение. Причиной для такого обращения в суд послужил тот факт, что газета "Комсомольская правда", зарегистрированная как электронное средство массовой информации в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций опубликовала в сети интернет статью. В этой статье содержалось интервью журналиста с гражданином с размещением его личной фотографии, а также упоминаются сведения о личной жизни гражданина, по большей части не соответствующие действительности и его персональные данные. Поскольку, гражданин уверен, что не давал такого интервью, не принимал какого-либо участия в размещении статьи, а также не давал кому-либо разрешения на опубликование своего изображения, в том числе, в данной газете, он обратился в суд. Разрешите спор согласно действующему законодательству.
9-15	После нескольких безрезультатных попыток проверить электронную почту дома, Миша решил сходить на работу к своему отцу и повторить попытку, используя рабочий компьютер родителя. Получив одобрение отца, Миша пришел в офис во время обеденного перерыва, чтобы не отвлекать никого от работы (не нарушать течение рабочего процесса). Когда мальчик вошел в почтовую систему, то он увидел 7 новых писем. Некоторые из этих писем он не стал просматривать, сразу определив их как спам, а остальные начал внимательно читать и отвечать на них. Особое внимание вызвало последнее письмо с заманчивой темой «Веселый прикол», полученное от Димы. После того как Миша щелкнул по пиктограмме конверта и перешел по гиперссылке, он увидел письмо и прикрепленный файл «prikol.exe». Мальчик не стал читать письмо, так как уже заканчивался обеденный перерыв, и сразу начал скачивать прикрепленный файл. Через несколько секунд после начала скачивания, экран монитора стал черным, а системный блок начал сильно пищать. Испугавшись, Миша позвал папу, который сразу сказал, что это опасный вирус, “гуляющий ” в настоящее время по интернету, заблокировал работу компьютера. Однако вместе с папиным компьютером были поражены до конца рабочего дня и все компьютеры, подключенные по локальной сети. Приведение компьютерной сети в рабочее состояние потребовало значительных усилий и времени. Определите, что произошло, чья вина и какова ответственность за подобного рода происшествия?
16-23	Аспирант университета Хохлов занимался исследовательской работой по компьютерной "вирусологии". Целью работы было выяснение масштаба глобальной сетевой инфраструктуры. В результате ошибки в механизме размножения вирусы, так называемые "сетевые черви", проникли в университетскую компьютерную сеть и уничтожили информацию, содержащуюся в компьютерах факультетов и подразделений. В результате этого были полностью уничтожены списки сотрудников университета, расчеты бухгалтерии по зарплате, повреждены материалы научно исследовательской работы, в том числе "пропали" две кандидатские и одна докторская диссертации. Решите вопрос о правомерности действий Хохлова. В чем заключается субъективная сторона преступлений в сфере компьютерной информации? Какова ответственность за действия Хохлова предусмотрена действующим законодательством.
24-30	Студент технического вуза Иванченко во время занятий по информатике подключился к сети "Интернет" и регулярно получал в течение семестра материалы разного содержания, в том числе и сексуального характера. В конце семестра в институт поступил запрос о работе в "Интернет" и пришел чек на оплату 105 часов пребывания в сети "Интернет". Руководство института поставило вопрос о привлечении Иванченко к уголовной и гражданской ответственности. Дайте правовую оценку действиям студента Иванченко.
	Группа ПТ2
1-8	Оператор ЭВМ одного из государственных учреждений Утевский, используя многочисленные дискеты с информацией, получаемые от сотрудников других организаций, не всегда проверял их на наличие "вирусов", доверяясь заверениям поставщиков о том, что "вирусов" нет. В результате этого в компьютер Утевского, а затем и в компьютерную сеть учреждения попал комбинированный вирус, что привело к утрате информации, содержащей государственную тайну, и поставило под угрозу срыва запуск одного из космических объектов. Дайте юридический анализ действий Утевского. Что следует понимать под тяжкими последствиями нарушений правил эксплуатации информационно-телекоммуникационных сетей?
9-15	Савченко осуществлял рассылку подложных электронных писем с целью завладения персональной информацией клиентов «Ситибанка». Рассылка представляла собой

	электронное письмо с сообщением о переводе 100 долларов США на личный счет клиента и содержала просьбу зайти в систему Интернет-бакинта «CitibankOnline» для подтверждения перевода. В случае следования по указанной ссылке происходило попадание на сайт, созданный Савченко, и очень похожий на стартовый экран «CitibankOnline». Десять человек ввели номер кредитной карты и пин-код для того, чтобы войти в систему. Воспользовавшись полученной таким образом информацией, Савченко совершил завладение денежными средствами Павлова и Костенко, находящимися в Ситибанке, в сумме 15 и 20 тысяч долларов соответственно. Квалифицируйте содеянное Савченко, дайте правовую оценку.
16-23	Гуляшов, студент факультета вычислительной математики, организовывал сетевые атаки, заключающиеся в получении обманным путем доступа в сеть посредством имитации соединения. Таким образом, он получил доступ к информации о счетах пользователей интернета и номерах некоторых кредитных карт и пин кодов. Полученную информацию Гуляшов передавал Сорокиной за вознаграждение, которая использовала ее для хищения денежных средств. Что такое фишинг, спуфинг и фарминг? Признаки какого явления усматриваются в деянии Гуляшова? Фишинга, спуфинга или фарминга? Квалифицируйте содеянное Гуляшовым и Сорокиной.
24-30	ГУВД Московской области было возбуждено уголовное дело по факту совершение неправомерного доступа в охраняемой законом компьютерной информации в кассовых аппаратах одного из индивидуальных предпринимателей г.Павловский-Посад Лебедева. Следствие квалифицировало действие Лебедева по ч.2 ст.272 УК РФ, 38 т.е. изменение информации в контрольно-кассовых аппаратах, при которых записанная в них сумма выручки за смену искусственно занижалась. Информация, содержащаяся в контрольно-кассовых аппаратах, признана следствием разновидностью компьютерной информации. Адвокат Лебедева настаивал на изменении квалификации. Дайте юридическую оценку содеянного. Что следует понимать под компьютерной информацией?
	Группа ПИ1
1-8	Петров использовал доработанный сотовый телефон – «сканер», который позволял производить звонки за чужой счет. Всего в течение шести месяцев Петров таким образом «израсходовал» 15 тыс.рублей. Можно ли считать информацию, содержащуюся в сотовым телефоне, компьютерной информацией? Как соотносятся компьютерная информация и коммерческая тайна? Квалифицируйте содеянное Петровым.
9-15	Панченко и Будин, работали в компьютерной форме, распространяли «Троянские» программы и получали доступ к паролям пользователей компьютеров. Дайте анализ объективных и субъективных признаков данных составов преступлений. Решите вопрос о квалификации содеянного и укажите нормы права, согласно которым Панченко и Будим могут быть привлечены к ответственности
16-23	Харламова А.Е. работала в 2012 г. секретарем нотариуса в нотариальной конторе. Некто Толкачёв Л.Э. пришёл к нотариусу и оформил завещание на своего сына. В 2018 г. Харламова А.Е. опубликовала информацию о данном завещании на своём форуме, где дочь Толкачёва Л.Э. прочитала её. После семейного скандала Толкачёв Л.Э. обратился к Харламовой А.Е. с претензиями и просьбой удалить данные материалы с сайта, на что она ответила: «Во-первых, я не нотариус, чтобы хранить ваши тайны. А во-вторых, я могу публиковать любую информацию на своем сайте» Можно ли привлечь Харламову А.Е. к ответственности? Какие нормы права нарушила Харламова А.Е.?
24-30	Сотрудником подразделения объектового режима при выходе из лабораторного корпуса НИИ у сотрудника был обнаружен машинный носитель информации, что является нарушением регламента информационной безопасности, введённом на предприятии. Что должен предпринять сотрудник службы безопасности, чтобы удостовериться в обеспечении информационной безопасности вверенного ему подразделения?

Литература по теме

1. http://elib.cspu.ru/xmlui/bitstream/handle/123456789/15213/Гафарова%20Сборник%20задач%20кейсов%20итоговый.pdf?sequence=1&isAllowed=y

Тема 5 Экспертиза преступлений в области компьютерной информации. Аппаратно-компьютерная экспертиза

Цель и задачи практического занятия

Дать студентам знания об экспертизах преступлений в области компьютерной информации.

Изучить объекты компьютерно-технической экспертизы и аспекты исследования машинных носителей информации

К объектам исследования **компьютерной экспертизы** принадлежат:

1. Настольные и портативные персональные компьютеры;
2. Периферийные устройства (такие, как принтеры, модемы и прочие);
3. Сетевые аппаратные средства (рабочие станции, сетевые кабели, серверы и т.д.);
4. Интегрированные системы (мобильные телефоны, пейджеры, органайзеры и т.д.);
5. Комплектующие для всех вышеуказанных компонентов (микросхемы, платы расширения, аппаратные блоки);
6. Программное обеспечение, системное и прикладное;
7. Информация, принадлежащая форматам баз данных, различных приложений прикладного характера и т.д.

Ниже приведены основные задачи и цели, выполняемые компьютерной экспертизой:

1. **Компьютерная экспертиза** при непосредственном исследовании компьютерной системы устанавливает вид предоставления и свойства информации;
2. Устанавливает первичное состояние информации на носителях данных;
3. **Компьютерная экспертиза** определяет, при каких условиях изменялись свойства исследуемой информации, время (период) изменения, хронологическую последовательность влияния на информацию;
4. **Компьютерная экспертиза** находит следы возможных людей, участвовавших в событии, по признакам, характерным для определенных пользовательских и профессиональных навыков, привычек, умений; ставит условия, при которых информация была создана, скопирована, изменена, удалена;
5. Устанавливает причинную связь между совершенными манипуляциями с информацией компьютера и наступившими последствиями (к примеру, связь между нарушением работоспособности системы и удалением информации).

Наиболее часто **компьютерная экспертиза** проводится с использованием специализированного программного обеспечения — Encase Forensis Edition,

которое специально предназначено для исследования компьютерных носителей и ЭВМ.

Распоряжением Правительства N 1735-р от 20.09.2012 г. определены научные направления судебной компьютерно-технической экспертизы. Среди них: связь; электроника; автоматизация; информационные процессы; вычислительная техника; программирование; радиотехника; электротехника. С учетом знаний по эксплуатации, разработке компьютерных средств, которые отвечают за реализацию информационных процессов, устанавливаются обстоятельства преступлений.

Экспертиза, выполняемая по решению судебной инстанции (СКТЭ) – самостоятельно-проводимое исследование при расследовании компьютерных преступлений и относится к разряду инженерно-технических экспертиз. Данное исследование помогает получить доступ к цифровой информации, связанной с преступлением, совершенным через компьютерное средство. Полученные данные подвергаются всестороннему исследованию и помогают в раскрытии гражданского или уголовного дела. СКТЭ состоит из двух исследований: Компьютеров и их комплектующих. Изучаются конструктивные особенности цифровой машины, состояние ее периферийных устройств, компьютерных сетей, магнитных носителей. Устанавливаются реальные причины в нормальной работе техники. Программного обеспечения и данных. Определяется назначение, содержание, алгоритм функционирования программных продуктов.

Нормативные акты регулируют методику проведения, цели и задачи судебной компьютерно-технической экспертизы. К ним относятся: Письмо ФССП России N 00043/14/56151-ВВ от 18.09.2014 г. содержит методические рекомендации; Распоряжение Правительства РФ N 1735-р от 20.09.2012 г. определяет концепцию целевой программы; Приказ Минюста России N 237 от 27.12.2012 г. содержит перечень экспертиз, кто проводит; Постановление Правительства РФ N 1406 от 27.12.2012 г. сообщает о целевой программе развития отрасли.

Экспертиза подразделяется на виды с учетом обеспечивающих компонентов. Основными являются: программно-компьютерная; аппаратно-компьютерная; компьютерно-сетевая; информационно-компьютерная. Благодаря такому делению становится возможным провести наиболее тщательное исследование эксплуатационных, технологических свойств объектов.

Объект и задачи

Объекты и задачи разнятся от вида применяемой экспертизы. Главная цель – установить точную информацию по использованию компьютерной техники и всего, что с ней связано. Это может быть: съемный носитель; программное обеспечение; файлы; интернет. Устанавливается пользователь, хронология событий, операции с данными, причинная связь действий с последствиями, что немаловажно для вынесения правильного решения по возбужденному делу.

Вопросы эксперту

Чтобы правильно проводить расследование, оперуполномоченный и следователь должны ясно понимать значение СКТЭ (возможности, ограничения). Также им понадобится грамотно сформулировать задачи специалистов. В этом помогут соответствующие знания из области компьютерной технологии.

Поиск информации

Цель метода состоит в поиске на информационном носителе изображений, документации, сообщений, которые относятся к рассматриваемому делу. Принимаются во внимание разного рода сведения: зашифрованные, удаленные, скрытые. Просматривая большое количество информации, эксперт самостоятельно выбирает, что достойно внимания. Для этого важно его ознакомить с возбужденным делом.

Следы

Задачей исследования является определение действий, связанных с использованием информации: доступ, ввод, просмотр, обработка, хранение, удаленное управление. Экспертиза помогает понять, происходило ли создание веб-страниц с исследуемого компьютерного устройства. Любое действие оставляет определенные следы на средстве. СКТЭ устанавливает в отношении осуществления доступа: когда; при каких условиях; каким методом.

Программы

Программы для ЭВМ исследуются на наличие вирусов, предоставление способов незаконного доступа к защищенной информации, удаленных сведений. Специалистов интересует не только их происхождение, функциональность, но и взаимодействие с другими утилитами, процесс создания.

Время

В процессе экспертизы устанавливается последовательность и время событий. Что стало возможным благодаря наличию встроенных энергонезависимых часов. На каждый документ и действие устанавливается время. Даже при ручном переводе часов, что тоже оставляет след, восстанавливается последовательность событий. Если совершался выход в интернет, легче сопоставить действия на компьютере с событиями вне его. Это позволяет определить причину перевода времени.

Пользователи

При постоянном пользовании техники человек оставляет на ней свой след. Что ясно выражается в переписке, оформлении, документах, музыке, фотографиях, временном режиме работы, настройках, подборе программ, закладках браузера. Исследование подобных данных многое расскажет о наклонностях, интеллекте, способностях, эмоциях пользователя. Стоит помнить, что все сделанные выводы о характере человека будут не точными, а предварительными.

Неприемлемые вопросы

Несмотря на то, что СКТЭ отвечает на многие вопросы, касающиеся техники, но некоторые остаются без ответа. Они касаются: прав пользователя

на найденную информацию; стоимости лицензий, компьютеров, цифровых носителей, программ; правомерности производившихся действий с исследуемыми объектами; переводов текстов.

Образец постановления о назначении компьютерно-технической экспертизы Документ состоит из нескольких частей:

Вводная. Содержит полные реквизиты судебной инстанции и заявителя. Описательная. Цитирует совершенное правонарушение. Кто виновник, суть происшедшего, результат, описание действий пострадавшей стороны. Мотивационная. Требовательная. Выдвигаемые требования со стороны пострадавшего со ссылкой на законодательные акты.

Заключение

Заключением судебной компьютерно-технологической экспертизы станет акт, содержащий описание найденной информации, выявленных недостатков, исследованного оборудования. Эксперты изложат свое видение ситуации, покажут взаимосвязь с преступлением, при наличии. Стоимость компьютерно-технической экспертизы необходимо узнавать в выбранной организации по проведению исследования. Порядок проведения компьютерно-технической экспертизы регулируется нормативными актами РФ. Процедура помогает своевременно выявить нарушителей действующего законодательства.

Общие рекомендации по выполнению данного цикла практических занятий

В данном цикле практических занятий студенты могут исследовать области следообразования в файловой системе и осваивать формальные основы составления экспертного заключения.

Основная цель при проведении таких работ — использование методов и средств для сохранения (неизменности), сбора и анализа цифровых вещественных доказательств, для того чтобы восстановить события инцидента.

Термин "forensics" является сокращенной формой "forensic science", дословно "судебная наука", то есть наука об исследовании доказательств — именно то, что в русском именуется криминалистикой. Русский термин "форензика" означает не всякую криминалистику, а именно компьютерную. Некоторые авторы разделяют компьютерную криминалистику (computer forensics) и сетевую криминалистику (network forensic).

Основная сфера применения форензики — анализ и расследование событий, в которых фигурируют компьютерная информация как объект посягательств, компьютер как орудие совершения преступления, а также какие-либо цифровые доказательства.

Для полноценного сбора и анализа информации используются различные узкоспециализированные утилиты

Фреймворки

- dff — Digital Forensics Framework — платформа с открытым исходным кодом для проведения работ по извлечению и исследованию данных.

- PowerForensics — PowerForensics утилита, написанная на PowerShell, предназначенная для исследования жестких дисков.
- The Sleuth Kit — The Sleuth Kit (TSK) — это библиотека на языке C и коллекция инструментов командной строки, которые позволяют исследовать образы дисков.

Реал-тайм утилиты

- grr — GRR Rapid Response: инструмент для расследования и анализа инцидентов.
- mig — Mozilla InvestiGator — распределенная реал-тайм платформа для расследования и анализа инцидентов.

Работа с образами (создание, клонирование)

- dc3dd — улучшенная версия консольной утилиты dd.
- adulau/dcfldd — еще одна улучшенная версия dd.
- FTK Imager — FTK Imager- просмотр и клонирования носителей данных в среде Windows.
- Guymager — просмотр и клонирования носителей данных в среде Linux.

Извлечение данных

- bstrings — улучшенная версия популярной утилиты strings.
- bulk_extractor — выявления email, IP-адресов, телефонов из файлов.
- floss эта утилита использует расширенные методы статического анализа для автоматической деобфускации данных из двоичных файлов вредоносных программ.
- photorec — утилита для извления данных и файлов изображений.

Работа с RAM

- inVtero.net — фреймворк, отличающийся высокой скоростью работы.
- KeeFarce — извлечение паролей KeePass из памяти.
- Rekall — анализ дампов RAM, написанный на python.
- volatility — Volatility Framework представляет собой набор утилит для разностороннего анализа образов физической памяти.
- VolUtility — веб-интерфейс для Volatility framework.

Сетевой анализ

- SiLK Tools — инструменты для анализа трафика для облегчения анализа безопасности крупных сетей.
- Wireshark — известнейший сетевой сниффер.

Артефакты Windows (извлечение файлов, историй загрузок, USB устройств и т.д.)

- FastIR Collector — обширный сборщик информации о системе Windows (реестр, файловая система, сервисы, автозагрузка и т.д.)
- FRED — кросплатформенный анализатор реестра Windows.
- MFT-Parsers — лист сравнения MFT-парсеров (MFT — Master File Table).
- MFTExtractor — MFT-парсер.
- NTFS journal parser — парсер журналов NTFS.

- NTFS USN Journal parser — — парсер журналов USN.
- RecuperaBit — восстановление NTFS данных.
- python-ntfs — анализ NTFS данных.

Исследование OS X

- OSXAuditor — OS X аудитор.

Internet Artifacts

- chrome-url-dumper — извлечение информации из Google Chrome.
- hindsight — анализ истории Google Chrome/Chromium.

Анализ временных интервалов

- plaso — извлечение и агрегация таймстапов.
- timesketch — анализ таймстапов.

Hex редакторы

- 0xED — HEX редактор OS X.
- Hexinator — Windows версия Synalyze It.
- HxD — маленький и быстрый HEX редактор.
- iBored — кросс-платформенный HEX редактор.
- Synalyze It! — HEX редактор в тимплейтами.
- wxHex Editor — кросс-платформенный HEX редактор со сравнением файлов.

Конверторы

- CyberChef — мультиинструмент для кодирования, декодирования, сжатия и анализа данных.
- DateDecode — конвертирование бинарных данных.

Анализ файлов

- 010 Editor Templates — тимплейты для редактора 010.
- Contruct formats — парсер различных видов файлов на python.
- HFSPlus Grammars — HFS+ составляющие для Synalysis
- Sleuth Kit file system grammars — составляющие для различных файловых систем.
- Synalyse It! Grammars — файловые составляющие для Synalyze It!
- WinHex Templates — файловые составляющие для WinHex и X-Ways

Обработка образов дисков

- imagemounter — утилита командной строки для быстрого монтирования образов дисков
- libewf — Libewf библиотека и утилиты доступа и обработки форматов EWF, E01.
- xmount — конвертирования образов дисков.

Для проведения работ по исследованию и сбору цифровых доказательств необходимо придерживаться принципов неизменности, целостности, полноты информации и ее надежности. Для этого необходимо следовать рекомендациям к ПО и методам проведения расследований.

Могут использоваться бесплатные инструменты для проведения в сфере компьютерной безопасности

Дисковые инструменты и сбор данных

- Arsenal Image Mounter утилита для работы с образами дисков в Windows, доступ к разделам и томам и т. д.
- DumpIt утилита для создания дампа физической памяти компьютеров Windows, 32/64 бит. Может работать с USB-накопителя.
- EnCase Forensic Imager утилита для создания доказательных файлов EnCase.
- Encrypted Disk Detector утилита для выявления зашифрованных томов TrueCrypt, PGP или Bitlocker.
- EWF MetaEditor утилита для редактирования метаданных EWF (E01).
- FAT32 Format утилита для форматирования дисков большой емкости в FAT32.
- Forensics Acquisition of Websites браузер, предназначенный для захвата веб-страниц для проведения расследований.
- FTK Imager просмотр и клонирование носителей данных в среде Windows.
- Guymager многопоточная утилита с GUI для создания образов дисков под управлением Linux.
- Live RAM Capturer утилита для извлечения дампа RAM, в том числе защищенный анти-отладочной или антидампинговой системой.
- NetworkMiner инструмент сетевого анализадля обнаружения ОС, имени хоста и открытые портов сетевых узлов с помощью перехвата пакетов / анализа PCAP.
- Magnet RAM Capture утилита для захвата RAM от Windows XP до Windows 10, Win Server 2003, 2008, 2012.
- OSFClone утилита live CD/DVD/USB для создания dd или AFF образов.
- OSFMount утилита для монитирования образов дисков, также позволяет создавать RAM-диски.

Анализ электронной почты

- EDB Viewer утилита для просмотра файлов EDB Outlook без сервера Exchange.
- Mail Viewer утилита для просмотра файлов Outlook Express, Windows Mail/Windows Live Mail, базы данных сообщений Mozilla Thunderbird и отдельных файлов EML.
- MBOX Viewer утилита для просмотра электронных писем и вложений MBOX.
- OST Viewer утилита для просмотра файлов OST Outlook без сервера Exchange.
- PST Viewer утилита для просмотра файлов PST Outlook без сервера Exchange.

Анализ файлов и данных

- analyzeMFT утилита парсинга MFT из файловой системы NTFS, позволяя анализировать результаты с помощью других инструментов.
- bstrings утилита поиска в двоичных данных, включая поиск регулярных выражений.
- CapAnalysis утилита просморта PCAP.

- Crowd Response консольное приложение Windows для помощи в сборе системной информации для реагирования на инциденты и обеспечения безопасности.
- Crowd Inspect утилита для получения информации о сетевых процессах, перечислении двоичных файлов, связанных с каждым процессом. Создает запросы к VirusTotal и другим онлайн-средствам анализа вредоносных программ и служб репутации.
- DCode утилита преобразует различные типы данных в значения даты / времени.
- Defraser утилита для обнаружения полных и частичных данных о мультимедийных файлах в нераспределенном пространстве.
- eCryptfs Parser утилита рекурсивно анализирует заголовки каждого файла eCryptfs в выбранном каталоге.
- Encryption Analyzer утилита для анализа защищенных паролем и зашифрованных файлов, анализирует сложность шифрования отчетов и варианты дешифрования для каждого файла.
- ExifTool утилита для чтения и редактирования данных Exif в большом количестве типов файлов.
- File Identifier онлайн анализ типа файлов (более 2000).
- Forensic Image Viewer утилита для извлечения данных из изображений.
- Link Parser утилита для рекурсивного анализа папок, извлекающая более 30 атрибутов из файлов Windows .lnk (shortcut).
- Memoryze анализ образов RAM, включая анализ «page» файлов.
- MetaExtractor утилита для извеления мета-информации из офисных документов и pdf.
- Shadow Explorer утилита для просмотра и извлечения файлов из теневых копий.

Инструменты для Mac OS

- Audit утилита для вывода аудита и журналов OS X.
- Disk Arbitrator блокирует монтирование файловых систем, дополняя блокиратор записи при отключении арбитража диска.
- FTK Imager CLI for Mac OS консольная версия для Mac OS утилиты FTK Imager.
- IORegInfo утилита для отображении информации по подключенным к компьютеру устройствам (SATA, USB и FireWire, программные RAID-массивы). Может определять информацию раздела, включая размеры, типы и шину, к которой подключено устройство.
- mac_apt утилита для работы с образами E01, DD, DMG.
- Volafox утилита для анализа памяти в Mac OS X.

Мобильные устройства

- iPBA2 утилита анализа резервных копий iOS.
- iPhone Analyzer утилита анализа файловой структуры Pad, iPod и iPhone.

- ivMeta утилита для извлечения модели телефона и версии программного обеспечения, а также временные данные и данные GPS с видео iPhone.
- Rubus утилита для деконструирования резервных файлов Blackberry .ipd.
- SAFT извлечение SMS, журналов звонков и контактов из Android устройств.

Рекомендуется использовать примеры заключений по различным видам СКТЭ, которые можно найти здесь: http://computer-forensics-lab.org/lib/%D0%91%D0%B8%D0%B1%D0%BB%D0%B8%D0%BE%D1%82%D0%B5%D0%BA%D0%B0/%D0%AD%D0%BA%D1%81%D0%BF%D0%B5%D1%80%D1%82%D0%B8%D0%B7%D1%8B/

Судебная аппаратно-компьютерная экспертиза.

Сущность судебной аппаратно-компьютерной экспертизы заключается в проведении исследования технических (аппаратных) средств компьютерной системы. Предметом данного вида СКТЭ являются факты и обстоятельства, устанавливаемые на основе исследования закономерностей эксплуатации аппаратных средств компьютерной системы - материальных носителей информации о факте или событии гражданского либо уголовного дела.

Объектами судебной аппаратно-компьютерной экспертизы являются персональные компьютеры (настольные, портативные); периферийные устройства; сетевые аппаратные средства (серверы, рабочие станции, активное оборудование, сетевые кабели и т.д.); интегрированные системы (органайзеры); пейджеры; мобильные телефоны и т.п.; встроенные системы на основе микропроцессорных контроллеров (иммобилайзеры, транспондеры, круиз-контроллеры и проч.); любые комплектующие всех указанных компонент (аппаратные блоки, платы расширения, микросхемы и др.). В судебно-экспертном аспекте наиболее важны такие объекты, как запоминающие устройства и носители данных, включая все известные на момент проведения экспертизы электронные носители данных: микросхемы памяти, магнитные и лазерные диски, магнитооптические диски, магнитные ленты, флэш-карты и т.д.

При этом решаются задачи:

- классификации и определения свойств аппаратного средства; выяснения фактического и первоначального состояния;
- диагностики технологии изготовления, причин и условий изменения свойств (эксплуатационных режимов);
- определения структуры механизма и обстоятельства события за счет использования выявленных аппаратных средств как по отдельности, так и в комплексе в составе компьютерной системы;

Экспертиза разрешает вопросы, связанные с такими моментами: отношение устройства к разряду компьютерных средств; условия и хронологическая последовательность применения; наличие дефектов;

технические характеристики; отклонения от стандартных параметров; модель; установленные эксплуатационные режимы; роль в компьютерной системе.

При вынесении следователем постановления о назначении компьютерно-технической экспертизы в постановлении о ее назначении обязательно указываются серийный номер компьютера и его индивидуальные признаки (конфигурация, цвет, надписи на корпусе и т.д.).

Примерными вопросами, разрешаемыми судебной аппаратно-компьютерной экспертизой, являются следующие.

Относится ли представленное устройство к аппаратным компьютерным средствам?

К какому типу (марке, модели) относится аппаратное средство? Каковы его технические характеристики и параметры?

Каково функциональное предназначение аппаратного средства?

Какова роль и функциональные возможности данного аппаратного средства в конкретной компьютерной системе?

Относится ли данное аппаратное средство к представленной компьютерной системе?

Используется ли данное аппаратное средство для решения конкретной функциональной задачи?

Какое первоначальное состояние (конфигурацию, характеристики) имело аппаратное средство?

Каково фактическое состояние (исправен, неисправен) представленного аппаратного средства? Имеются ли в нем отклонения от типовых (нормальных) параметров, в том числе и физические дефекты?

Какие эксплуатационные режимы установлены на данном аппаратном средстве?

Является ли неисправность данного средства следствием нарушения определенных правил эксплуатации?

Каковы причины изменения функциональных (потребительских) свойств в начальной конфигурации представленного аппаратного средства?

Является ли представленное аппаратное средство носителем информации?

Каков вид (тип, модель, марка) представленного носителя информации?

Какое запоминающее устройство предназначено для работы с данным накопителем информации? Имеется ли в составе представленной компьютерной системы запоминающее устройство для работы с этим носителем информации?

Каковы параметры (форм-фактор, емкость, среднее время доступа к данным, скорость передачи данных и др.) носителя информации? Какой метод хранения данных реализован на представленном носителе?

Доступен ли для чтения представленный носитель информации?

Каковы причины отсутствия доступа к носителю информации?

Примером аппаратно-компьютерной экспертизы является изучение возможностей применения нетипичных или нештатных (например, в случае удара или внезапного отказа) способов исследования носителей данных (чаще всего жестких дисков) с целью извлечения криминалистически значимой информации, хранящейся на нем. Другой пример связан с установлением работоспособности системного блока компьютера.

Так, по одному из гражданских дел на экспертизу был представлен системный блок персонального компьютера. Вопросы эксперту были сформулированы следующим образом.

1. Находится ли системный блок в работоспособном состоянии, если нет, то какие имеются неисправности?

2. Является ли выявленная неисправность заводским браком либо следствием нарушения эксплуатации?

3. Имеется ли причинная связь между выходом из строя видеоконтроллера системного блока и установкой внутреннего модема?

4. Мог ли заряд статического электричества повредить комплектующие элементы системного блока при их самостоятельной установке либо замене?

В результате выявленного комплекса диагностических признаков в ходе экспертного исследования было доказано наличие в материнской плате системного блока компьютера заводского брака, приведшего к аппаратной неисправности всего компьютера.

Контрольные вопросы и задания

Контрольные вопросы

1. Что такое судебная компьютерно-техническая экспертиза?
- Перечислить объекты аппаратно-компьютерной экспертизы. Дать их описание.
- Какие вопросы, выносятся на разрешение аппаратно-компьютерной экспертизы?

Задания

1. Составить отчет о аппаратно-компьютерной экспертизе гипотетического компьютерного преступления.

Источники по теме

1 http://prosud24.ru/kompjuterno-tehnicheskaja-jekspertiza/

2 http://www.nhtcu.ru/jur

- http://computer-forensics-lab.org/
- https://habrahabr.ru/company/pentestit/blog/346910/%3A%2F%2Fzen.yandex.com

- https://habrahabr.ru/company/pentestit/blog/327740/
- https://habrahabr.ru/company/pentestit/blog/338378/

Тема 6 Экспертиза преступлений в области компьютерной информации. Программно-компьютерная экспертиза

Цель и задачи практического занятия

Дать студентам знания о судебной программно-компьютерной экспертизе преступлений в области компьютерной информации.

Изучить аспекты исследования программного обеспечения

ПО – совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата.

Вся информация, относящаяся к программному обеспечению, независимо от формы носителя, является объектом экспертизы и должна быть предоставлена эксперту.

Для осуществления экспертного исследования программного обеспечения предназначена судебная программно-компьютерная экспертиза. Ее предметом являются закономерности разработки (создания) и применения (использования) программного обеспечения компьютерной системы, представленной на исследование в целях установления истины по гражданскому или уголовному делу. Целью судебной программно-компьютерной экспертизы является изучение функционального предназначения, характеристик и реализуемых требований, алгоритма и структурных особенностей, текущего состояния представленного на исследование программного обеспечения компьютерной системы.

Объектами программно-компьютерной экспертизы являются:

а) системное программное обеспечение (операционные системы);

б) вспомогательные программы - утилиты;

в) средства разработки и отладки программ;

г) служебная системная информация;

д) прикладное программное обеспечение (приложения общего назначения: текстовые и графические редакторы, системы управления базами данных, электронные таблицы, редакторы презентаций и т.д.; приложения специального назначения для решения задач в определенной области науки, техники, экономики и т.д.).

На разрешение судебных экспертиз этого рода ставятся следующие вопросы.

Какова общая характеристика представленного программного обеспечения, из каких компонент (программных средств) оно состоит?

Какую классификацию имеют конкретные программные средства (системные или прикладные) представленного программного обеспечения? Обладают ли они признаками контрафактности?

Каково наименование, тип, версия, вид представления (явный, скрытый, удаленный) программного средства?

Каковы реквизиты разработчика и владельца данного программного средства?

Каков состав соответствующих файлов программного обеспечения, каковы их параметры (объемы, даты создания, атрибуты)?

Какое общее функциональное предназначение имеет программное средство?

Имеются ли на носителях информации программные средства для реализации определенной функциональной задачи?

Какие требования предъявляет данное программное средство к аппаратным средствам компьютерной системы?

Какова совместимость конкретного программного средства с программным и аппаратным обеспечением компьютерной системы?

Используется ли данное программное средство для решения определенной функциональной задачи?

Каково фактическое состояние программного средства, его работоспособность по реализации отдельных (конкретных) функций?

Каким образом организован ввод и вывод данных в представленном программном средстве?

Имеются ли в программном средстве отклонения от нормальных параметров типовых программных продуктов (например, свойства инфицирования, недокументированных функций)?

Имеет ли программное средство защитные возможности (программные, аппаратно-программные) от несанкционированного доступа и копирования?

Каким образом организованы защитные возможности программного средства?

Каков общий алгоритм данного программного средства?

Какие программные инструментальные средства (языки программирования, компиляторы, стандартные библиотеки) использовались при разработке данного программного средства?

Имеются ли на носителях информации тексты (коды) с первоначальным состоянием программы?

Подвергался ли алгоритм программного средства модификации по сравнению с исходным состоянием? В чем это нашло отражение?

Какой вид имело программное средство до его последней модификации?

Использованы ли в алгоритме программы и ее тексте какие-либо специфические (нестандартные) приемы алгоритмизации и программирования?

С какой целью было произведено изменение каких-либо функций в программном средстве?

Направлены ли внесенные изменения в программное средство на преодоление его защиты?

Достигается ли решение определенных задач после внесения изменений в программное средство?

Каким способом были произведены изменения в программе (преднамеренно, воздействием вредоносной программы, ошибками программной среды, аппаратным сбоем и др.)?

Какова хронология внесения изменений в программном средстве?

Какова хронология использования программного средства (начиная с ее инсталляции)?

Имеются ли в программном средстве враждебные функции, которые влекут уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютерной системы?

Каковы последствия дальнейшей эксплуатации определенного программного средства?

Показательным примером программно-компьютерной экспертизы является экспертное исследование программного обеспечения, позволившее успешно расследовать хищение денежных средств путем использования несовершенства компьютерной программы. Л., являясь клиентом одного из коммерческих банков, обратил внимание на частичную несовместимость программы автоматизации банковских операций "ПАБА" и программы обслуживания пластиковых карточек "Арканзас". Первая программа предусматривала для любой валюты два дополнительных знака, рассчитанных на центы, копейки и т.д. Вторая же программа при операциях с валютами, не имеющими деления на более мелкие единицы (такие, как итальянская лира, японская иена и проч.), считывала последний знак как единицу основной валюты. В результате при снятии через банкомат средств со счета в иностранной валюте, не имеющей деления на мелкие единицы, остаток на счету оставался большим в сто раз, чем было в действительности. Это позволяло снимать со счета суммы в указанной валюте, стократно превышающие вклад. Произведенное в процессе экспертного исследования изучение используемого программного обеспечения позволило выявить имеющуюся нестыковку и установить фактические обстоятельства выполнения ошибочных операций.

Контрольные вопросы и задания

Контрольные вопросы

1Что такое программно-компьютерная экспертиза?

- 2 Перечень вопросов, разрешаемых при исследовании ПО.

Задания

1. Составить отчет о программно-компьютерной экспертизе гипотетического компьютерного преступления.

Литература

1: http://prosud24.ru/kompjuterno-tehnicheskaja-jekspertiza/

Тема 7 Экспертиза преступлений в области компьютерной информации. Информационно-компьютерная экспертиза

Цель и задачи практического занятия

Дать студентам знания об информационно-компьютерной экспертизе преступлений в области компьютерной информации.

Судебная информационно-компьютерная экспертиза, имеет целью поиск, обнаружение, анализ и оценку информации, подготовленной пользователем или порожденной программами для организации информационных процессов в компьютерной системе.

Информационные объекты (данные) включают:

- текстовые и графические документы (в бумажной и электронной формах), изготовленные с использованием компьютерных средств;
- данные в форматах мультимедиа;
- базы данных и другие приложения, имеющие прикладной характер.

Экспертными задачами здесь являются: установление вида, свойств и состояния информации (фактического и первоначального, в том числе до ее удаления и модификации) в компьютерной системе;

- определение причин и условий изменения свойств исследуемой информации;
- определение механизма, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям;
- установление участников события, их роли, места, условий, при которых была создана (модифицирована, удалена) информация;
- установление соответствия либо несоответствия действий с информацией специальному регламенту (правилам), например, правомерно ли конкретное использование информации, защищенной паролем, и др.;

Судебная информационно-компьютерная экспертиза (данных) является ключевым видом СКТЭ, так как позволяет завершить целостное построение

доказательственной базы путем окончательного разрешения большинства вопросов, связанных с компьютерной информацией. Целью этого вида является поиск, обнаружение, анализ и оценка информации, подготовленной пользователем или порожденной (созданной) программами для организации информационных процессов в компьютерной системе.

Судебная информационно-компьютерная экспертиза (данных) производится для разрешения следующих вопросов.

Как отформатирован носитель информации и в каком виде на него записаны данные?

Каковы характеристики физического размещения данных на носителе информации?

Каковы характеристики логического размещения данных на носителе информации?

Какие свойства, характеристики и параметры (объемы, даты создания-изменения, атрибуты и др.) имеют данные на носителе информации?

Какого вида (явный, скрытый, удаленный, архив) информация имеется на носителе?

К какому типу относятся выявленные (определенные) данные (текстовые, графические, база данных, электронная таблица, мультимедиа, запись пластиковой карты, данные ПЗУ и др.) и какими программными средствами они обеспечиваются?

Каким образом организован доступ (свободный, ограниченный и проч.) к данным на носителе информации и каковы его характеристики?

Какие свойства, характеристики имеют выявленные средства защиты данных и какие пути ее преодоления возможны?

Какие признаки преодоления защиты (либо попыток несанкционированного доступа) имеются на носителе информации?

Каково содержание защищенных данных?

Каково фактическое состояние выявленных данных и соответствует ли оно типовому состоянию на соответствующих носителях данных?

Какие несоответствия типовому представлению имеются в выявленных данных (нарушение целостности, несоответствие формата, вредоносные включения и проч.)?

Каковы пользовательские (потребительские) свойства и предназначение данных на носителе информации?

Какие данные для решения определенной функциональной (потребительской) задачи имеются на носителе информации?

Какие данные с фактами и обстоятельствами конкретного дела находятся на представленном носителе информации?

Какие данные о собственнике (пользователе) компьютерной системы (в том числе имена, пароли, права доступа и проч.) имеются на носителях информации?

Какие данные с представленных на экспертизу документов (образцов) и в каком виде (целостном, фрагментарном) находятся на носителе информации?

Каково первоначальное состояние данных на носителе (в каком виде, какого содержания и с какими характеристиками, атрибутами находились определенные данные до их удаления или модификации)?
Каким способом и при каких обстоятельствах произведены действия или операции (блокирование, модификация, копирование, удаление) определенных данных на носителе информации?
Какой механизм (последовательность действий) по решению конкретной задачи отражен в определенных данных на носителе информации?
Какая хронологическая последовательность действий (операций) с выявленными данными имела место при решении конкретной задачи (например, подготовки изображений денежных знаков, ценных бумаг, оттисков печатей т.п.)?
Какая причинная связь имеется между действиями (вводом, модификацией, удалением и проч.) с данными и имевшим место событием (например, нарушением в работе компьютерной системы, в том числе сбои в программном и аппаратном обеспечении)?
Какова степень соответствия (или несоответствия) действий с конкретной информацией специальному регламенту или правилам эксплуатации определенной компьютерной системы?

Вся информация, относящаяся к базам данных, независимо от формы носителя, является объектом экспертизы и должна быть предоставлена эксперту.

Перечень вопросов, разрешаемых при исследовании баз данных.

1. Каким образом организована база данных?
2. В каком формате записана информация и какие СУБД могут ее обрабатывать?
3. Какая информация записана в данной базе?
4. Информация в базе записана обычным образом или закодирована?
5. Когда последний раз обновлялась информация?
6. Имеются ли в данной базе скрытые (помеченные для удаления) поля и их содержание?
7. Имеются ли повреждения или изменения в записях базы по сравнению с эталоном или резервной копией, если да, то какие?
8. Сколько записей в базе?
9. Имеется ли в данной базе запись конкретного содержания?
10. Можно ли внести изменение в данную базу с помощью простейших программных средств (например, текстовых редакторов и пр.)?

Примером судебной информационно-компьютерной является экспертиза по выявлению фактов и обстоятельств образования недостачи в одной крупной торговой компьютерной фирме. На разрешение экспертизы был поставлен вопрос: "Какая информация по реализации товарно-материальных ценностей за период с марта по август 200... г. имеется на представленных компьютерах?"

В ходе предварительно проведенного допроса сетевого администратора данной фирмы было установлено, что информация по реализации товарно-материальных ценностей представлена следующими реквизитами: номер товарного чека, наименование товара, цена в долларах и рублях, количество, сумма по чеку, менеджер, дата - и хранится в сводных таблицах помесячно. При производстве экспертизы эксперт СКТЭ исследовал все файлы, имеющиеся на жестких дисках представленных компьютеров, на предмет наличия в них вышеперечисленной информации за указанный период. Все найденные файлы оказались электронными таблицами, подготовленными средствами Microsoft Excel, что соответствовало показаниям сетевого администратора. Для дальнейшего анализа реализации товарно-материальных ценностей полученная информация была распечатана и передана эксперту судебно-бухгалтерской экспертизы, участвующему в данной комплексной экспертизе.

Контрольные вопросы и задания

Контрольные вопросы

1 Перечень вопросов, разрешаемых при исследовании баз данных.

1 Что помогает установить информационно-компьютерная экспертиза?

Задания

1. 1Составить отчет об проведении информационно-компьютерной экспертизы гипотетического компьютерного преступления.

Литература

1: http://prosud24.ru/kompjuterno-tehnicheskaja-jekspertiza/

.

Тема 8 Экспертиза преступлений в области компьютерной информации. компьютерно-сетевая экспертиза

Цель и задачи практического занятия

Дать студентам знания о компьютерно-сетевой экспертизе преступлений в области компьютерной информации.

Судебная компьютерно-сетевая экспертиза, основывается прежде всего на функциональном предназначении компьютерных средств, реализующих какую-либо сетевую информационную технологию. Задачи этой экспертизы

включают практически все основные задачи рассмотренных выше видов экспертизы. Это объясняется тем, что ее объекты интегрированы из объектов рассмотренных выше видов экспертиз (аппаратные, программные и данные), но лишь с той разницей, что они все функционируют в определенной сетевой технологии.

Компьютерно-сетевая экспертиза предназначена исследовать функциональное предназначение, возможности компьютерных устройств, участвующих в реализации сетевой информационной технологии. Проведение анализа требует особых знаний из области сетевых средств. Большей частью решаются задачи с использованием интернет-технологий. Предмет исследований в каждом отдельном случае сильно отличается. Основными являются: компьютеры с выходом в интернет; сетевые услуги провайдера; электронная почта; телеконференции; www-сервис; служба электронных объявлений.

Экспертиза помогает в решении поставленных задач: место и роль изучаемого оборудования, программного обеспечения во всемирной сети; отправленные/полученные сообщения; свойства; несанкционированный доступ к чужим компьютерам; изначальное состояние; программные закладки; отображение информации с носителей; исправность; работа в сети; внесенные изменения в первоначальную конфигурацию; использование средств; принадлежность к клиентской части приложения; результат применения.

Судебная компьютерно-сетевая экспертиза, в отличие от предыдущих, основывается прежде всего на функциональном предназначении компьютерных средств, реализующих какую-либо сетевую информационную технологию. Она выделена в отдельный вид в связи с тем, что лишь использование специальных знаний в области сетевых технологий позволяет соединить воедино полученные объекты, сведения о них и эффективно решить поставленные экспертные задачи. Особое место в компьютерно-сетевой экспертизе занимают экспертные исследования, связанные с интернет-технологиями .

Судебная экспертиза этого рода производится для решения следующих задач:

а) определение свойств и характеристик аппаратного средства и программного обеспечения, установление места, роли и функционального предназначения исследуемого объекта в Сети (например, для программного средства в отношении к сетевой операционной системе; для аппаратного средства - отношение к серверу, рабочей станции, активного сетевого оборудования и т.д.);

б) выявление свойств и характеристик вычислительной сети, установление ее архитектуры, конфигурации, выявление установленных сетевых компонент, организации доступа к данным;

в) определение соответствия выявленных характеристик типовым для конкретного класса средств сетевой технологии, определение принадлежности средства к серверной или клиентской части приложений;

г) определение фактического состояния и исправности сетевого средства, наличия физических дефектов, состояния системного журнала, компонент управлением доступа;

д) установление первоначального состояния вычислительной сети в целом и каждого сетевого средства в отдельности, возможного места покупки (приобретения), уточнение изменений, внесенных в первоначальную конфигурацию (например, добавление дополнительных сетевых устройств, устройств расширения на сервере либо рабочих станциях и проч.);

е) определение причин изменения свойств вычислительной сети (например, по организации уровней управления доступом), установление факта нарушения режимов эксплуатации сети; фактов (следов) использования внешних ("чужих") программ и т.п.;

ж) определение свойств и состояния вычислительной сети по ее отображению в информации носителей данных (например, RAID-массивы; жесткие диски, флоппи-диски, CD-ROM, ZIP-накопители и т.п.);

з) определение структуры механизма и обстоятельства события в Сети по его результатам (например, сценария несанкционированного доступа, механизма распространения в сети вредоносных функций и т.д.);

и) установление причинной связи между использованием конкретных аппаратно-программных средств вычислительной сети и результатами их применения.

Как видно, задачи судебной компьютерно-сетевой экспертизы охватывают практически все основные задачи основных родов СКТЭ, т.е. решение аппаратных, программных и информационных аспектов при установлении фактов и обстоятельств дела.

Наиболее часто встречаемыми в практике вопросами являются следующие.

Имеются ли признаки работы данного компьютерного средства в сети Интернет?

Какие аппаратные средства использовались для подключения к Интернету?

Имеются ли заготовленные соединения с узлом сети Интернет и каковы их свойства (номера телефонов провайдера, имена и пароли пользователя, даты создания)?

Каково содержание установок программы удаленного доступа к сети Интернет и протоколов соединений?

Какие имеются адреса Интернета, по которым осуществлялся доступ с данного компьютерного средства?

Имеется ли какая-либо информация о проведении электронных платежей и использовании кодов кредитных карт?

Имеются ли почтовые сообщения, полученные (а также отправленные) по электронной почте?

Имеются ли сообщения, полученные (отправленные) посредством использования программ персональной связи через Интернет, и каково их содержание?

Экспертиза технологий и систем электронных расчетов разрешает вопросы диагностического характера, перечень которых находится в настоящее время на стадии формирования. Представляется, что такие вопросы возможно решать по результатам предварительно проведенной компьютерно-технической экспертизы, которая технически интерпретирует содержимое файлов данных, относящихся к работе программных средств, функционирующих на компьютере пользователя.

Считается целесообразным решение следующих вопросов:

1. Клиентом какой (каких) электронной платежной системы (систем) и в какой период являлся пользователь?

2. Какие виды электронных кошельков поддерживаются электронной платежной системой (системами), какие из них использовались для проведения расчетов и операций?

3. Каковы особенности проведения операций с использованием выявленных в ходе производства экспертизы электронных кошельков?

4. Каков статус пользователя электронной платежной системы?

5. Каким способом и когда осуществлялся ввод и вывод денежных средств в электронную платежную систему на счет электронного кошелька?

6. Совершению каких операций с кошельками электронной платежной системы соответствуют записи, обнаруженные в ходе производства компьютерно-технической экспертизы и представленные на исследование?

7. Каким способом и когда осуществлялся обмен титульных знаков клиентом электронной платежной системы? Каковы эквиваленты валюты титульных знаков при проведении обмена и курс обмена?

8. Какой курс обмена был установлен владельцем обменного пункта на момент ввода и/или вывода наличных денег в/из электронной платежной системы?

Весьма показательным является пример проведения судебной компьютерно-сетевой экспертизы так называемых программных закладок, предоставляющих возможность несанкционированного доступа по Сети к данным чужих компьютеров. Суть экспертного исследования программных закладок заключается в установлении признаков "несанкционированных" действий (т.е. возможности выполнения своих действий с информацией на ЭВМ без уведомления и согласия ее законного пользователя), а также выявлении адресов, по которым производится "несанкционированная" пересылка тех или иных данных с ЭВМ.

Наиболее достоверным методом проведения подобной экспертизы является метод эксперимента в среде вычислительной сети. В случае решения задач экспертизы программных закладок относительно сети Интернет (при постановке вопросов относительно механизма действий программ-"троянцев") требуется создание некой модели сети Интернет (точнее ее сегмента). Эта модель обычно состоит из четырех компьютеров,

имитирующих основных участников сетевого взаимодействия в Интернете. Первый компьютер имитирует компьютер какого-либо физического лица или организации, подключенный к сети Интернет через определенного провайдера. Вторым имитируемым компьютером является сервер интернет-провайдера. Именно с его помощью определяются интернет-адреса других компьютеров в Сети, к которым обращается программная закладка. Третий компьютер имитирует работу сервера доменной системы имен (DNS). Четвертым компьютером имитируется компьютер-получатель, по адресу которого программная закладка передает те или иные данные.

Таким образом, только использование в ходе производства экспертизы указанного аппаратно-программного комплекса позволяет провести достоверное исследование программных закладок, которые отправляют по электронной почте (e-mail) регистрационные данные пользователей для доступа к сети Интернет, и получить соответствующие категорические выводы.

В связи со стремительным развитием современных телекоммуникаций и связи в судебной компьютерно-сетевой экспертизе можно выделить судебную телематическую экспертизу, предметом которой являются фактические данные, устанавливаемые на основе применения специальных знаний при исследовании средств телекоммуникаций и подвижной связи как материальных носителей информации о факте или событии, имеющем отношение к гражданскому или уголовному делу.

Практика показывает, что рассмотренные выше основные виды СКТЭ при производстве большинства экспертных исследований применяются комплексно и чаще всего последовательно. Поэтому в настоящее время в постановлении на производство судебной экспертизы целесообразно указывать не родовое наименование экспертизы, а назначать судебную компьютерно-техническую экспертизу.

Можно сформулировать вопросы комплексного исследования при судебной экспертизе целостной компьютерной системы (устройства).

Является ли представленное оборудование компьютерной системой?

Является ли представленное оборудование целостной компьютерной системой или же ее частью?

К какому типу (марке, модели) относится компьютерная система?

Каковы общие характеристики сборки компьютерной системы и изготовления ее компонент?

Какой состав (конфигурацию) и технические характеристики имеет компьютерная система?

Является ли конфигурация компьютерной системы типовой или расширенной под решение конкретных задач?

Какое функциональное предназначение имеет компьютерная система?

Имеются ли в компьютерной системе наиболее выраженные функции (потребительские свойства)?

Решаются ли с помощью представленной компьютерной системы определенные функциональные (потребительские) задачи?

Находится ли компьютерная система в рабочем состоянии?

Имеет ли компьютерная система какие-либо отклонения от типовых (нормальных) параметров, в том числе физические (механические) дефекты?

Какой перечень эксплуатационных режимов имеется в компьютерной системе?

Какие эксплуатационные режимы задействованы (установлены) в компьютерной системе?

Существуют ли в компьютерной системе недокументированные (сервисные) возможности, если да, то какие?

Какие носители информации имеются в данной компьютерной системе?

Реализована ли в компьютерной системе какая-либо система защиты информации?

Какая система защиты информации имеется в данной компьютерной системе? Каков тип, вид и характеристики этой системы защиты? Каковы возможности по ее преодолению?

Кроме того, в ходе ряда пограничных исследований иногда возникает потребность привлекать специальные знания и из других научных областей. Так, например, обстоит дело с решением задач снятия парольной защиты, получения доступа к закодированным данным, обнаруженным в ходе проведения экспертного исследования, расшифровки информации с поврежденной структурой данных, всестороннего анализа различных криптографических алгоритмов, программ и аппаратных средств. Это направление экспертной деятельности тесно связано с самостоятельной областью исследований - криптографией и защитой информации.

Ведущее место среди судебных экспертиз, назначаемых в комплексе с судебной компьютерно-технической экспертизой, занимает судебно-техническая экспертиза документов (СТЭД). Именно с необходимостью исследования поддельных документов, ценных бумаг и денежных знаков, оттисков печатей, кредитных и расчетных карт, изготовленных с применением современных информационных технологий, связано большинство комплексных экспертиз в рассматриваемой сфере. Объектами такой комплексной экспертизы являются как некоторые объекты СКТЭ, предназначенные для создания, хранения и передачи информации, так и некоторые объекты СТЭД - документы в бумажной форме. В качестве объектов может также выступать полиграфическое оборудование и оргтехника, интегрированные с компьютерными средствами.

В последние годы широкое распространение получают мультимедийные технологии, которые основаны на представлении данных в формате видеоизображения с применением анимации и звукового сопровождения. Звуковые и видеофайлы в форматах мультимедиа на носителях данных, в том числе на компакт-дисках с аудио- и видеопродукцией, могут фигурировать в деле в качестве объектов, несущих доказательственную информацию о фактах, событиях, людях. Для непосредственного исследования цифровых видеозаписей и звуковых записей должна быть назначена судебная видеофоноскопическая экспертиза. Только в ходе указанного исследования

могут быть полностью разрешены вопросы относительно достоверности мультимедийной записи, а также установлено, выполнена ли она на конкретном устройстве. Пограничными здесь оказываются и вопросы, связанные с возможностью монтажа записи, непрерывности ее выполнения и т.п. В случае разрешения вопросов, касающихся исследования звуковой речевой информации, т.е. файлов со звуковыми форматами, требуется назначение комплексной СКТЭ и судебной фоноскопической экспертизы. Эти вопросы часто возникают в связи с широким распространением контрафактной продукции на компакт-дисках.

Следующая пограничная область специальных знаний явно просматривается в экономической и кредитно-финансовой сфере. При производстве судебно-экономических экспертиз информация о действительном состоянии исследуемых объектов зачастую имеется лишь в компьютере, а документированные сведения на бумажных носителях представлены в значительно измененном виде и могут не отражать действительного положения вещей. Использование "двойной" бухгалтерии становится типичным способом сокрытия таких преступлений, как присвоение или растрата, уклонение от уплаты налогов, мошенничество и другие, служит средством противодействия расследованию. В общем случае следы хозяйственных операций, сопоставление фактически совершенных операций с данными, отраженными в бухгалтерском учете и отчетности, устанавливаются судебно-бухгалтерской экспертизой, которая часто производится по гражданским делам при разрешении споров между юридическими и физическими лицами.

Для автоматизации бухгалтерского учета используется разнообразное программное обеспечение. Весьма ценная доказательственная и ориентирующая информация может быть получена при исследовании компьютерных средств, обеспечивающих бухгалтерские проводки, а также данных, содержащихся в компьютерных системах хозяйственных субъектов разных форм собственности. В таких случаях целесообразно назначение комплексной СКТЭ и судебно-бухгалтерской экспертизы.

Для решения задач, касающихся финансовой деятельности предприятий, соблюдения законодательных актов, регулирующих их финансовые отношения с государственным бюджетом, выполнения договорных обязательств, распределения и выплаты дивидендов, операций с ценными бумагами, инвестициями, и назначаются судебные финансово-экономические экспертизы, которые также должны, как правило, выполняться комплексно с судебными компьютерно-техническими экспертизами.

Другой род класса экономических экспертиз - судебно-товароведческая экспертиза также стыкуется в определенных случаях с СКТЭ. Если при рассмотрении гражданского или уголовного дела речь заходит о технологии производства (изготовления) компьютерной техники, то налицо необходимость назначения комплексной товароведческой и компьютерно-технической экспертизы. В сути этого исследования лежит интеграция специальных знаний в технологии производства товара и компьютерных

технологий. Эксперты изучают в этом случае не только сами товары - компьютерные средства, но и их потребительские свойства, факторы, оказывающие влияние на потребительскую стоимость, основные и вспомогательные материалы, из которых изготовлено компьютерное средство, изучается тара и упаковка.

Контрольные вопросы и задания

Контрольные вопросы

Что помогает установить компьютерно-сетевая экспертиза?

Задания

2. 1Составить отчет о проведении компьютерно-сетевой экспертизы гипотетического компьютерного преступления.

Литература

1: http://prosud24.ru/kompjuterno-tehnicheskaja-jekspertiza/

2. : http://cyberleninka.ru/article/n/o-naznachenii-ekspertiz-pri-rassledovanii-prestupleniy-sovershennyh-s-ispolzovaniem-elektronnyh-platezhnyh-sredstvi-sistem#ixzz4XiBYSQMk

Литература

1.Правовое обеспечение информационной безопасности: Учеб. пособие для студ. высш. учеб. заведений / С.Я. Казанцев, О.Э. Згадзай, Р.М. Оболенский и др.: Под ред. С.Я. Казанцева.- М. : Издательский центр «Академия», 2005. – 240 с.

2.Уголовный Кодекс Российской Федерации

3.Конявский В.А., Лопаткин С.В. Компьютерные преступления. В 2-х томах. Том 1 – М.: РФК-Имидж Лаб., 2006.

4. ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации.-М. 2013: http://genproc.gov.ru/documents/nauka/document-104550/

5. http://prosud24.ru/kompjuterno-tehnicheskaja-jekspertiza/

6. Гафарова, Е.А. Сборник кейс-задач по информационной безопасности. [Текст]: Учебное пособие / Е.А. Гафарова – 122 с. http://elib.cspu.ru/xmlui/bitstream/handle/123456789/15213/Гафарова%20Сборник%20задач%20кейсов%20итоговый.pdf?sequence=1&isAllowed=y

Приложение 1 Описания совершенных деяний в сфере компьютерной информации

№ студента в списке группы	Описания деяния
ПТ1 1-3	Оператором автоматизированной системы управления реактором атомной электростанции в рабочее время неумышленно введен в систему компьютерный вирус, что привело к чрезвычайной ситуации федерального масштаба.
4-6	Гражданка И., желая проверить верность ей гражданина П., посетив сайт электронного почтового сервиса, используя ранее полученный неправомерным путем логин и пароль гражданина П., осуществляет визуальный просмотр содержимого его почтового ящика и его копирование.
7-9	Главный врач санатория присвоила информационно-обрабатывающий центр установки лазерной терапии стоимостью 59 тыс. рублей. Она, используя компьютер в личных целях, загрузила его новыми программами, при этом медицинские программы из-за нехватки оперативной памяти были уничтожены. В результате этих действий была уничтожена охраняемая законом информация и причинен существенный вред санаторию, выразившийся в утрате информации, требующейся для лечения, и дезорганизована работа установки лазерной терапии.
10-13	Гражданин Ч. работая главным специалистом службы сбыта и маркетинга ОАО, создал заведомо ложную запись в компьютерном реестре клиентов фирмы о несуществующем договоре с ООО на поставку ликеро-водочной продукции с отсрочкой платежа. Гражданин З. привлек для исполнения роли экспедитора своего знакомого, гражданина И., не раскрывая последнему преступных намерений, а для сбыта похищенного - гражданина Н., у которого получил круглую печать 000 для оформления доверенности. Используя имеющийся у гражданина Ч. бланк доверенности и печать 000, граждане Ч. и З. составили доверенность на получение 200 ящиков ликеро-водочной продукции. Для вывоза похищенного гражданин З. заказал автомашину, передал гражданину И. доверенность 000 на получение 200 ящиков водки, подробно проинструктировал его о действиях при оформлении товарно-транспортных документов и получении продукции в фирме, сообщил номер и место стоянки автомобиля, на котором предполагалось вывезти груз. Гражданин И. прибыл в ОАО и, предъявив доверенность, получил в отпускном цехе 4000 бутылок водки, после чего вывел машину с продукцией и оставил её в условленном месте. Таким образом, действиями граждан Ч. и З. ОАО был причинен имущественный ущерб на общую сумму 800000 рублей.
14-16	Работник коммерческой организации «Окна» Воронин, не имеющий достаточного опыта работы на компьютере, случайно удалил из памяти главного компьютера организации информацию о ее новых разработках, из–за чего эта организация понесла значительные убытки. По заявлению директора в отношении Воронина было возбуждено уголовное дело по признакам ч. 2 ст. 274 УК. Однако Воронин заявил следователю, что никаких правил работы на компьютере руководство организации не утверждало, и потому он не должен подлежать уголовной ответственности
17-19	Компьютерный энтузиаст Доменов, придерживаясь определенных политических взглядов, в разгар предвыборной кампании проник в один из «серверов имен» глобальной сети интернет и подменил сетевой адрес вебсайта партии «Яблоко» на адрес вебсайта КПРФ, из–за чего все пользователи сети, запрашивающие новости партии «Яблоко», попадали на агитационную страницу КПРФ.
20-22	Студент технического университета Рывин перехватил данные, которые банкомат отправляет в банк, дабы удостовериться в наличии запрашиваемой суммы денег на счету. Для этого он подключил к соответствующему кабелю специально купленное в интернете техническое устройство и считал необходимые данные. После этого изготовив дубликат карты, снял деньги со счетов 8 клиентов на сумму 10 млн рублей
23-24	Для того чтобы узнать пин-код, студент технического университета Куренков оставил неподалеку от клавиатуры банкомата миниатюрную видеокамеру. Сам же в это время находился в ближайшем автомобиле с ноутбуком, на экране которого были видны вводимые владельцем карты цифры. После этого изготовив дубликат карты, снял деньги со счета клиент на сумму 50 тыс. рублей
25-27	В Пензенской области сотрудники полиции и ФСБ России задержали еще одну “хакерскую” группировку «BlowMind», промышлявшую воровством YouTube-каналов. В

	совершении преступления подозреваются шесть жителей Пензы в возрасте от 17 до 20 лет, которые были задержаны 16.07.2020. Группировка была создана в январе 2020 г. Злоумышленники договорились о написании “стиллера”, который будет воровать cookies и логины/пароли из браузеров.В состав группировки вошли: организатор и координатор группы (blackhatqq, bet1sh, estilmate), Python-разработчик (munqush), поддержка (ParatrooperA), “логер” (SwedenOptimaTeen) и др. Затем были наняты (за процент от последующей продажи украденных каналов) более 200 т.н. “воркеров”, в чьи задачи входил поиск владельцев YouTube-каналов и навязывание им (через методы социальной инженерии) запуска “стиллера”. Для них даже было написано специальное руководство.“Воркеров” искали через многочисленные теневые форумы. Что интересно, позже на этих форумах стали появляться жалобы на «BlowMind» (жаловались на обман, маленькие выплаты и т.п.). Некоторые аккаунты членов группировки даже были заблокированы за мошенничество. Жертвам (владельцам YouTube-каналов) “стиллер” засылался под видом легитимного ПО. Под это ПО создавались фейковые сайты и владельцам каналов предлагалось за деньги сделать его обзор (для этого и надо было запустить вредоносный EXE-файл). Размер исполняемого файла “стиллера” специально был раздут до 550 Мб, чтобы его невозможно было загрузить на проверку в virustotal.com. В ранних версиях “стиллер” фактически поддерживал только браузер Chrome начиная с версии 80 (из Edge/Yandex Browser/Firefox данные не воровались), но позднее была добавлена поддержка всех популярных браузеров и даже не самых популярных (например, Vivaldi). В результате действий злоумышленников были взломаны и похищены несколько сотен популярных YouTube-каналов. Похищенные таким образом каналы затем перепродавались
28-30	В Пензенской области силами отдела «К» регионального управления МВД и УФСБ России по Пензенской области при участии Управления «К» БСТМ МВД России и ФСБ России пресечена деятельность "хакерской" группировки, известной на теневых форумах под именем «Gods Of Logs»: 21-летний уроженец одной из стран ближнего зарубежья, 27-летний житель города Заречного Пензенской области и 32-летний житель Москвы. В начале 2019 г. все трое договорились о создании вредоносной программы (HVNC-бот плюс т.н. “стиллер”), предназначенной для похищения логинов/паролей и данных банковских карт с зараженных компьютеров, и последующем её распространении для использования сторонними лицами. Уроженец ближнего зарубежья занимался написанием кода, а задачей двух других было тестирование и продажа вредоносной программы, а также поиск и поддержка клиентов. После того, как программа была готова к использованию, она стала распространяться на теневых форумах (wwh, xss, skynetzone и др.) по модели подписки (Malware-as-a-Service). В Telegram был создан канал программы (@GodsOfLogs) и бот для ее поддержки (@hvnc_bot). По данным следствия, в период с марта по октябрь 2019 г. доступ к программе оплатили не менее четырёх неустановленных лиц. Кроме того, злоумышленники и сами использовали свою программу, “заливая” на HVNC-бота американский и европейский трафик, а затем, используя данные банковских карт жертв, “вбивали” на booking.com отели Турции и Грузии, зарабатывая на кешбэке и выводя деньги в биткоины. Тут хочется отметить, что свою деятельность некоторые члены группировки начинали в 2016 г. именно с кардинга и позже даже продавали скиммеры. В декабре 2019 г. злоумышленники встретились в Пензе, где планировали совместно продолжить работу над вредоносной программой, но были арестованы и помещены под стражу. В ходе обысков были изъяты компьютеры, мобильные телефоны и другие носители информации, содержащие доказательства незаконной деятельности.
ПТ2 1-3	Студенты технического университета Конев, Колечкин, Победин установили в людном месте свой собственный «банкомат». Он не выдавал денег, но успешно считывал с карточек граждан все необходимые данные. После этого он, изготовив дубликат карты, сняли деньги со счетов клиентов на сумму 800 тыс. рублей
4-6	Студенты технического университета Барбинюк и Жирюк установили в отверстия для кредиток специальное устройство, которое запоминало все данные о вставленной в банкомат карте. Потом они подсматривали пин-код подглядывая из-за плеча клиента и, изготовив дубликат карты, сняли деньги со счетов клиентов на сумму 20 тыс. рублей.
7-9	На въезде в тоннель на Садовом кольце Москвы установлен монитор, принадлежащий рекламной компании. Однажды демонстрация рекламы неожиданно была прервана показом порнографии. Показ порнографии на уличном экране получил огромный общественный резонанс. Рекламная компания заявила, что стала жертвой атаки хакеров, и обратилась с заявлением в милицию. Житель Новороссийска через чужой сервер проник на сервер, контролирующий работу световодного экрана в Москве,. После того как взломал его, запустил крутое порно.. Ресурс взломанной хакером организации располагался в

	городе Грозном, где даже не подозревали, что их официальный сайт был взломан.
10-12	Государственный служащий либо работник (в лице системного администратора), используя имеющуюся у него на легитимной основе техническую возможность, вопреки установленному для него должностной инструкцией запрету осуществляет доступ к «закрытой» категории компьютерной информации, после чего осуществляет её копирование.
13-15	Программист М. с ноября по апрель следующего года он рассылал клиентам пяти интернет-провайдеров троянские программы, и получал логины с паролями, которыми пользовался для доступа в Интернет.
16-18	В октябре-ноябре 1998 года программист государственного предприятия Р., пользуясь своим служебным положением, совершил изменение ведомости начисления заработной платы на предприятии так, что у работников, которым начислялось более ста рублей, списывалось по одному рублю, эти средства поступали на счет, откуда их впоследствии снял Р.
19-21	Подросток в текстовом редакторе набирает краткое утверждение о том, что он любит своих родителей (сообщение), фиксируя, таким образом, сведения о его частной жизни, после чего сохраняет его на своем персональном ноутбуке. Сверстник-злоумышленник, подбирая BIOS-пароль, осуществляет доступ к данному файлу и осуществляет его копирование на свой флэш-носитель.
22-25	Гражданин в период с 1.05. по 31.08, , находясь у себя дома, используя свой персональный компьютер с установленным модемным устройством и соответствующим программным обеспечением, телефон, установленный по месту своего жительства, а также реквизиты пользователя сети Интернет: пароль и имя пользователя , зарегистрированный в ЗАО ", осуществлял неправомерный доступ к компьютерной информации, содержащейся на серверах ЗАО ". С телефонного номера за указанный период времени гражданин осуществил не менее 180 неправомерных выходов в Интернет. Указанные действия повлекли изменение статистической информации на сервере ЗАО об объеме услуг, представленных абоненту -., то есть модификацию компьютерной информации. Своими действиями, гражданин за указанный период времени нанес ЗАО ущерб в сумме 50000 рублей. Он показал, что весной 2004 года на одном из сайтов сети Интернет он обнаружил программу, при помощи которой можно получить реквизиты доступа в сеть Интернет, которыми пользуются зарегистрированные абоненты. При помощи указанной программы он получил реквизиты доступа (логин). С весны и до конца августа он осуществлял выход в сеть Интернет под данными реквизитами почти каждый день.
26-28	27-летний уроженец Пензенской области работал сотрудником оператора сотовой связи. В июле 2019 года он нарушил должностные инструкции: воспользовался доступом к базе данных и передал своей знакомой информацию о телефонных соединениях третьего лица без его ведома
ПТв1 1-4	Предприниматель без образования юридического лица, имея высшее техническое образование, опыт работы с ЭВМ и его программным обеспечением, приобретя у не установленного следствием лица лазерный компакт-диск «HACKER PRO», заведомо зная, что на данном диске содержится информация в виде компьютерных программ, зараженных кодом программ-вирусов, которые при запуске заведомо приводят к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, умышленно, из корыстных побуждений, преследуя цель распространения данного диска, продал указанный выше лазерный компакт-диск. После приобретения диска покупателем этот диск был изъят сотрудниками полиции.
5-8	Гражданин Д.. в марте, апреля, мае и июне 2014 года получал от своего знакомого по имени С. соответствующее оборудование, после чего в марте и апреле 2014 года, действуя совместно с незнакомой ему девушкой, а в мае и июне 2014 года с гражданином Ж., в ночное время устанавливал это оборудование на банкоматы, а через сутки также в ночное время снимал оборудование и передавал С. При снятии оборудования он и гражданин Ж.. были задержаны. В результате установки осужденными нештатного оборудования на банкомат 16 марта 2014 года были скомпрометированы (отсканированы) 316 банковских карт клиентов, на счетах которых находились денежные средства. В период с 20 по 21 марта 2014 года с восьми карт были обналичены и похищены денежные средства, которые позже были возвращены клиентам.
9-12	В январе текущего года года неустановленные лица неоднократно и незаконно осуществляли неправомерный доступ к охраняемой законом компьютерной информации, хранящейся на машинном носителе и в сети организации-провайдера – ЗАО «Колол», при незаконном подключении к сети Интернет под логином и паролем, предоставленными на

	основании договора № 16-ФЛ от 10 сентября 2012года Колову Р.Ю., проживающему по адресу: г. Москва ул. Гагарина д. 77 кв. 53. При этом к Колову приходили явно завышенные счета на оплату доступа к сети Интернет, однако о том, что в отношении него совершено преступление, он не догадывался. В ходе работы по уголовному делу было установлено, что неправомерный доступ осуществлялся посредством персонального компьютера, находящегося по адресу: г. Москва, ул. Вехова, д. 9,кв.9.В данной квартире проживают Бемёнова Н.А., 1960 г.р. и ее дети: Бемёнов Петр, 1990 г.р. и Бемёнова Дарья, 1983 г.р.
13-16	Служащий банка «Южный» Игрунков приобрел на рынке компакт–диск с компьютерной игрой «Звездные войны II». На следующий день Игрунков установил игру на своем рабочем компьютере, связанном по сети с другими компьютерами банка. В результате распространения вируса, записанного на компакт–диске, компьютерная система банка была выведена из строя и не могла нормально функционировать более суток, из–за чего банк понес существенные убытки.
17-20	Работники магазина стройматериалов Аханенко и Волкова провели «двойную прокатку» предъявленной к оплате кредитной карты без ведома ее держателя, в последующем изъяв наличные деньги на сумму 300 тыс. рублей по поддельному слипу (товарному чеку с оттиском кредитной карты и поддельной подписью истинного держателя)
21-24	Работник банка Ухина подделала пластиковую кредитную карту клиента, указав номера действительной кредитной карты, срока ее действия, но фиктивную фамилию владельца, и сняла со счета клиента 250 тысяч рублей.
ПИ1 1-3	Гражданин А. в неустановленное время, находясь по адресу: <адрес>, используя свой планшет фирмы «Asus» с Imei- кодом № -№ и доступ к глобальной сети Интернет через оператора сотовой связи ОАО «МТС», имея прямой преступный умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации, ее уничтожение, блокирование и модификацию, из корыстной заинтересованности, с целью получения материального вознаграждения в размере 5 000 рублей, совершил неправомерный доступ к принадлежащей ФИО1 учетной записи, Интернет сервиса «icloud», под логином № путем ввода пароля к ней № после чего не имея на то прав и разрешения законного владельца, изменил пароль к данной учетной записи, тем самым заблокировал к ней доступ, далее, используя эту учетную запись, заблокировал и стер всю имеющуюся на планшете гражданки Б.., марки «ipad 3» с lmei-ко<адрес>, компьютерную информацию, охраняемую Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», и вывел на экране устройства текст: «Это устройство было утеряно и стерто. Для возврата напишите письмо на id2015@ok.de Укажите в письме этот код устройства: 271». Продолжая свой преступный умысел, после получения электронного письма от гражданки Б. на гражданина А. электронную почту «id2015@ok.de», с текстом 271 последний направил в ответ инструкцию в виде текста, согласно которой, он требовал для разблокировки устройства перевода денежных средств, чего гражданка Б., делать не стала, а обратилась в отдел «К» УВД
4-6	Между администратором WEB сайта http://<данные изъяты>.ru/ Ч. и З.. произошел конфликт, в ходе которого последнему было сообщено о том, что тот нарушил пользовательское соглашение данного сайта, размещая не конкретизированную информацию и некорректно общаясь с пользователями сайта, в связи с чем, администратором было принято решение об удалении учетной записи З., о чем ему было сообщено. Учетная запись З. на WEB сайте http://<данные изъяты>.ru/ была удалена Ч. в тот же день, и в этот момент у З. возник преступный умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации и блокирование работы данного сайта, о чем он и сообщил администратору посредством электронного сообщения. Исполняя свой преступный умысел, с целью блокирования работы WEB сайта http://<данные изъяты>.ru/, З. нашел в информационно-телекоммуникационной сети «Интернет» вредоносную программу «<данные изъяты>», и установил ее на свой персональный компьютер. С помощью вредоносной программы «<данные изъяты>» З., используя принадлежащую ему ПЭВМ с IP-адресом ДД.ММ.ГГГГ, совершил неправомерный доступ к охраняемой законом компьютерной информации и неправомерное закрытие информации WEB сайта http://<данные изъяты>.ru/ и смежного с

	ним WEB сайта http://<данные изъяты>.ru/, осуществив DDOS-атаку. В результате действий З. произошло блокирование компьютерной информации и в целом работы WEB сайта http://<данные изъяты>.ru/, принадлежащего Б. и Ч., а также блокирование компьютерной информации и в целом работы сайта http://<данные изъяты>.ru/, принадлежащего И.
7-9	Гражданин Р. с личного мобильного телефона <данные изъяты> где были установлены специализированные программы <данные изъяты> через беспроводную сеть <данные изъяты> проигнорировав предупреждение об уголовной ответственности, осуществил сканирование трафика и перехватил сессию пользователя социальной сети <данные изъяты> Д. и Ч. и неправомерный доступ к охраняемой законом информации на аккаунте (учетная запись пользователя) последних, преодолев установленную пользовательскую защиту Д. и Ч. без введения логина и пароля и без согласия законного пользователя. После этого Р. осуществил доступ к охраняемой законом информации и ознакомился с защищенной от других пользователей сайта <данные изъяты> личной перепиской Д. и Ч. с иными лицами.
10-12	Гражданин Г. обладающий навыками пользования компьютерной техникой ДД.ММ.ГГГГ используя персональный компьютер, осуществил вход через Интернет, на сайт, с которого, незаконно скопировал на принадлежащие ему на USB- накопители <данные изъяты> вредоносные компьютерные программы <данные изъяты> предназначенную для нейтрализации средств защиты программного продукта <данные изъяты> и <данные изъяты> предназначенную для нейтрализации средств защиты программного продукта <данные изъяты>. Реализуя задуманное, Г. использовал компьютерные программы, в ходе проведения ОРМ <данные изъяты> с корыстной целью сбыл сотрудникам ОЭБ и ПК ЛО МВД России на транспорте, за денежное вознаграждение в размере <данные изъяты> рублей, путем инсталляции на жесткий диск компьютера <данные изъяты> незаконно приобретенные программные продукты: <данные изъяты> стоимостью <данные изъяты> рублей, <данные изъяты> стоимостью <данные изъяты> рублей, <данные изъяты> стоимостью <данные изъяты> рублей и <данные изъяты> стоимостью <данные изъяты> рублей, при этом использовал вредоносные компьютерные программы <данные изъяты> и <данные изъяты> которые позволили запустить установленные им экземпляры указанного программного продукта без установленного правообладателем аппаратного ключа защиты.
13-15	Гражданин В. посредством своего персонального компьютера с IP-адресом – 62.68.159.56, зарегистрированном в ООО «...» по адресу: <адрес>, с доступом к информационно-телекоммуникационной сети «Интернет», использовал вредоносную компьютерную программу «Intercepter-NG», что привело к копированию парольно-кодовой информации пользователей ресурса «odnoklassniki.ru» П. («...»), А.1 («...»), В.(«...»). После этого были взломаны страницы пользователей П., А.. Б., от имени которых начали рассылаться различные сообщения.
16-18	Гражданин К., приобрел, путем копирования через сеть Интернет с последующим сохранением на жестком диске своего компьютера, компьютерную программу предназначенную для внедрения в структуру Интернет-сайтов и компьютерную программу, предназначенную для внесения изменений в Интернет-сайты, путем модификации структуры сайта. Затем, К., находясь по месту своего проживания по указанному выше адресу, из личной заинтересованности скопировал через сеть Интернет с последующим сохранением на жестком диске своего компьютера информацию об уязвимости сайта, что дало возможность устанавливать другие программы для доступа к информационным ресурсам сайта <***> принадлежащего <***>, а также использовав вредоносную компьютерную программу приобретенную ранее, загрузил ее на сайт <***> что привело к несанкционированной модификации компьютерной информации на указанном сайте и изменило структуру сайта, непредусмотренным правообладателем способом.
19-21	Гражданин А, находясь на своем рабочем месте, предоставленном ООО «Грайд», расположенном по адресу: город М., используя средства авторизации (логин и пароль), предоставленные ООО «Грайд», и имея, в силу исполняемых обязанностей, доступ к информационным носителям, на которых содержится охраняемая компьютерная информация, и действуя в нарушение Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года №149-ФЗ, ст.1225 ГК РФ «Охраняемые результаты интеллектуальной деятельности и средства индивидуализации», Указа Президента Российской Федерации от 06 марта 1997 года №188 «Перечень сведений конфиденциального характера», соглашения о сохранении служебной и коммерческой тайны, соглашения о конфиденциальности для сотрудников ООО «Грайд», а так же должностной инструкции по должности ведущий системный администратор UNIX ООО «Грайд», скопировал на USB – носитель информацию из базы

	данных ООО «Грайд», а именно: не менее 40.000 записей, содержащих не прошедших проверку имен, фамилий, никнеймов (имена, которые используется при регистрации на интернет сайтах), а так же адресов электронной почты. После чего А. передал вышеуказанную информацию И., который не был осведомлен о том, что полученная им информация охраняется внутренними документами ООО «Грайд», а так же действующим законодательством РФ.
22-24	Студент Технического университета Артемов, Преодолев ради любопытства систему защиты коммерческого эротического вебсайта, распространил информацию о способе взлома системы защиты этого сайта в компьютерной сети. Там же он поместил информацию о зарегистрированных пользователях упомянутого сайта, включая сведения о номерах их кредитных карт. В последующие несколько часов сайт подвергся массированным атакам сетевых хулиганов со всего мира, в результате чего прекратил функционирование на несколько дней. Кроме того, нелегальным использованием кредитных карт был причинен ущерб их законным владельцам.
25-27	Студент Технического университета Тыганова установила на клавиатуры специальную «насадку», которая внешне повторяла оригинальные кнопки. Владелец карты снял деньги со счета, поддельная клавиатура запомнила все нажатые клавиши, в том числе и пин-код. Тыганова спустя некоторое время сняла насадку, и после анализа записанной на ней информации, изготовив дубликат карты, сняла со счета владельца 500 тысяч рублей.
28-30	Студент Технического университета Личев использовал «Другое устройство» – это то, что англичане еще называют lebanese loops. Это пластиковые конверты, размер которых немного больше размера карточки, их закладывают в щель банкомата. Хозяин кредитки пытался снять деньги, но банкомат не мог прочитать данные с магнитной полосы. К тому же из-за конструкции конверта вернуть карту не получилось. В это время подошел Личев и сказал, что буквально день назад с ним «случилось то же самое» и для того, чЧтобы вернуть карту, надо просто ввести пин-код и нажать два раза на Cancel. Владелец карточки попробовал, и, конечно же, у него ничего не получилось. Он решил, что карточка осталась в банкомате, и ушел, чтобы связаться с банком. Личев достал кредитку вместе с конвертом при помощи простых подручных средств. Пин-код он уже знал, т.к. владелец (теперь уже бывший) «пластика» сам его ввел в присутствии Личева. Личев снял со счета 100 тысяч долларов

Содержание