Методика расследования неправомерного доступа к компьютерной информации

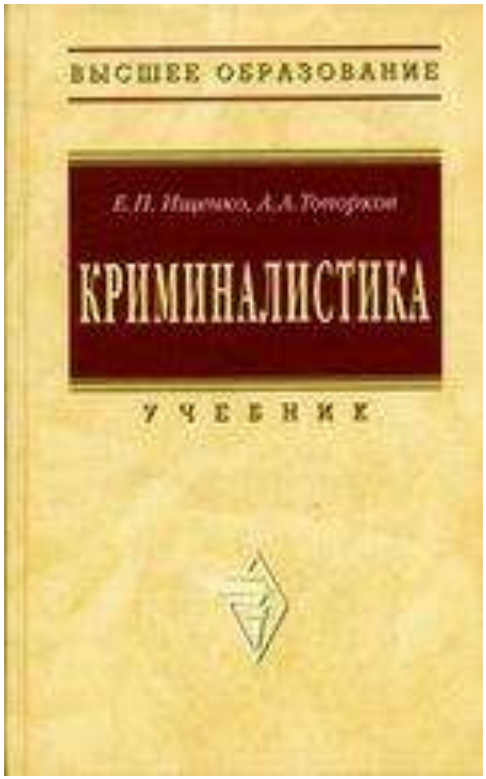
Выполнила: студентка
2 курса, гр. ЮФм-42
Белоусова Елена Александровна

Методика расследования неправомерного доступа к компьютерной информации

Вопросы

1. Криминалистическая характеристика
2. Первоначальный этап
3. Последующий этап

Литература



1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 31.12.2014)
2. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: учебник / под ред. Р.С. Белкина. – М.: НОРМА, 2011. – 990 с.
3. Криминалистика. Ищенко Е.П., Топорков А.А 2-е изд., испр., доп. и перераб. - М.: Контракт, ИНФРА-М, 2010. - 784 с.

Элементы криминалистической характеристики

Наиболее важными элементами криминалистической характеристики преступлений, связанных с неправомерным доступом к компьютерной информации, являются:

1. Способы совершения преступлений;
2. Орудия совершения преступлений;
3. Обстановка совершения преступлений;
4. Время;
5. Место;
6. Следообразования;
7. Характеристика личности преступника;
8. Мотивы;
9. Цели;
10. Характеристика личности потерпевшего;

Способы совершения преступлений

Первая группа:

Реализуется без использования компьютерных средств в качестве инструмента для проникновения в информационные системы или воздействия на них.

Вторая группа:

Осуществляется с использованием компьютерных и коммуникационных устройств.

Способы совершения преступлений (первая группа)

а) хищение машинных носителей информации в виде блоков и элементов ЭВМ;

б) использование визуальных, оптических и акустических средств наблюдения за ЭВМ;

в) считывание и расшифровка различных электромагнитных излучений компьютера и обеспечивающих систем;

Способы совершения преступлений (первая группа)

г) фотографирование информации в процессе ее обработки;

д) изготовление бумажных дубликатов входных и выходных документов, копирование распечаток;

е) использование оптических и акустических средств наблюдения за лицами, имеющими отношение к необходимой злоумышленнику информации, фиксация их разговоров;

Способы совершения преступлений (первая группа)

ж) осмотр и изучение не полностью утилизированных отходов деятельности компьютерных систем;

з) вступление в прямой контакт с лицами, имеющими отношение к необходимой злоумышленнику информации, получение от них под разными предлогами нужных сведений и др.

Способы совершения преступлений (вторая группа)

1) использование чужого имени;

2) изменение физического адреса технического устройства;

3) подбор пароля;

4) нахождение и использование «пробелов» в программе;

5) любой другой обман системы защиты информации.

Орудия совершения преступлений

- Средства компьютерной техники;
- Специальное программное обеспечение;
- Средства непосредственного и удаленного доступа.

Одним из распространенных орудий неправомерного доступа к компьютерной информации является сам компьютер.

Обстановка совершения преступлений

Благоприятная обстановка:

- Невысокие технико-организационный уровень деятельности;
- Слабый контроль за информационной безопасностью;
- Не установлена система защиты информации;
- Атмосфера равнодушия к эпизодам нарушения требований информационной безопасности.

Обстановка совершения преступлений

- Время

Время несанкционированного доступа можно определить:

- С помощью программ общесистемного назначения;
- В ходе следственного осмотра компьютера, его распечаток или дискет;
- Путем допроса свидетелей из числа сотрудников данной компьютерной системы.

Обстановка совершения преступлений

- Место

Место несанкционированного доступа может быть :

- В отличительном месте от нахождения информации;
- На какой-либо конкретной территории;
- На территории нескольких государств;
- В месте совершения преступления.

Обстановка совершения преступлений

• Следы

Следами могут быть :

- Следы на магнитных носителях информации;
- Рукописные записи, распечатки и т. п.;
- Следы на технике (отпечатки рук, микрочастицы на клавиатуре и т. д.);
- Результаты работы некоторых программ;
- Следы образуемые при удаленном доступе.

Обстановка совершения преступления

- Следы

Следами, указывающие на неправомерный доступ к информации:

1. Трасологические следы;
2. Переименование файлов;
3. Изменение размеров и содержания файлов;
4. Изменение стандартных реквизитов файлов, даты и времени их создания;
5. Появление новых каталогов, файлов и т.д.

Характеристика личности преступника

- Мужчины в возрасте — от 15 до 45 лет;
- Высокий интеллектуальный уровень;
- Высшее или среднее математическое, инженерно-техническое, экономическое образование;
- Наличие соответствующего опыта, навыков или специальной подготовки в данной области;
- Профессиональная деятельность связана с информационными ресурсами или свободным доступом к компьютерным сетям;
- Психологические аспекты: замкнутость, скрытность, небольшой круг общения;
- Интересы: чтение литературы по компьютерной технике, информационным технологиям, программным обеспечением;
- Ранее не судим;

Характеристика личности преступника

«Компьютерные хулиганы» - хакеры:

• Цель – озорство, овладение информацией, введение ложных данных;

• Заинтересованные компьютерной техникой лица – школьники, студенты – совершенствующиеся на взломах защитных механизмов компьютерных систем;

• Действуют ради спортивного интереса; самовыражение;

• Любопытство, желание проверить свои силы;

Характеристика личности преступника

Особенности:

• отсутствие целеустремленной, продуманной подготовки к преступлению;

• оригинальность способа;

• использование в качестве орудий преступления бытовых технических средств и предметов;

• непринятие мер к сокрытию преступления.

Характеристика личности преступника

Профессиональные преступники:

- наличие корыстной цели;
- обладание устойчивыми преступными умениями;
- высококвалифицированные специалисты;
- возможная принадлежность к организованным преступным группам и сообществам, оснащенным продвинутой техникой;
- характерно совершение особо опасных должностных преступлений, совершаемых с использованием средств компьютерной техники, присвоение денежных средств в особо крупных размерах и т.д.;

Характеристика личности преступника

Особенности:

• целеустремленная, продуманная подготовка к противоправным действиям;

• использование модифицированных известных вредоносных программ, либо специально разработанных для совершения конкретного противоправного действия;

• сокрытие следов незаконного деяния.

Характеристика личности преступника

Большинство лиц, совершивших компьютерные преступления, это:

• Пользователи ЭВМ, имеющие определенную подготовку и доступ к компьютерной сети;

• Операторы, системные программисты, лица, производящие техническое обслуживание и ремонт компьютерных сетей или систем;

• Административно-управленческий персонал (руководители высшего и среднего звена, бухгалтеры, экономисты и др.).

Характеристика личности преступника

- Мотивы

- Корысть (65%) ;
- Политические (13%);
- Хулиганские побуждения (10%);
- Месть (5%);
- Коммерческий шпионаж, диверсия (5%);
- Иные (2%).

Характеристика личности преступника

• Цели

- Отмывание денежных средств;
- Подделка документов, счетов;
- Хищение наличных или безналичных денежных средств;
- Фальсификация платежных документов и т.п.;
- Незаконное получение кредита;
- Скрыть другое преступление;

Характеристика личности потерпевшего

Потерпевшими чаще всего являются:

1. Государство;

2. Собственники компьютерной системы, пользователи и их клиенты;

3. Граждане;

Потерпевший часто неохотно сообщает (или вовсе не сообщает) правоохранительным органам о преступных фактах в сфере движения компьютерной информации.

Характеристика личности потерпевшего

Причины не сообщения о факте преступного деяния:

- Некомпетентность сотрудников правоохранительных органов в данном вопросе;
- Боязнь, что убытки от расследования превысят размер причиненного ущерба и к тому же будет подорван авторитет фирмы;
- Боязнь раскрытия в ходе судебного разбирательства системы безопасности организации;

Характеристика личности потерпевшего

Причины не сообщения о факте преступного деяния:

- Боязнь выявления собственных незаконных действий;
- Боязнь должностных лиц, что одним из итогов расследования станут выводы об их профессиональной непригодности (некомпетентности);
- Правовая неграмотность;
- Непонимание истинной ценности имеющейся информации.

Первоначальный этап расследования

1. Осмотр места происшествия;
2. Выемка;
3. Допрос свидетелей;
4. Проведение оперативно-розыскных мероприятий;
5. Опрос граждан;
6. Розыск лиц, компьютерного оборудования, компьютерной информации, программного обеспечения;
7. Задержание подозреваемого;
8. Допрос подозреваемого;
9. Назначение и проведение экспертиз.

Осмотр места происшествия

1) объект, на который направлено действие;

2) следы его совершения;

3) следы орудий и других средств, приспособлений, использованных в ходе преступного действия;

4) наступивший результат действия.

Осмотр места происшествия

Перед началом осмотра необходимо определить:

- Число компьютеров, их тип;
- Организацию электропитания и есть ли автономные источники питания;
- Используемые носители компьютерной информации;
- Подключение к локальной сети и выхода в другие сети (например, у провайдера - поставщика сетевых услуг);
- Используемое системное и прикладное программное обеспечение;

Осмотр места происшествия

• Наличие каких-либо систем защиты информации, их типы;

• Наличие средств срочного уничтожения компьютерной информации и возможность их применения;

• Квалификацию пользователей и владельцев компьютеров и сведения о них, а также отношения в коллективе сотрудников, которые обслуживают технику (в случае производства осмотра (обыска) в организации).

:

Выемка

Изъятие компьютерной информации:

1. Наличие у подозреваемого (обвиняемого) или потерпевшего специального образования в области вычислительной техники и информатики;
2. Сведения об увлечении вышеуказанных лиц компьютерной техникой, информатикой и программированием или об их нередких контактах с людьми, имеющими такие интересы;
3. Присутствие в материалах дела документов, которые изготовлены машинным способом;
4. Хищение носителей компьютерной информации.

Допрос свидетелей (руководство, персонал, иные сотрудники организации)

Необходимо выяснить следующие обстоятельства:

•время и обстоятельства выявления преступления;
•приметы, по которым оно было обнаружено;
•круг лиц, которые имеют доступ к компьютеру и в помещения, где располагалась компьютерная техника;
•появлялись ли там посторонние лица;
•круг лиц, которые могут знать коды и пароли доступа;
•кто разрешал доступ к закрытой компьютерной информации и кто действительно был допущен;
•круг лиц, которые обладают необходимыми знаниями и навыками, для совершения компьютерного преступления, или занимающихся программированием;

Допрос свидетелей (руководство, персонал, иные сотрудники организации)

Необходимо выяснить следующие обстоятельства:

•используемые на компьютере программы защиты от несанкционированного доступа и антивирусные программы;
•кто в организации использовал компьютер для посторонних целей, (например, устанавливал игры, программы, переносил фильмы, музыку и т.п.) и самостоятельно устанавливал и запускал какие-либо программы;
•привлекались ли в организации к решению определенных задач или устранению проблем посторонние нештатные программисты и сведения, которые имеются о них;
•какой вред причинен преступлением и имеются ли способы его уменьшить.

Проведение оперативно-розыскных мероприятий

1. Опрос
2. Наведение справок
3. Сбор образцов для сравнительного исследования
4. Исследование предметов и документов.
5. Наблюдение
6. Обследование помещений, зданий, сооружений, участков местности и транспортных средств.
7. Контроль почтовых отправлений, телеграфных и иных сообщений
8. Прослушивание телефонных переговоров.
9. Снятие информации с технических каналов связи
10. Оперативное внедрение.

Опрос граждан

Вербальный контакт сотрудника оперативного подразделения с гражданами, которые:

- Располагают
- Или могут располагать

информацией

представляющей определенный интерес для оперативно-розыскных органов.

Это могут быть:

- сведения о преступлениях
- лицах, его совершивших
- следах преступной деятельности и т.п.

Розыск лиц

Признаки:

•Общие (пол, возраст, национальность, внешние приметы, место проживания, род деятельности);

•Специальные (обладание навыками в информационных технологиях, знание компьютерного оборудования, обладание специальным компьютерным оборудованием и т.д.);

Розыск компьютерного оборудования

Признаки:

•Конфигурация компьютера, который был использован для совершения преступления;

•Мобильность такого компьютерного оборудования;

•Наличие какой-либо сетевой или периферийной техники;

•Установка на компьютере определенного программного обеспечения;

Розыск компьютерной информации и программного обеспечения

Признаки:

•Название отдельных файлов и архивов;

•Дата и время создания, изменения или перезаписи файлов;

•Дата и время поступления файлов по электронной почте;

•Содержание файла;

•Характер зашифровки компьютерной информации, особенности работы компьютерной программы и т.д.

Задержание и допрос подозреваемого

Устанавливается:

•сведения о его личности;

•об использовании для неправомерного доступа своего служебного, должностного положения и в чем это конкретно выразилось;

•взаимоотношения с сослуживцами;

•уровень профессиональной подготовки;

•наличие опыта по созданию компьютерных программ;

•причины совершения преступления;

Задержание и допрос подозреваемого

Устанавливается:

•мотивы совершения преступления;

•способ совершения преступления, способы преодоления информационной защиты;

•соучастники или он действовал один;

•какие изменения в работу компьютерных систем были внесены;

•какие использовались технические средства и программы для совершения преступления;

•источники финансовых средств для приобретения оборудования и программного обеспечения;

Задержание и допрос подозреваемого

Устанавливается:

•сведения об источнике приобретения программного обеспечения и идентификационных данных;

•способ разработки программ, которыми пользовался злоумышленник, алгоритм их действия;

•уровень доступа злоумышленника, имеются ли у подозреваемого пароли и коды доступа к зашифрованной им информации;

•есть ли возможность быстро устранить или уменьшить причиненный вред.

Назначение и проведение экспертиз

По данной категории преступлений проводятся следующие экспертизы:

- Аппаратно-компьютерная экспертиза;
- Программно-компьютерная экспертиза;
- Информационно-компьютерная экспертиза;
- Компьютерно-сетевая экспертиза;
- Товароведческая экспертиза;
- Трасологическая экспертиза;
- Дактилоскопическая экспертиза;
- Судебно-экономическая экспертиза;
- Технико-криминалистическая экспертиза;
- Экспертиза компьютерно-технической информации;

Последующий этап расследования

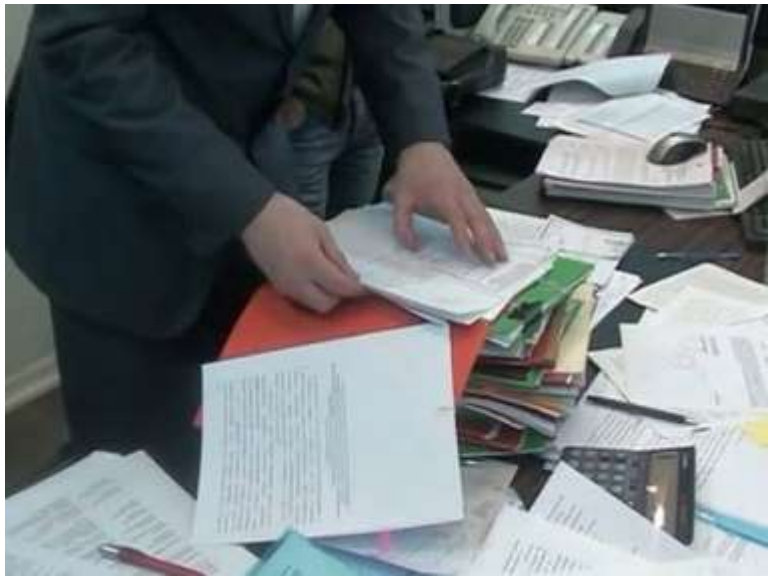
1. Обыск;
2. Допрос подозреваемого;
3. Предъявление для опознания;
4. Очная ставка;
5. Следственный эксперимент;
6. Проверка показаний на месте;
7. Назначение и проведение экспертизы.

Обыск

Следователю необходимо получить достоверные данные о:

- Виде и конфигурации используемой ЭВМ;
- Подключена ли она к локальной или глобальной сети (типа Интернет);
- Наличии службы информационной безопасности и защиты от несанкционированного доступа;
- Системе электропитания помещений, где установлена вычислительная техника;

Обыск



Следователю необходимо получить достоверные данные о:

- Квалификации пользователей;
- Установить местонахождение всех средств компьютерной техники;
- Собрать сведения о сотрудниках, обслуживающих вычислительную технику (взаимоотношениях в коллективе, его возможной криминализации и т. д.).

Обыск

- Поиск тайников, где могут храниться сменные компьютерные носители информации;

- Наличие специальной литературы по программированию, взлому, созданию вредоносных программ и т.д.;

- Наличие классических следов (следы рук и т.д.) на клавишах включения и перезагрузки компьютера, кнопках периферийных устройств, клавиатуре, розетке, мыши и т.д.;

Обыск

• Осмотреть имеющиеся документы, вплоть до записей на клочках бумаги (записи о паролях, пользователях, какой-либо план и т.д.);

• С помощью специалиста вскрывать корпуса аппаратных средств компьютерной техники, чтобы обнаружить специально отключенные внутренние носители информации;

• Изъятие средств компьютерной техники, технических устройств, документации, электронной информации и др.

Допрос подозреваемого

Следователю необходимо :

- Тщательно изучить все материалы дела;
- Особенности личности обвиняемого;
- Способы совершения преступления;
- Доказательства, указывающие на виновность конкретного лица;

Допрос подозреваемого

Следователю необходимо :

- Предъявить обвинение и допросить;
- Получить ответ обвиняемого на вопрос, признает ли он себя виновным в предъявленном ему обвинении;
- Предложить обвиняемому дать показания по существу обвинения.

Предъявление для опознания

Для опознания предъявляется :

- Компьютерная информация в виде программ, различных файлов;
- Носители информации;
- Компьютерная техника;
- Предметы;
- Люди;
- Объекты, изображенные на фотографиях.

Предъявление для опознания

Результат:

- Установить преступников;
- Компьютерную технику, использованную при совершении неправомерного доступа;
- Компьютерную информацию;
- Различные предметы и объекты, связанные с данным преступлением.

Очная ставка

Следователю необходимо :

• Предусмотреть вопросы, которые вызывали бы ассоциации;

• Запланировать рассмотрение смежных событий и обстоятельств;

• Решить, какие и когда именно доказательства (например, предметы, документы, компьютерную технику или компьютерную информацию) предъявить;

Очная ставка

Следователю необходимо :

• Демонстрировать результаты следственных действий (фотоснимки, схемы, планы, чертежи, распечатки компьютерной информации, изъятые черновые записи и пр.);

• Привлечение к участию свидетелей, которые дали правдивые показания и которые будут изобличать обвиняемого в даче ложных показаний, для того чтобы он принял решение о даче правдивых показаний.

Следственный эксперимент

Виды:

• По проверке возможности проникновения в помещение (через двери, окно, с отключением и без отключения сигнализации);

• По проверке возможности подключения компьютерной техники и совершения непосредственного доступа к компьютерной информации;

Следственный эксперимент

Виды:

• По проверке возможности проникновения в закрытые зоны (путем подбора паролей, идентификационных кодов и установлению периода времени на данный подбор);

• По проверке возможности подключения к компьютерной сети;

• По проверке возможности электромагнитного перехвата;

Следственный эксперимент

Виды:

• По установлению периода времени, необходимого на подключение к компьютерной сети;

• По установлению периода времени, необходимого на отключение технических средств защиты информации;

• По установлению промежутка времени, необходимого для модификации, копирования компьютерной информации;

Следственный эксперимент

Виды:

• По проверке возможности совершения определенных операций с компьютерной информацией в одиночку;

• По проверке возможности совершения определенных операций с помощью конкретной компьютерной техники за определенный промежуток времени и др.

Следственный эксперимент

Правила:

1. Оптимальное количество участников следственного эксперимента, которое ограничивается составом, без которого невозможно получить объективные результаты.

2. Наибольшее сходство условий проведения следственного эксперимента и условий, в которых совершался неправомерный доступ к компьютерной информации.

3. В целях исключения случайных результатов, обеспечения достоверности и наглядности, опытные действия необходимо осуществлять неоднократно.

Следственный эксперимент

Правила:

4. Производство действий в меняющихся по степени сложности условиях, если следствие не имеет точные данные об условиях проверяемого события.

5. Соответствие профессиональных навыков лица, которое осуществляет опыты, профессиональным навыкам непосредственного участника исследуемого события.

6. Обеспечение безопасности всех участников следственного эксперимента.

Проверка показаний на месте

Правила:

1. Организовать комплекс мероприятий, включающий сбор и анализ информации, необходимой для проведения СД;

2. Установить, что важные условия обстановки, в которой происходит проверка показаний, не претерпели существенных изменений, влияющих на ход и результаты СД;

Проверка показаний на месте

Правила:

3. Убедиться в наличии определенных объектов, их размещении, а так же соотнести показания проверяемого лица с фактической обстановкой;

4. Определение времени проведения СД для уменьшения опасности вмешательства посторонних лиц, создания безопасных условий для участников ;

Проверка показаний на месте

Правила:

5. Заранее известить граждан, работающих или проживающих в помещениях, в которые необходимо войти;

6. Подготовить разнообразные технические и иные средства (средства связи и освещения, средства фиксации хода и результатов СД, компьютерная техника, которая использовалась при совершении преступления или находилась на месте происшествия).

Назначение и проведение экспертиз

Эксперту предоставляются объекты:

- Изъятые в ходе следственного действия;
- Переданные кем-нибудь из участников процесса или посторонними лицами;
- Истребованная в учреждениях, предприятиях и у должностных лиц техническая документация на программные продукты, как проектного, так и пользовательского содержания.

Назначение и проведение экспертиз

Могут быть поставлены вопросы о:

1. Работоспособности объектов экспертизы, пригодности их использования для совершения тех или иных действий;
2. Периодах функционирования (использования) объектов экспертизы;
3. Действиях, произведенных с объектами экспертизы (или с использованием объектов экспертизы);

Назначение и проведение экспертиз

Могут быть поставлены вопросы о:

Наличии/отсутствии на объектах экспертизы интересующей информации, в том числе в удаленном или зашифрованном виде;

Функциях программного обеспечения, позволяющих отнести объект экспертизы к категории вредоносного программного обеспечения;

Назначение и проведение экспертиз

Могут быть поставлены вопросы о:

6. Функциях программного обеспечения;

7. Соответствии программного обеспечения заявленным (или требуемым) функциям, соответствии техническому заданию на разработку, соответствии договору на разработку;

8. Степени сходства объектов экспертизы между собой;

Назначение и проведение экспертиз

Могут быть поставлены вопросы о:

9. Проверке корректности (правильности) электронной цифровой подписи (ЭЦП);

10. Особенностях сетевого взаимодействия с объектами экспертизы (например, в случаях несанкционированного доступа с использованием каналов связи или в случаях атак на ресурсы сети Интернет).

Спасибо за внимание!