ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 4

1. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ. ОБЩАЯ ЧАСТЬ 8

1.1. Правовое регулирование отношений в области компьютерной информации 8

1.1.1. Основные понятия 8

1.1.2. Отечественное законодательство в области компьютерного права 12

1.2. Уголовно-правовая характеристика главы 28 УК РФ Преступления в сфере компьютерной информации 13

1.2.1. Общие признаки преступлений в сфере компьютерной информации 13

1.2.2. Уголовно-правовой анализ ст. 272 гл. 28 УК РФ Неправомерный доступ к компьютерной информации 16

1.2.3. Уголовно-правовой анализ ст. 273 гл. 28 УК РФ Создание, распространение и использование вредоносных программ для ЭВМ 18

1.2.4. Уголовно-правовой анализ ст. 274 гл. 28 УК РФ Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети 20

2. РАССЛЕДОВАНИЕ 22

2.1. Понятие: значение и виды предварительного расследования 22

2.2. Понятие: и виды следственных действий 24

2.3. Следственные действия по делам рассматриваемой категории 25

2.3.1. Допрос свидетеля и потерпевшего 25

2.3.2. Следственный осмотр 27

2.3.3. Обыск и выемка 30

2.3.4. Назначение и производство экспертизы 32

2.3.5. Следственный эксперимент 33

2.3.6. Допрос обвиняемого и подозреваемого 35

3. РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ. 37

3.1. Расследование неправомерного доступа к компьютерной информации 37

3.1.1. Общая схема расследования неправомерного доступа к компьютерной информации. 37

3.1.2. Способы краж в банковских информационно-вычислительных системах 47

3.2. Расследование создание: распространение и использование вредоносных программ для ЭВМ 52

3.3. Расследование нарушения правил эксплуатации ЭВМ: системы ЭВМ или их сети 57

ЗаклюЧение 68

Список использованной литературы 71

Приложение 73

ВВЕДЕНИЕ

В динамичных условиях XX в? общество постоянно сталкивается с проблемами различного характера: порождение которых зачастую вызвано стремлением общества к созданию более совершенных и эффективных моделей своего существования? Сказанное в полной мере относится и к такой специфической сфере: как область применения электронной техники и информационных технологий? Создание электронно-вычислительной техники четвертого и пятого поколения с потенциально неограниченными возможностями: их широкое распространение в экономической: социальной и управленческой сферах: появление в быту значительного количества персональных ЭВМ явились не только новым свидетельством технического прогресса: но и с неизбежностью повлекли за собой и негативные последствия: связанные со злоупотреблениями при использовании средств ЭВМ: информационных технологий? Вот вкратце история возникновения проблемы %

Первым человеком: использовавшим возможности ЭВМ для совершения налогового преступления на сумму 620 тыс? долл? в 1969 г? в США: считается Альфонсе Конфессоре? Последующий: даже краткий по изложению: послужной список злоупотреблений с ЭВМ выглядит внушительно? В конце 70-х годов — хищение более 10 млн? долл? из Секьюрити пасифик бэнк\* 1979 г компьютерное хищение в Вильнюсе 78584 руб?\* 1984 г?— сообщение о первом в мире компьютерном вирусе\* 1985 г?— вывод из строя при помощи вируса электронной системы голосования в конгрессе США\*1987 г? — заражение в США Пакистанским вирусом более 18 тыс? компьютеров\* 1989 г? — попытка компьютерного ограбления на сумму более 69 млн? дол? чикагского банка Фэрст нэшнл бэнк\* блокировка американским студентом 6000 ЭВМ Пентагона\* международный съезд компьютерных пиратов в Голландии с демонстрацией возможности неограниченного внедрения в системы ЭВМ\* 1991 г?— хищение во Внешэкономбанке на сумму в 125:5 тыс? долларов\* 1992 г?— умышленное нарушение работы АСУ реакторов Игналинской АЭС путем попытки внедрения вирусов\* 1993 г? — попытка электронного мошенничества в ЦЕ России на сумму более 68 млрд? руб 68 млрд? руб? 309 млн? руб?\* 1995 г? — попытка российского инженера Левина путем перевода на счета в банки 7 стран похитить из *Сити* бэнк в США 10 млн? долл? 400 тысяч из которых до сих по не обнаружены?\* и наконец: в конце 1997 г? компьютерные умельцы прорвались в Яху — одну популярных поисковых систем в Интернете и под угрозой заражения всей сети компьютерным вирусом потребовали освобождения • из-под ареста одного из своих коллег?

Обвальное появление в России большого числа персональных компьютеров импортного производства и построение на их базе компьютерных сетей: имеющих прямой доступ к глобальным информационным системам: заставляет пристальнее приглядеться к подлинным и мнимым опасностям: которые таит в себе современная информатизация общества: оценить ущерб от взлома широкого класса компьютерных сетей — от локальных до глобальных телекоммуникационных систем? Ежегодный экономический ущерб от такого рода преступлений только в США составляет около 100 млрд долларов: причем многие потери не обнаруживаются или о них не сообщают по причине высокой латентности данных преступлений порядка 90?? В Европе: по данным Ассоциации производителей компьютерного обеспечения: убытки оцениваются в 6 млрд? долларов ежегодно? Ежедневно только американские крекеры специалисты по взлому программного обеспечения ЭВМ крадут около 4 млн? долларов в 2 раза больше: чем во всех остальных кражах? В настоящее время только в Москве с помощью поддельной кредитной карточки для электронных расчетов за один раз похищается порядка 300 тыс? долларов? По данным МВД РФ: потери российского бюджета от неуплаты налогов продавцами компьютерных программ составляют 85 млн? долларов? Деньга: полученные от продажи: часто уходят в распоряжение криминальных структур? Кроме того: 105 млн? долларов теряют российские предприятия? В области разработки компьютерных программ и баз данных в стране работает около шести тысяч фирм: обеспечивающих занятость более 200 тыс? человек? Если положение не изменится: этой сфере производства грозит стагнация: поскольку программисты попросту потеряют стимулы к созданию новых передовых программных продуктов?

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том: что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных: включая и жизнеобеспечивающие: объектов: серьезное нарушение работы ЭВМ и их систем? Несанкционированные действия по уничтожению: модификации: искажению: копированию информации и информационных ресурсов: иные формы незаконного вмешательства в информационные системы способны вызвать тяжкие и необратимые последствия: связанные не только с имущественным ущербом: но и с физическим вредом людям? Опасность компьютерных преступлений многократно возрастает: когда они совершаются в отношении функционирования объектов жизнеобеспечения: транспортных и оборонных систем: атомной энергетики?

Вышеприведенные факты убедительно свидетельствуют о действительной остроте проблемы с преступлениями в сере компьютерной информации? Преступления данной категории причиняют как серьезный экономический ущерб: так и непосредственную угрозу даже существованию человечества?

Практическим работникам следственных органов довольно сложно расследовать данную категорию дел? Необходимо в совершенстве владеть знаниями компьютерной технологии: а также механизма обработки компьютерных данных?[20]

Цель данной работы – подвергнуть всестороннему изучению специфики расследования преступлений в сфере компьютерной информации?

Для этого были поставлены следующие задачи %

1 изучение стержневых понятий по данному вопросу: а именно понятие преступления в сфере компьютерной и понятие расследование\*

2 изучение производства следственных действий по делам рассматриваемой категории: последовательность их проведения\*

3 по возможности выработать общий план расследования преступлений в сфере компьютерной информации\*

4 рассмотреть имеющиеся методики расследования преступлений в сфере компьютерной информации и: главным образом: изучить методику: содержащуюся в книге Руководство для следователей Руководство для следователей / Под ред? Н?А? Селиванова: В?А? Снеткова – М?: ИНФРА – М: 1997? – IV: 732 с?: как одну из рекомендуемых методик: разработанных для уголовных дел рассматриваемой категории?

В процессе работе над дипломной работой использовалась следующая литература% федеральные законы\* учебники по уголовному праву: уголовному процессу: и криминалистике\* журнальные публикации ряда практических и теоретических работников?

# ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ? ОБЩАЯ ЧАСТЬ

## Правовое регулирование отношений в области компьютерной информации

### Основные понятия

#### Информация

Важно различать информацию как термин обыденной жизни и *как* правовую категорию? Информация: как таковая: представляет собой категорию идеального: она неосязаема: непотребляема не амортизируется и не может быть объектом правоотношений безотносительно к ее носителю: содержанию: идентифицирующим признакам? В праве под информацией понимаются сведения о лицах: предметах: фактах: событиях: явлениях и процессах: содержащихся в информационных системах? Весьма тесно связано с понятием информации и понятие информационных ресурсов: под которыми понимаются от дельные документы и отдельные массивы документов: документы и массивы документов в информационных системах?**[17]**

#### Компьютерная информация

Введение законодателем в Уголовный кодекс термина компьютерная информация является новшеством? Ранее в Российском законодательстве: регулирующем информационные правоотношения: определения информации как компьютерной не существовало? Вероятней всего: определение компьютерная применительно к информации возникло для отграничения данного объекта посягательства от информационных преступлений: предусмотренных другими разделами Уголовного кодекса РФ? Крылов предлагает следующее криминалистическое определение компьютерной информации как специального объекта преступного посягательства? Компьютерная информация есть сведения: знания или набор команд программа: предназначенные для использования в ЭВМ или управления ею: находящиеся в ЭВМ или на машинных носителях — идентифицируемый элемент ин формационной системы: имеющей собственника: установившего правила ее использования?**[16]**

#### Конфиденциальная информация

Понятие конфиденциальной информации было введено в отечественную правовую практику с принятием Таможенного кодекса Российской Федерации? В ст? 16 приводится точное и емкое определение: конфиденциальная информация — это информация: не являющаяся общедоступной и могущая нанести ущерб правам и законным интересам предоставившего ее лица**[14]?** В законе Об информации: информатизации и защите информации ст? 2 предлагается другая формулировка: документированная информация: доступ к которой ограничивается в соответствии с законодательством Российской Федерации Указ Президента РФ Об утверждении перечня сведений конфиденциального характера» от 06:03:97г? N188?

Конфиденциальными в соответствии с законом являются: в частности: такие виды информации: как:

 содержащая государственную тайну Закон РФ О государственной тайне ст?ст? 275: 276: 283: 284 УК РФ\*

передаваемая путем переписки: телефонных переговоров: почтовых телеграфных или иных сообщений ч? 2 ст? 23 Конституции РФ: ст? 138 УК РФ\* касающаяся тайны усыновления ст? 155 УК РФ\*

содержащая служебную тайну ст? 139 ГК РФ: коммерческую тайну ст? 139 ГК РФ и ст? 183 УК РФ: банковскую тайну ст? 183 УК РФ: личную тайну ст? 137 УК РФ: семейную тайну ст? 137 УК РФ: информация: являющаяся объектом авторских и смежных прав Закон РФ Об авторском праве и смежных правах: ст? 146 УК РФ\*

информация: непосредственно затрагивающая права и свободы гражданина или персональные данные Федеральный закон Об информации: информатизации и защите информации: ст? 140 УК РФ и др?

#### Информационные ресурсы

Понятие информационных ресурсов: весьма тесно связано с понятием информации под которыми понимаются отдельные документы и отдельные массивы документов: документы и массивы документов в информационных системах: в частности: в банках данных ст?2 Федерального закона Об информации: информатизации и защите информации?

#### Компьютерное право

Термин компьютерное право возник в промышленно развитых странах в середине нашего столетия в связи с широким использованием средств вычислительной техники и других: связанных с ними технических средств: в различных сферах общественной деятельности и частной жизни и формированием отношений: возникающих в процессе производства и применения новых информационных технологий? В самостоятельную отрасль права оно не выделилось ни в одной стране мира и состоит из нормативно-правовых актов разного уровня: относящихся к различным отраслям права % государственному: административному: гражданскому: уголовному и т л? В России аналогичное законодательство чаше всего называется законодательством в сфере информатизации и охватывает: по разным оценкам: от 70 до 500 НПА включая НПА: которыми предусматривается создание отраслевых или специализированные автоматизированных систем: и не включая НПА? регулирующие на общих основаниях хозяйственную деятельность субъектов на рынке новых информационных технологий? **13]**

#### Неправомерный доступ к компьютерной информации

В специальной литературе под неправомерным доступом к компьютерной информации понимается несанкционированное собственником информации ознакомление лица с данными: содержащимися на машинных носителях или в ЭВМ? В? С? Комиссаров: д? ю? н?: профессор: определяет под неправомерным доступом к компьютерной информации получение возможности виновным лицом на ознакомление с информацией или распоряжения ею по своему усмотрению: совершаемое без согласия собственника либо иного уполномоченного лица? Самостоятельной формой неправомерного доступа являются случаи введения в компьютерную систему: сеть или в определенный массив информации без согласия собственника этого массива или иного лица заведомо ложной информации: которая искажает смысл и направленность данного блока информации?**[17]?**

#### Уничтожение информации

*Уничтожение* информации — это приведение ее полностью либо в существенной части в непригодное для использования по назначению состояние?**[17]**

#### Блокирование информации

*Блокирование* информации — это создание недоступности: невозможности ее использования в результате запрещения дальнейшего выполнения последовательности команд либо выключения из работы какого-либо устройства: или выключения реакции какого-либо устройства ЭВМ при сохранении самой информации?**[17]**

#### Модификация информации

Под *модификацией* понимается изменение первоначальной информации без согласия ее собственника или иного законного лица?**[17]**

#### Копирование информации

*Копирование* информации — это снятие копии с оригинальной информации с сохранением ее не поврежденности и возможности использования по назначению?**[17]**

#### Нарушение работы ЭВМ: системы ЭВМ или их сети

*Под нарушением работы ЭВМ: системы ЭВМ или их сети* следует понимать нештатные ситуации: связанные со сбоями в работе оборудования: выдачей неверной информации: отказе в выдаче информации: выходом из строя отключением ЭВМ: элементов системы ЭВМ или их сети и ò?ä? Однако во всех этих случаях обязательным условием является сохранение физической целости ЭВМ: системы ЭВМ или их сети? Если наряду с названными последствиями нарушается и целостность компьютерной системы: как физической веши: то содеянное требует дополнительной квалификации по статьям о преступлениях против собственности?**[17]**

#### Машинные носители

Под машинными носителями следует понимать мобильные устройства накопления информации: обеспечивающие взаимодействие ЭВМ с окружающей средой накопители на гибких и жестких: а также записываемых магнитооптических дисках: стримеры и т? д?? **[17]**

#### Система ЭВМ

Система — это совокупность взаимосвязанных ЭВМ и их обеспечения: предназначенная для повышения эффективности их работы?**[17]**

#### Сеть ЭВМ

Сеть — совокупность распределенных на какой-либо территории и взаимосвязанных для коллективного пользования ими ЭВМ?**[17]**

### Отечественное законодательство в области компьютерного права

Законодательство России в области компьютерного права начало формироваться с конка 1991 года? Оно базируется на нормах Конституции и Гражданского кодекса и включает следующие основные законы: О средствах массовой информации 27?12?91г? ¹2124-1: Патентный закон РФ от 23?09?92г? ¹3517?1? О правовой охране топологий интегральных микросхем от 23?09 92г ¹3526-1: О правовой охране программ для электронных вычислительных машин и баз данных от 23 09?92г? ¹3523-1: О товарных знаках: знаках обслуживания и наименования мест происхождения товаров от 23?09 92ã? ¹3520-1: Основы законодательства об Архивном фонде РФ и архивах от 7 07 93 г ¹5341-1: Об авторском праве и смежных правах? от 90793 г? ¹5351-1: О государственной тайне-от 21?07 93 г? ¹5485-1: Об обязательном экземпляре документов от 29?12 94 Г? №77?-ФЗ: О связи от 1602 95 г? №15-ФЗ: Об информации: информатизации и защите информации от 20 02 95 г? №24-ФЗ? Об участии в международном информационном обмене от 04 07 96 г? ¹ 85-ФЗ? Значительный пласт компьютерного права составляют указы Президента РФ: которые касаются? прежде всего: вопросов формирования государственной политики в сфере информатизации: включая организационные механизмы: создания системы право вой информации и информационно-правового со трудничества с государствами СНГ: обеспечения ин формацией органов государственной власти: мер по защите информации в частности: шифрования?**[13]**

Конституция РФ непосредственно не регулирует отношения в области производства и применения новых информационных технологий: но создает предпосылки для такого регулирования: закрепляя права граждан свободно искать: получать: передавать: производить и распространять информацию любым законным способом ч 4 ст? 29: право граждан на охрану личной тайны ч 1 ст 24 и другие: обязанности государства: в частности: по обеспечению возможности ознакомления гражданина с документами и материалами: непосредственно затрагивающими его права и свободы ч 2 ст 24? Соответствующее законодательство формирует механизмы реализации этих норм?**[1]**

## Уголовно-правовая характеристика главы 28 УК РФ Преступления в сфере компьютерной информации

### Общие признаки преступлений в сфере компьютерной информации

Последствия неправомерного использования информации могут быть самыми разнообразными — это не только нарушение неприкосновенности интеллектуальной собственности: но и 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 IX «Преступления против общественной безопасности и общественного порядка»? Таким образом: если исходить из учения о четырехзвенной структуре объекта преступления: общим объектом **компьютерных** преступлений будет выступать совокупность всех общественных отношений: охраняемых уголовным законом\* родовым — общественная безопасность и общественный порядок\* видовым — совокупность общественных отношений по правомерному и безопасному использованию информации\* 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?**[19]**

Практически все анализируемые преступления относятся к преступлениям средней тяжести: т? е? их максимальная наказуемость в виде лишения свободы не превышает 5 лет? Исключением является лишь создание использование и распространение вредоносных программ для ЭВМ: повлекшее по неосторожности тяжкое последствие: которое наказывается лишением свободы на срок от 3 до 7 лет и поэтому относится к тяжким преступлениям? При характеристике объективной стороны рассматриваемых составов: отмечается: что большинство из них конструктивно сформулированы как материальные: поэтому предполагают не только совершение общественно опасного деяния: но и наступление общественно опасных последствий: а также установление причинной связи между этими двумя признаками? Однако в силу ч? 2 ст? 9 временем совершения каждого из этих преступлений будет признаваться время окончания именно деяния независимо от времени наступления последствий? Сами же общественно опасные деяния чаще всего выступают здесь 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 он: а также время: место: обстановка: орудия: средства совершения преступления могут быть учтены судом в качестве смягчающих или отягчающих обстоятельств?**[19]**

Из всех признаков субъективной стороны значение будет иметь только один — вина? При этом: исходя из ч? 2 ст? 24: для всех преступлений данного вида необходимо наличие вины в форме умысла: и лишь два квалифицированных состава 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? Так: мотивами совершения таких 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 вызовет проблема отграничения неосторожного и невиновного причинения вреда: что связано с повышенной сложностью и скрытностью процессов: происходящих в сетях и системах ЭВМ?**[4]**

Субъект нескольких составов является специальным? В остальных случаях им может стать: в принципе: любой человек: особенно если учесть всевозрастающую компьютерную грамотность населения? Ответственность за преступления против компьютерной безопасности наступает с 16 лет ст? 20 УК? **[2]**

Диспозиции статей 28-й главы описательные: зачастую — бланкетные или отсылочные? Так: для применения ряда их необходимо обратиться к ст? 35 УК: к нормативно-правовому акту об охране компьютерной информации: правилам эксплуатации ЭВМ и т? п? **[2]**

Санкции — альтернативные: за исключением двух квалифицированных составов: где они — в силу тяжести последствий преступления — «урезаны» до относительно-определенных?**[15]**

### Уголовно-правовой анализ ст? 272 гл? 28 УК РФ Неправомерный доступ к компьютерной информации

Эта статья: которая: как и последующие: состоит из 2 частей: содержит достаточно много признаков: обязательных для объекта: объективной и субъективной сторон состава преступления? Непосредственным объектом ее являются общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ: их системы или сети? *Предметом* преступления будет компьютерная машинная информация: содержащаяся на машинном носителе: в ЭВМ: их системе или сети: охраняемая законом: т?е? изъятая из открытого оборота на основании закона: иного нормативного правового акта: а также правил внутреннего распорядка: основанных на названных правовых актах?**[19]**

Состав преступления сформулирован как материальный: причем если деяние в форме действия определено однозначно неправомерный доступ к охраняемой законом компьютерной информации: то последствия хотя и обязательны: могут быть весьма разнообразны: 1 уничтожение информации: 2 ее блокирование: 3 модификация: 4 копирование: 5 нарушение работы ЭВМ: 6 то же — для системы ЭВМ: 7 то же— для их сети? Деяние: как видно из диспозиции статьи: предполагает наличие двух обязательных признаков — информация должна охраняться законом: а доступ к ней должен быть неправомерен: т? е? пользователь ЭВМ не имел права вызывать ее: знакомиться с ней: а тем более распоряжаться ею? Среди способов совершения такого доступа можно назвать: использование чужого имени: изменение физического адреса технического устройства: подбор пароля: нахождение и использование пробелов в программе: любой другой обман системы защиты информации? Вопрос о том: когда окончено данное деяние: должен решаться так? Моментом окончания его является момент отсылки пользователя компьютеру последней интерфейсной команды голосовой: нажатием клавиши вызова хранящейся информации: независимо от наступления дальнейших последствий? Однако преступлением это деяние станет только лишь при наличии последнего условия? Все действия: выполненные до подачи последней команды: будут образовывать состав неоконченного преступления? Что касается преступных последствий: то под уничтожением информации следует понимать такое изменение се состояния: при котором она перестает существовать в силу утраты основных качественных признаков: под блокированием — невозможность доступа к ней со стороны законного пользователя: под модификацией — видоизменение: характеризующееся появлением новых очевидно: нежелательных свойств: под копированием — получение точного или относительно точного воспроизведения оригинала опять-таки без соответствующей санкции: под нарушением работы — остановку действия программы: ее зацикливание: замедление работы: нарушение порядка выполнения команд: ущерб самой аппаратной части и другие последствия? **[19]**

Субъективная сторона основного состава характеризуется виной в форме умысла: прямого или косвенного: лицо должно осознавать общественную опасность своего действия: предвидеть возможность или неизбежность наступления общественно опасных последствий и желать их наступления: либо сознательно допускать их: либо относиться к ним безразлично? Естественно: установление наличия в деянии виновного умысла: а не неосторожности: будет существенно затруднено: хотя бы потому: что при различных состояниях вычислительной системы причем часто неизвестных преступнику одни и те же действия могут приводить к разным последствиям? **[18]**

Субъектом преступления: указанного в ч? 1 ст? 272: может быть любое вменяемое физическое лицо: достигшее 16 лет: кроме: конечно: легального пользователя данной компьютерной информации?**[2]**

Санкция основного состава альтернативно предусматривает три вида наказаний: штраф: исправительные работы и лишение свободы? Первый: в свою очередь: может быть двух видов: кратный минимальному размеру оплаты труда от 200 до 500 и кратный размеру зарплаты или иного дохода осужденного период от 2 до 5 месяцев? Исправительные работы могут быть назначены в размере от 6 месяцев до 1 года: а лишение свободы — от 6 месяцев до 2 лет? Часть 2 ст? 272 предусматривает в качестве квалифицирующих признаков несколько новых: характеризующих объективную сторону и субъект состава? Это совершение деяния: 1 группой лиц по предварительному сговору\* 2 организованной группой\* 3 лицом с использованием своего служебного положения\* 4 лицом: имеющим доступ к ЭВМ: их системе или сети? Если описание первых двух признаков дано в ст? 35 УК: то специальный субъект двух последних можно трактовать как отдельных должностных лиц: программистов: операторов ЭВМ: наладчиков оборудования: специалистов-пользователей автоматизированных рабочих мест и т? д Заметим: однако: что вряд ли оправданно отнесение слов те же действия *—* т? е? неправомерный доступ — к лицам: имеющим доступ к ЭВМ: системе: сети: поскольку их обращение к компьютерной информации: чаще всего: правомерно? Санкция за квалифицированные виды данного преступления ужесточена: в нее введен новый вид наказания арест на срок от 3 до 6 мес?: размеры остальных увеличены: штраф от 500 до 800 минимальных размеров оплаты труда или зарплаты за период от 5 до 8 месяцев\* исправительные работы от 1 года до 2 лет\* лишение свободы до 5 лет?**[19]**

### Уголовно-правовой анализ ст? 273 гл? 28 УК РФ Создание: распространение и использование вредоносных программ для ЭВМ

Статья 273 явилась преемницей ст? 269 проекта УК Создание: использование и распространение вирусных программ? Смена дефиниций произошла от того: что термин “вирусная программа” “компьютерный вирус” понимается в теории программирования несколько в ином значении: более узком? В случае принятия только такого типа программ в качестве средства совершения данного преступления произошло бы неоправданное смещение в понимании такого средства? Во первых: компьютерный вирус может быть безвредным и карать за его внесение при помощи уголовного закона было бы бессмысленным: а во вторых: существует множество программ другого типа: приводящих к столь же нежелательным последствиям: как и в случае действия вредоносных вирусов?**[19]**

Непосредственным объектом данного преступления являются общественные отношения по безопасному использованию ЭВМ: ее программного обеспечения и информационного содержания?

Обязательными признаками объективной стороны ч? 1 ст? 273 будут два: характеризующих способ и средство совершения преступления Это: во-первых: то: что последствия должны быть несанкционированными: во-вторых: наличие самой вредоносной программы или изменения в программе?

*С субъективной стороны* преступление: предусмотренное ч? 1 ст? 273 К: может быть совершено только с прямым умыслом? Виновный сознает: что он создает вредоносную компьютерную программу или вносит соответствующие изменения в существующую: а равно использует либо распространяет такую программу или машинный носитель с ней? Желает этого? Мотив и цель при этом не имеют значения: но могут быть Учтены при назначении наказания? Если же совершение данного преступления происходит с целью совершить другое преступление: например: хищение материальных средств: повреждение или уничтожение компьютерной сети и ò?ä?: то содеянное подлежит квалификации по совокупности ст? 273 и соответствующей статьи УК РФ?**[19]**

 *Субъектом* данного преступления может быть любое лицо: достиг шее 16-летнего возраста?**[2]**

Санкция предусматривает один основной вид наказания лишение свободы на срок до 3 лет и один дополнительный штраф в размере 200—500 минимальных размеров оплаты труда или зарплаты либо иного дохода лица за период 2—5 мес??**[2]** Частью 2 ст? 273 криминализируется более опасное преступление: те же деяния: повлекшие тяжкие последствия? Это — преступление с материальным составом и с двумя формами вины: по отношению к действиям присутствует умысел: а к общественно опасным последствиям — неосторожность: легкомыслие или небрежность?**[19]**

 Санкция данной части — относительно-определенная: лишение свободы на срок от 3 до 7 лет? Таким образом: именно это преступление из всей главы относится к категории тяжких?

Тяжкие последствия — оценочное понятие: наличие их в каждом конкретном случае определяется: исходя из особенностей дела? Так: в данном случае под тяжкими последствиями можно понимать смерть одного или нескольких человек: причинение тяжкого вреда здоровью: катастрофы: серьезную дезорганизацию работы: крупный материальный ущерб и т? п?**[5]**

### Уголовно-правовой анализ ст? 274 гл? 28 УК РФ Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Целью действия ст? 274 должно быть предупреждение невыполнения пользователями своих профессиональных обязанностей: влияющих на сохранность хранимой: и перерабатываемой информации? Непосредственный объект преступления: предусмотренного этой статьей:— отношения по соблюдению правил эксплуатации ЭВМ: системы или их сети: т? е? конкретно аппаратно-технического комплекса? Под таковыми правилами понимаются: во-первых: Общероссийские временные санитарные нормы и правила для работников вычислительных центров: во-вторых: техническая документация на приобретаемые компьютеры: в-третьих: конкретные: принимаемые в определенном учреждении или организации: оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка? Нарушение этих правил несоблюдение: ненадлежащее соблюдение либо прямое нарушение может быть осуществлено путем как активного действия: так и бездействия? Состав ч? 1 сформулирован как материальный? При этом общественно опасные последствия заключаются в одновременном наличии двух факторов: 1 уничтожения: блокирования или модификации охраняемой законом информации ЭВМ\* 2 вызванного этим существенного вреда? Поскольку речь идет о правилах эксплуатации именно ЭВМ: т? е? аппаратно-технической структуры: то и нарушение их должно затрагивать только техническую сторону несоблюдения требований безопасности компьютерной информации: а не организационную или правовую?**[7]**

 С *субъективной стороны* преступление: предусмотренное ч? 1 ст? 274: может быть совершено умышленно — как с прямым: так и с косвенным умыслом? Мотив и цель виновного для квалификации содеянного значения не имеют: но могут быть учтены при назначении наказания?**[8]**

 Субъект данного преступления специальный —лицо: имеющее доступ к ЭВМ: системе ЭВМ или их сети программист: оператор ЭВМ: техник по обслуживанию и т? п??**[8]**

 Санкция ч? 1 ст? 274 состоит из трех альтернативных видов наказания: лишение права занимать определенную должность или заниматься определенной деятельностью на срок до 5 лет: обязательные работы от 180 до 240 часов и ограничение свободы до 2 лет? Часть 2 ñò? 274 — состав с двумя формами вины: предусматривающий в качестве квалифицирующего признака наступление по неосторожности тяжких последствий? Содержание последних: очевидно: аналогично таковому для ч? 2 ст? 273? Санкция нормы существенно отличается от предыдущей: только лишение свободы до 4 лет?**[19]**

# РАССЛЕДОВАНИЕ?

## Понятие: значение и виды предварительного расследования

Расследование предварительное расследование: стадия уголовного процесса: осуществляемая в форме дознания или предварительного следствия? В ходе расследования осуществляется процессуальная деятельность: направленная на выяснение обстоятельств совершения преступления: виновных в нем лиц и т? д??: т? е? на доказывание всех тех фактов и обстоятельств: которые входят в предмет доказывания по делу расследование завершается принятием итогового процессуального решения (прекращение уголовного дела: направление уголовного дела в суд) или приостанавливается по основаниям: указанным в законе **[10]**?

Расследование уголовных дел часто называют предварительным расследованием? Обусловлено это тем: что оно приводит к предварительным выводам и предшествует разбирательству в суде уголовных дел? Предварительное расследование представляет собой деятельность особо уполномоченных государством органов по установлению события преступления: по розыску и изобличению виновного или виновных в совершении преступления: по возмещению причиненного преступлением ущерба и принятию мер по устранению причин совершенного преступления и предупреждению новых [3]?

Стадия предварительного расследования следует непосредственно за стадией возбуждения уголовного дела? Ее содержанием является деятельность органа дознания: следователя и прокурора: направленная на то: чтобы с помощью производства следственных действий по собиранию доказательств быстро и полно раскрыть преступление: всесторонне и объективно установить обстоятельства дела: изобличить виновных в совершении данного преступления: обеспечить привлечение их к уголовной ответственности и подготовить материалы уголовного дела для судебного разбирательства? Кроме этого: по конкретному уголовному делу необходимо выяснить причины и условия: способствовавшие совершению преступления: принять меры к их устранению: а также принять меры к возмещению причиненного преступлением ущерба?**[6]**

Расследование определяется как предварительное потому: что оно осуществляется до судебного разбирательства дела: в ходе которого: как известно: решается вопрос о виновности лица в совершении преступления и назначается наказание за совершенное деяние? Однако в судебном заседании исследуются в основном материалы: собранные на предварительном следствии? Поэтому: для того: чтобы суд имел возможность разрешить уголовное дело и вынести законный: обоснованный и справедливый приговор: орган расследования должен собрать достаточные доказательства: которые могут быть положены в основу приговора? Помимо этого: на предварительном следствии могут быть установлены обстоятельства: дающие основание прекратить уголовное дело?**[6]**

Предварительное расследование проводится по подавляющему большинству дел: направляемых для разбирательства в суд? Особый порядок прохождения уголовных дел предусмотрен лишь по делам частного обвинения (ст? 27 УПК) и по делам с протокольной формой досудебной подготовки материалов (гл? 34 УПК)? Однако и по ним в определенных случаях также может быть проведено предварительное следствие или дознание?

Предварительное расследование по действующему уголовно-процессуальному законодательству происходит в двух формах - предварительное следствие и дознание? Основной формой расследования является предварительное следствие? Это определяется: во-первых: тем: что законодатель относит к этой сфере производство по большинству уголовных дел (ст? 128 УПК): а во-вторых: тем: что предварительное следствие может проводиться и по делам: относимым к компетенции органов дознания: если это признает необходимым суд или прокурор? Осуществление всей этой деятельности возложено на ряд специально уполномоченных органов **[6]**?

## Понятие: и виды следственных действий

Процессуальные действия: совершаемые в ходе дознания и предварительного следствия: именуют следственными действиями? В зависимости от задач: которые решаются при производстве этих действий: их обычно принято подразделять на две относительно самостоятельные группы:

 1? Следственные действия исследовательского характера: посредством которых орган дознания: следователь или прокурор решают задачи: связанные с выявлением: закреплением и исследованием доказательств в предварительном досудебном порядке?

 2? Иные следственные действия: направленные прежде всего на обеспечение прав участвующих в деле лиц ознакомление обвиняемого с постановлением о его привлечении в качестве обвиняемого: разъяснение и обеспечение ему соответствующих прав: ознакомление с соответствующими постановлениями потерпевшего: гражданского истца или гражданского ответчика: разъяснение и обеспечение этим лицам их прав и т?п??

 В настоящей главе речь идет о следственных действиях первой группы?

 Следственными действиями: посредством которых выявляют: закрепляют и исследуют доказательства: являются %

1. допрос свидетеля: потерпевшего: обвиняемого и подозреваемого: а в некоторых случаях также эксперта\*
2. очная ставка\*
3. предъявление для опознания\*
4. обыск\*
5. выемка\*
6. осмотр\*
7. освидетельствование\*
8. следственный эксперимент\*
9. производство экспертизы?

**[6]**

## Следственные действия по делам рассматриваемой категории

### Допрос свидетеля и потерпевшего

Допрос свидетеля и потерпевшего - пожалуй: одно из наиболее распространенных следственных действий? Он является способом получения: закрепления и проверки такого вида доказательств: как показания названных лиц? По внешности допрос имеет определенное сходство с опросом: получением объяснений и интервью? Однако он существенно отличается от них своей правовой природой и прежде всего установленным для него законом процессуальным порядком? Если опросы и подобные им способы получения информации обычно не нуждаются в особых формальностях и правовых гарантиях: то допрос строится таким образом: чтобы порядок его производства по возможности позволял получать в максимальной степени заслуживающие доверия значимые для дела фактические данные и в то же время надежно гарантировал права человека и гражданина: оберегал честь и достоинство допрашиваемого?

 Важнейшим условием ценности показаний любого лица является его правдивость: которая обеспечивается прежде всего добровольностью и моральным долгом дающего показания говорить правду и только правду? Добровольность дачи показаний обеспечивается нашим законодательством ч?3 ст? 20 УПК и ст? 179 УК: запрещающим под страхом уголовной ответственности домогаться показаний путем насилия: угроз и других незаконных мер? Обеспечивается она и моральным долгом граждан не лгать и оказывать содействию правосудию?

 Сам допрос производится по общим правилам: выработанным практикой и закрепленным в действующем законодательстве для данного следственного действия? **[6]**

Допрос свидетелей: потерпевших и подозреваемых необходимо начинать со свободного рассказа о всем: что им известно по делу? Выслушав свободный рассказ: следователь может задать вопросы ст?ст? 158:161 УПК?

 Допрос обвиняемого надо начинать с вопроса - признает ли он себя виновным? Затем обвиняемому предлагается дать показания по существу обвинения?**[22]**

При расследовании неправомерного доступа к компьютерной информации путем допросов разработчиков и пользователей компьютерной системы можно установить: предусмотрены ли в данной компьютерной системе меры защиты от несанкционированного доступа к определенным файлам? Допросами лиц: обслуживающих компьютерную систему: можно установить: кто запускал нештатную программу: было ли это зафиксировано каким-либо способом? Следует также выяснить: кто увлекается программированием: учится или учился на компьютерных курсах??

Когда производится расследование создания: использования и распространения вредоносных программ для ЭВМ то при допросе свидетелей из числа представителей потерпевшей стороны следует выяснить: какая информация подвергалась неправомерному воздействию: ее назначение и содержание\* как осуществляется доступ к ресурсам ЭВМ: системы ЭВМ или их сети: кодам: паролям и другой компьютерной информации\* как организована противовирусная защита\* каким образом ведется учет пользователей компьютерной системы?**[9]?**

При расследовании нарушения правил эксплуатации ЭВМ: системы ЭВМ или их сети: а точнее для установления конкретного правила эксплуатации ЭВМ: нарушение которого привело к вредным последствиям: следователю целесообразно допросить всех лиц: работавших на ЭВМ и обслуживавших компьютерное оборудование в соответствующий период времени? В необходимых случаях к участию в допросе привлекается специалист? Допрашиваемому могут быть поставлены примерно следующие вопросы %

- Каковы Ваши обязанности при работе с ЭВМ либо оборудованием к ней: какими правилами они установлены;

- Какую конкретно работу на ЭВМ и в каком порядке Вы выполняли: когда произошло уничтожение: блокирование: изменение компьютерной информации или наступили иные вредные последствия;

- Какие неполадки в компьютерной системе Вы обнаружили при работе на ЭВМ: не было ли при этом каких-либо сбоев: чреватых причинением существенного вреда компьютерной информации;

- Какие правила работы с компьютером нарушены в данной ситуации;

- Каким образом должны фиксироваться факты уничтожения: блокирования или модификации компьютерной информации в случае нарушения определенных правил эксплуатации ЭВМ;

- Связаны ли уничтожение: блокирование: модификация информации с нарушением правил эксплуатации ЭВМ либо они явились следствием непредвиденных обстоятельств: если связаны: то с нарушением каких правил;

Кроме того: могут быть допрошены в качестве свидетелей администратор сети и специалисты: обслуживающие файловый сервер: в котором произошло уничтожение: блокирование или модификация компьютерной информации?

Им могут быть заданы примерно следующие вопросы:

На какой рабочей станции могли быть нарушены правила эксплуатации компьютерной сети: где она расположена;

Могли ли быть нарушены правила эксплуатации данной локальной вычислительной сети на рабочей станции: расположенной там-то; **[9]**

### Следственный осмотр

Следственный осмотр есть следственное действие: состоящее в непосредственном восприятии и изучении следователем любых объектов в целях исследования обстоятельств деяния: обнаружения: фиксации и изъятия предметов: документов: веществ и следов: которые имеют или могут иметь значение для раскрытия преступления и расследования уголовного дела?

 Уголовно-процессуальный закон: являющийся: как известно: правовой основой следственной практики: в качестве главных процессуально а: следовательно: и криминалистически значимых целей этого следственного действия: относящихся к любому его виду: называет следующее: обнаружение следов преступления и других вещественных доказательств: выяснение обстановки происшествия\* выяснение иных обстоятельств: имеющих для дела ст? 178 УПК?**[23]**

В зависимости от обследуемых объектов существует множество разновидностей осмотра?

Все виды осмотра вправе производить орган дознания: следователь и прокурор? Осмотр местности или помещения в некоторых случаях производит также суд ст? 293 УПК? При осмотре местности или помещения судом участие понятых не требуется? Во всех остальных случаях осмотр производится в присутствии понятых? Для участия в осмотре могут привлекаться обвиняемый: подозреваемый: защитники этих лиц: потерпевший: а также свидетель? В необходимых случаях для участия в осмотре могут привлекаться соответствующие специалисты?

Перед началом осмотра всем приглашенным для участия в нем лицам: в том числе понятым разъясняют их права и обязанности: а специалист предупреждается об ответственности за отказ или уклонение от выполнения своих обязанностей: о чем отмечается в протоколе осмотра и удостоверяется подписью специалиста?

Осмотр условно принято делить на статическую и динамическую стадии? В ходе первой стадии объект обследуется в том виде: в каком он был обнаружен в начале осмотра: а во второй - производится более детальное изучение осматриваемого объекта: в ходе которого отдельные предметы могут перемещаться?

Участвующие в осмотре лица могут обращать внимание того: кто производит данное следственное действие: на необходимость отражения в протоколе тех или иных обстоятельств: имеющих значение? Специалист помогает в обнаружении и закреплении доказательств: а также дает пояснения по поводу отдельных обстоятельств: связанных с их обнаружением?

В ходе осмотра могут производиться соответствующие измерения: фото-: кино- или видео-съемка: могут составляться планы: схемы: изготовляться слепки и оттиски следов? ?

Осмотр предметов и документов: обнаруженных при выемке или обыске: осмотре места происшествия: местности и помещения: может производиться в зависимости от конкретных условий на месте производства соответствующего следственного действия либо после их изъятия отдельно: в ходе самостоятельного их затем осмотра? В первом случае результаты их осмотра отражаются в общем протоколе соответствующего следственного действия? Во втором случае изъятые предметы и документы должны быть упакованы и опечатаны: а затем подробно описаны в протоколе их последующего самостоятельного осмотра ч? 4 ст? 179 УПК? **[6]**

При расследовании неправомерного доступа к компьютерной информации при следственном осмотре компьютера и его компонентов устанавливается причастность конкретного лица к несанкционированному доступу к компьютерной информации могут способствовать различные материально-фиксированные отображения? Это: например: следы пальцев рук: отдельные записи на внешней упаковке дискет: дисков? Для их исследования назначаются криминалистические экспертизы — дактилоскопическая: почерковедческая: технико-криминалистическая? При осмотре изьятого при обыске целесообразно привлекать специалиста: который может: например: прочесть информацию: содержащуюся на машинных носителях: либо в памяти изъятого компьютера?

При расследовании нарушения правил эксплуатации ЭВМ: системы ЭВМ или их сети конкретное место нарушения правил эксплуатации ЭВМ можно установить при осмотре автоматизированных рабочих мест АРМ пользователя компьютерной системы или сети? Осмотру подлежат все подключенные к ним компьютеры? Осмотр проводится обычно с участием специалиста: помогающего установить местонахождение компьютера: работа с которым привела к вредным последствиям в результате преступного нарушения правил его эксплуатации **[9]**

### Обыск и выемка

Особо повышенные требования к гарантиям прав человека: охраны чести и достоинства личности предъявляются при производстве таких следственных действий: которые могут привести к ограничению конституционных прав и свобод? Прежде всего это относится к обыску и выемке: наложению ареста на имущество? В определенной мере они предъявляются также к некоторым разновидностям осмотра например: осмотру жилых помещений и т?п?: освидетельствованию: следственному эксперименту: отдельным видам экспертиз помещение обвиняемого или подозреваемого в медицинское учреждение и др??

Обыском является следственное действие: посредством которого отыскивают и при необходимости изымают объекты орудия преступления: добытые преступным путем предметы и ценности и т?п?: могущие иметь значения для дела? Целью обыска может быть обнаружение разыскиваемых лиц: а также трупов? Для производства обыска требуется достаточно обоснованное предположение: что в каком-либо помещении: ином месте или у кого-либо скрываются объекты: могущие иметь значение для дела?

Выемка отличается от обыска тем: что для ее производства должно быть точно известно: где и у кого подлежащие изъятию объекты находятся ст? 167 УПК?

Решение о производстве обыска и выемки оформляется в виде мотивированного постановления ст?ст? 167 - 168 УПК: которое: как правило ч? 2 ст? 167 и ч? 3 ст? 168 УПК: требует санкции прокурора? Разрешение на производство обыска: связанного с проникновением в жилище против воли проживающих в нем лиц: может быть получено и у суда ст? 25 Конституции РФ?

Вместе с тем: при некоторых разновидностях обыска допускаются и более простые решения? В случаях: не терпящих отлагательства: обыск может быть произведен без санкции прокурора: но с последующим сообщением прокурору в суточный срок ч? 3 ст? 168 УПК? Личный обыск без вынесения о том отдельного постановления и без санкции прокурора допускается:

а при задержании или заключении лица под стражу\* и

б при наличии достаточных оснований полагать что лицо: находящееся в помещении или ином месте: в котором производится выемка или обыск: скрывает при себе предметы и документы: могущие иметь значение для дела ст? 172 УПК?

При этом личный обыск должен производиться только лицом одного пола с обыскиваемым и в присутствии понятых того же пола?

Порядок производства обыска и выемки детально регламентирован законом ст? 170 УПК? Производство этих действий не допускается в ночное время: кроме случаев: не терпящих отлагательства? Приступая к совершению этих действий: полномочное производить их должностное лицо следователь: лицо: производящее дознание или прокурор обязано предъявить постановление об этом? При осуществлении данных действий требуется присутствие понятых? В необходимых случаях приглашаются и соответствующие специалисты? **[6]**

При расследовании неправомерного доступа к компьютерной информации у лиц: заподозренных в неправомерном доступе к компьютерной информации: при наличии достаточных оснований производится обыск: при котором могут быть обнаружены: компьютеры разных конфигураций: принтеры: средства телекоммуникационной связи с компьютерными сетями: записные книжки с уличающими записями: в том числе электронные: дискеты: диски: магнитные ленты: содержащие сведения: могущие иметь значение для дела: в том числе коды: пароли: идентификационные номера пользователей конкретной компьютерной системы: а также данные о ее пользователях? В ходе обыска следует обращать внимание на литературу: методические материалы по компьютерной технике и программированию?

К производству обыска и последующего осмотра изъятого при обыске целесообразно привлекать специалиста: который может: например: прочесть информацию: содержащуюся на машинных носителях либо в памяти изъятого компьютера? [**9**]

При расследовании создания: использования и распространения вредоносных программ для ЭВМ установлению факта создания вредоносной программы способствует выявление фактов ее использования и распространения и особенно получение данных: позволяющих заподозрить то или иное лицо в соответствующей деятельности? Этому может способствовать своевременно и тщательно произведенный обыск по месту работы и месту жительства подозреваемого: а также в местах: где он мог иметь доступ к компьютерной системе? К участию в обыске целесообразно привлечь специалиста-программиста: стремясь обнаружить все: что может иметь отношение к созданию вредоносной программы? **[9]**

### Назначение и производство экспертизы

Судебная экспертиза - это процессуальное действие: проводимое в целях получения заключения по вопросам: имеющим доказательственное значение по делу? Лицо: обладающее специальными полномочиями и назначенное в соответствии с постановлением следователя для дачи такого заключения: именуется экспертом?

 Судебные экспертизы выполняются в специализированных экспертных учреждениях: относящихся к системе министерства юстиции: внутренних дел: здравоохранения: обороны: службы контрразведки Российской Федерации?**[24]**

Назначение любого вида экспертизы оформляется постановлением следователя? В нем обязательно должны содержаться: мотивировка необходимости этого следственного действия: сведения об эксперте или экспертном учреждении: вопросы: на которые должен дать эксперт: а также описание материалов: предоставляемых для исследования ст? 184 УПК?

С постановлением обязательно знакомят обвиняемого: которому даны достаточно широкие права: заявить отвод эксперту: просить о назначении эксперта из числа указанных им лиц: представить дополнительные вопросы эксперту для получения по ним заключения: присутствовать с разрешения следователя при производстве экспертизы и давать объяснения эксперту: знакомиться с его заключением до окончания расследования? При отказе в удовлетворении ходатайства обвиняемого должно быть вынесено мотивированное постановление? Если же оно удовлетворяется: то должно быть составлено новое постановление о назначении экспертизы? **[6]**

По делам данной категории расследование неправомерного доступа к компьютерной информации путем производства информационно-технической судебной экспертизы может быть установлен способ несанкционированного доступа? Перед экспертом следует поставить вопрос % Каким способом мог быть совершен несанкционированный доступ в данную компьютерную систему;? Целесообразно представить эксперту всю проектную документацию на исследуемую систему если таковая имеется: а также имеющиеся данные о ее сертификации?

При производстве такой экспертизы рекомендуется использовать компьютерное оборудование той же системы: в которую проник преступник: либо специальные технические и программные средства? **[9]**

По делам рассматриваемой категории расследовании нарушения правил эксплуатации ЭВМ: системы ЭВМ или их сети по результатам информационно-технической судебной экспертизы может быть установлено место нарушения правил? Перед экспертами могут быть поставлены вопросы:

1? На какой рабочей станции локальной вычислительной сети могли быть нарушены правила ее эксплуатации: в результате чего наступили вредные последствия;

2? Могли ли быть нарушены правила эксплуатации сети на рабочей станции: расположенной там-то;

###  Следственный эксперимент

Следственный эксперимент представляет собой познавательный прием: посредством которого путем воспроизведения действий: обстановки или иных обстоятельств определенного события или явления и совершения необходимых опытных действий: в контролируемых и управляемых условиях исследуются эти события или явления? Такой прием с давних пор применяют и при исследовании каких-либо обстоятельств преступного события в ходе расследования: а также судебного разбирательства уголовных дел?

Действующим УПК для производства следственного эксперимента предусмотрены специальные правила ст? 183 Его вправе производить следователь или прокурор: а также орган дознания по делам о преступлениях: по которым предварительное следствие не обязательно? Известны случаи: когда интересные и убедительные эксперименты подобного рода проводились и в суде?

Если эксперимент проводится в ходе предварительного следствия или дознания: то для этого приглашаются понятые? При необходимости могут приглашаться соответствующие специалисты?

Суть самого следственного эксперимента: как сказано в законе ст?183 УПК: заключается в воспроизведении действий: обстановки или иных обстоятельств определенного события и совершения необходимых опытных действий в целях проверки и уточнения данных: имеющих значение для дела? Посредством такого рода действий обычно проверяют возможность видеть: слышать определенные: значимые для дела обстоятельства в тех или иных условиях: возможность совершения определенных действий и получения определенных результатов при наличии конкретных условий и т?п?

При производстве следственного эксперимента в необходимых случаях могут участвовать обвиняемый или подозреваемый: защитники этих лиц: а также потерпевший и свидетель?

Производство следственного эксперимента допускается при условии: если при этом не унижается достоинство и честь участвующих в нем лиц и окружающих и не создается опасности для их здоровья?

Ход и результаты производства следственного эксперимента описываются в протоколе с соблюдением требований статей 141 и 142 УПК? Если при производстве следственного эксперимента производились какие-либо измерения или применялись технические средства: то все это должно найти отражение в протоколе? **[6]**

Следственный эксперимент по делам данной категории преступления в сфере компьютерной информации производится с целью проверки возможности преодоления средств защиты компьютерной системы одним из предполагаемых способов? Его целью может стать и проверка возможности появления на экране дисплея закрытой информации или ее распечатка вследствие ошибочных: неумышленных действий оператора или в результате случайного технического сбоя в компьютерном оборудовании:

Для установления возможности создания вредоносной программы определенным лицом: сознавшимся в этом: проводится следственный эксперимент с использованием соответствующих средств компьютерной техники расследование создания: использования и распространения вредоносных программ для ЭВМ?

При проведении следственного эксперимента выясняется возможность наступления вредных последствий при нарушении определенных правил? Он проводится с использованием копий исследуемой информации и по возможности на той же ЭВМ: при работе на которой нарушены правила расследование нарушения правил эксплуатации ЭВМ: системы ЭВМ или их сети?

### Допрос обвиняемого и подозреваемого

Закон ст? 150 УПК предписывает приступить к допросу обвиняемого сразу же после предъявления обвинения и разъяснения его прав? Допрос собственно и является прежде всего способом обеспечения одного из важнейших прав обвиняемого - давать объяснения по предъявленному обвинению в интересах собственной защиты ст? 46 УПК? Он в меньшей мере необходим и следователю: для которого служит способом получения доказательства - показаний обвиняемого и тем самым одним из важных способов проверки правильности сформулированной по делу версии обвинения? Допрос обвиняемого является также одним из средств: с помощью которого его изобличают в совершении преступления?

Следует: однако: иметь в виду: что дача показаний для обвиняемого - это его право: а не обязанность? Поэтому обвиняемого: в отличие от свидетеля и потерпевшего: нельзя перед допросом: а также в ходе допроса предупреждать об уголовной или какой-либо иной например: административной и т?п? ответственности за отказ от дачи показаний: равно как и за дачу ложных показаний?

По смыслу ст? 51 Конституции РФ обвиняемый и подозреваемый вообще вправе отказаться от дачи показаний и не отвечать ни на какие вопросы либо отвечать на них сугубо добровольно? Потому при возникновении у суда сомнений относительно добровольности данных этими лицами показаний в ходе предварительного следствия или дознания обязанность доказывания: что показания действительно были даны добровольно: следовало бы возлагать на органы уголовного преследования: получившие такие показания?

О каждом допросе обвиняемого составляется протокол с соблюдением требований: предусмотренных ст? ст? 141: 142 и 151 УПК? После дачи обвиняемым показаний: в случае его просьбы: ему предоставляется возможность изложить свои показания собственноручно (ст? 152 УПК) **[6]**

Обычно по уголовным делам рассматриваемой категории расследование создания: использования и распространения вредоносных программ для ЭВМ при допросе обвиняемого необходимо выяснить обстоятельства подготовки и совершения преступления: алгоритм функционирования вредоносной программы: а также на какую информацию и как она воздействует?

По делам данной категории при допросе подозреваемого требуется установить уровень его профессиональной подготовленности как программиста: опыт его работы по созданию программы конкретного класса на данном языке программирования: знание им алгоритмов работы про грамм: подвергшихся неправомерному воздействию?

Также необходимо выяснить допрос подозреваемого% места его жительства: работы или учебы: профессию: взаимоотношения с сослуживцами: семейное положение: образ жизни: сферу интересов: привычки: наклонности: круг знакомых: навыки в программировании: ремонте и эксплуатации средств вычислительной техники: какими средствами вычислительной техники: машинными носителями: аппаратурой и приспособлениями он располагал: где: на какие средства их приобрел и где хранил? **[6]**

# РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ?

## Расследование неправомерного доступа к компьютерной информации

Согласно ст? 272 УК ответственность за деяние наступает при условии: если неправомерный доступ к компьютерной информации повлек за собой хотя бы одно из следующих негативных последствий: уничтожение: блокирование: модификацию либо копирование информации: нарушение работы ЭВМ: системы ЭВМ или их сети?

### Общая схема расследования неправомерного доступа к компьютерной информации?

В ходе расследования основные следственные задачи целесообразно решать в такой последовательности:

1? Установление факта неправомерного доступа к информации в компьютерной системе или сети?

2? Установление места несанкционированного проникновения в компьютерную систему или сеть?

3? Установление времени совершения преступления?

4? Установление надежности средств защиты компьютерной информации?

5? Установление способа несанкционированного доступа?

6? Установление лиц: совершивших неправомерный доступ: их виновности и мотивов преступления?

7? Установление вредных последствий преступления?

8? Выявление обстоятельств: способствовавших преступлению?

**Установление факта неправомерного доступа к информации** в компьютерной системе или сети? Такой факт : как правило: первыми обнаруживают пользователи автоматизированной информационной системы: ставшие жертвой данного правонарушения?

Факты неправомерного доступа к компьютерной информации иногда устанавливаются в результате оперативно-розыскной деятельности органов внутренних дел: ФСБ: налоговой полиции? Установить их можно в ходе прокурорских проверок: при проведении ревизий: судебных экспертиз: следственных действий по уголовным делам? Рекомендуется в необходимых случаях при рассмотрении материалов: связанных с обработкой информации в компьютерной системе или сети: установление фактов неправомерного доступа к ним поручать ревизорам и оперативно-розыскным аппаратам?'

На признаки несанкционированного доступа или подготовки к нему могут указывать следующие обстоятельства:

появление в компьютере фальшивых данных\*

необновление в течение длительного времени в автоматизированной информационной системе кодов: паролей и других защитных средств\*

частые сбои в процессе работы компьютеров\*

участившиеся жалобы клиентов компьютерной системы Или сети\*

осуществление сверхурочных работ без видимых на то причин\*

немотивированные отказы некоторых сотрудников: обслуживающих компьютерные системы или сети: от отпусков\*

неожиданное приобретение сотрудником домашнего дорогостоящего компьютера\*

чистые дискеты либо диски: принесенные на работу сотрудниками компьютерной системы под сомнительным предлогом перезаписи программ для компьютерных игр\*

участившиеся случаи перезаписи отдельных данных без серьезных на то причин\*

чрезмерный интерес отдельных сотрудников к содержанию чужих распечаток листингов: выходящих из принтеров?

Особо следует выделить признаки неправомерного доступа: относящиеся к отступлению от установленного порядка работы с документами: а именно:

а нарушение установленных правил оформления документов: в том числе изготовления машинограмм\*

6 повторный ввод одной и той же информации в ЭВМ\*

в наличие в пачке лишних документов: подготовленных для обработки на компьютере\*

г отсутствие документов: послуживших основанием для записи во вторичной документации\*

д преднамеренная утрата: уничтожение первичных документов и машинных носителей информации: внесение искажений в данные их регистрации?

Для фактов неправомерного доступа к компьютерной информации характерны также следующие признаки: относящиеся к внесению ложных сведений в документы:

а противоречия логические или арифметические между реквизитами того или иного бухгалтерского документа\*

б несоответствие данных: содержащихся в первичных документах: данным машинограмм\*

в противоречия между одноименными бухгалтерскими документами: относящимися к разным периодам времени\*

г несоответствие учетных данных взаимосвязанных показателей в различных машинограммах\*

д несоответствие между данными бухгалтерского и другого вида учета?

Следует иметь в виду: что указанные признаки могут быть следствием не только злоупотребления: но и других причин: в частности случайных ошибок и сбоев компьютерной техники?

**Установление места несанкционированного доступа в компьютерную систему или сеть?** Решение данной задачи вызывает определенные трудности: так как таких мест может быть несколько?

Чаше обнаруживается место неправомерного доступа к компьютерной информации с целью хищения денежных средств?

При обнаружении факта неправомерного доступа к информации в компьютерной системе или сети следует выявить все места: где расположены компьютеры: имеющие единую телекоммуникационную связь?

Проще рассматриваемая задача решается в случае несанкционированного доступа к отдельному компьютеру: находящемуся в одном помещении? Однако при этом необходимо учитывать: что информация на машинных носителях может находиться в другом помещении: которое тоже надо устанавливать?

Труднее определить место непосредственного применения технических средств удаленного несанкционированного доступа не входящих в данную компьютерную систему или сеть? К установлению такого места необходимо привлекать специалистов?

Установлению подлежит и место хранения информации на машинных носителях либо в виде распечаток: добытых в результате неправомерного доступа к компьютерной системе или сети?

**Установление времени несанкционированного доступа?** С помощью программ общесистемного назначения в работающем компьютере обычно устанавливается текущее время: что позволяет по соответствующей команде вывести на экран дисплея информацию о дне недели: выполнения той или иной операции: часе и минуте? Если эти данные введены: то при входе в систему или сеть в том числе и несанкционированном время работы на компьютере любого пользователя и время конкретной операции автоматически фиксируются в его оперативной памяти и отражаются: как правило: в выходных данных на дисплее: листинге или на дискете?

С учетом этого время несанкционированного доступа можно установить путем следственного осмотра компьютера либо распечаток или дискет? Его целесообразно производить с участием специалиста: так как неопытный следователь может случайно уничтожить информацию: находящуюся в оперативной памяти компьютера или на дискете?

Время неправомерного доступа к компьютерной информации можно установить также путем допроса свидетелей из числа сотрудников данной компьютерной системы: выясняя у них: в какое время каждый из них работал на компьютере: если оно не было зафиксировано автоматически? **[9]**

**Установление способа несанкционированного доступа?** В ходе установления способа несанкционированного доступа к компьютерной информации следствие может вестись по трем не взаимоисключающим друг друга вариантам:

Допросом свидетелей из числа лиц: обслуживающих компьютер: компьютерную систему или сеть системный администратор: операторы: разработчиков системы и: как правило: поставщиков технического и программного обеспечения? В данном случае необходимо выяснить: каким образом преступник мог преодолеть средства защиты данной системы: в частности: узнать идентификационный номер законного пользователя\* код\* пароль для доступа к ней\* получить сведения о других средствах защиты?

 Производством судебной информационно-технической экспертизы? В ходе экспертизы выясняются возможные способы проникнуть в систему при той технической и программной конфигурации системы в которую проник преступник: с учетом возможного использования последним специальных технических и программных средств? При производстве судебной: информационно-технической экспертизы целесообразно поставить эксперту следующий вопрос: Каким способом мог быть совершен несанкционированный доступ в данную компьютерную систему

Проведением следственного эксперимента: в ходе которого проверяется возможность несанкционированного доступа к информации одним из предполагаемых способов?

**Установление надежности средств защиты компьютерной информации?** Прежде всего необходимо установить: предусмотрены ли в данной компьютерной системе меры защиты от несанкционированного доступа к определенным файлам? Это можно выяснить путем допросов ее разработчиков и пользователей: а также изучением проектной документации: соответствующих инструкций по эксплуатации данной системы? При ознакомлении с инструкциями особое внимание должно уделяться разделам о мерах защиты информации: порядке допуска пользователей к определенным данным: разграничении их полномочий: организации контроля за доступом: конкретных методах защиты информации аппаратных: программных: криптографических: организационных и других?

Надо иметь в виду: что в целях обеспечения высокой степени надежности информационных систем: в которых обрабатывается документированная информация с ограниченным доступом: осуществляется комплекс мер: направленных на их безопасность?

В частности: законодательством предусмотрены обязательная сертификация средств защиты этих систем и обязательное лицензирование всех видов деятельности в области проектирования и производства таких средств? Разработчики: как правило: гарантируют надежность своих средств при условии: если будут соблюдены установленные требования к ним? Поэтому в процессе расследования требуется установить: во-первых: имеется ли лицензия на производство средств защиты информации от несанкционированного доступа: используемых в данной компьютерной системе: и: во-вторых: соответствуют ли их параметры выданному сертификату? Для проверки такого соответствия может быть назначена информационно-техническая экспертиза с целью решения вопроса % «Соответствуют ли средства защиты информации от несанкционированного допуска: используемые в данной компьютерной системе: выданному сертификату;»

Вина за выявленные при этом отклонения: ставшие причиной несанкционированного доступа к компьютерной информации: возлагается на пользователя системы: а не на разработчика средств защиты?

**Установление лиц: совершивших неправомерный доступ к компьютерной информации?**

Опубликованные в прессе результаты исследований: проведенных специалистами: позволяют составить примерный социологический портрет современного хакера? Возраст правонарушителей колеблется в широких границах —от 15 до 45 лет: причем на момент совершения преступления у трети возраст не превышал 20 лет? Свыше 80 преступников в компьютерной сфере — мужчины: абсолютное большинство которых имело высшее и среднее специальное образование? При этом у более 50 преступников была специальная подготовка в области автоматизированной обработки информации: а 30 — были непосредственно связаны с эксплуатацией ЭВМ и разработкой программного обеспечения к ней? Однако: согласно статистики: профессиональными программистами из каждой тысячи компьютерных преступлений совершено только семь? 38 отечественных хакеров действовали без соучастников: 62 — в составе преступных групп По оценкам специалистов основная опасность базам данных исходит от внутренних пользователей ими совершается 94 преступлений: а внешними — только 6?**[21]**

Данные вышеприведенного статистического анализа показывают: что несанкционированный доступ к ЭВМ: системы ЭВМ или их сети совершают специалисты с достаточно высокой степенью квалификации в области информационных технологий? Поэтому поиск подозреваемого следует начинать с технического персонала пострадавших компьютерных систем или сетей разработчиков соответствующих систем: их руководителей: операторов: программистов: инженеров связи: специалистов по защите информации и других?

Следственная практика показывает: что чем сложнее в техническом отношении способ проникновения в компьютерную систему или сеть: тем легче выделить подозреваемого: поскольку круг специалистов: обладающих соответствующими способностями: обычно весьма ограничен?

При выявлении лиц: причастных к совершению преступления: необходим комплекс следственных действий: включающий в себя следственный осмотр компьютера системы ЭВМ и ее компонентов: допрос лиц: обязанных обеспечивать соблюдение доступа к компьютерной системе или сети: обыск у лиц: заподозренных в неправомерном доступе к компьютерной информации: при наличии к тому достаточных оснований изложенных ранее в главе расследование?

**Установление виновности и мотивов лиц: совершивших неправомерный доступ к компьютерной информации?** Установить виновность и мотивы несанкционированного доступа к компьютерной информации можно только по совокупности результатов всех процессуальных действий? Решающими из них являются показания свидетелей: подозреваемых: обвиняемых: потерпевших: заключения судебных экспертиз: главным образом информационно-технологических и информационно-технических: а также результаты обыска? В процессе расследования выясняется: во-первых: с какой целью совершен несанкционированный доступ к компьютерной информации\* во-вторых: знал ли правонарушитель о системе ее защиты\* в-третьих: желал ли он преодолеть эту систему и: в-четвертых: если желал: то по каким мотивам и какие действия для этого совершил?

Установление вредных последствий неправомерного доступа к компьютерной системе или сети? Прежде всего необходимо установить: в чем заключаются вредные последствия такого доступа хищение денежных средств или материальных ценностей: завладение компьютерными программами: информацией путем изъятия машинных носителей либо копирования: а также незаконное изменение: уничтожение: блокирование информации или выведение из строя компьютерного оборудования: введение в компьютерную систему заведомо ложной информации или компьютерного вируса и т?д??

Хищение денежных средств чаще совершается в банковских электронных системах путем несанкционированного доступа к их информационным ресурсам: внесения в них изменений и дополнений? Обычно такие правонарушения обнаруживаются самими работниками банков? Устанавливаются они и в результате проведения оперативно-розыскных мероприятий? Сумма хищения устанавливается судебно-бухгалтерской экспертизой?

Факты неправомерного завладения компьютерными программами вследствие несанкционированного доступа к той или иной системе и их незаконного использования выявляются: как правило: потерпевшими?

Наибольший вред приносит незаконное получение информации из различных компьютерных систем: ее копирование: размножение с целью продажи и получения материальной выгоды либо использования в других преступных целях например: для сбора компроматов на кандидатов в депутаты различных представительных органов власти?

Похищенные программы и информационные базы данных могут быть обнаружены путем производства обысков у обвиняемых: а также при проведении оперативно-розыскных мероприятий? Так: сотрудниками санкт-петербургской милиции было проведено несколько операций: в ходе которых выявлены многочисленные факты распространения копий разнообразных компьютерных программ: добытых в результате несанкционированного доступа к компьютерным системам: вследствие чего некоторым фирмам - производителям программ причинен крупный материальный ущерб?

Если незаконно приобретенная информация относится к категории конфиденциальной или государственной тайны: то конкретный вред: причиненный разглашением: устанавливается представителями Гостехкомиссии РФ?

Факты незаконного изменения: уничтожения: блокирования информации: выведения из строя компьютерного оборудования: введения в компьютерную систему заведомо ложной информации устанавливаются прежде всего самими пользователями информационной системы или сети?

Следует иметь в виду: что не все эти последствия наступают в результате умышленных действий? Нередко их причиной становится случайный сбой в работе компьютерного оборудования?

По имеющимся сведениям: серьезные сбои в работе сетевого оборудования и программного обеспечения в большинстве российских фирм происходят не реже одного раза в месяц'?

При определении размера вреда: причиненного несанкционированным доступом: учитываются не только прямые затраты на ликвидацию его последствий: но и упущенная выгода негативные последствия неправомерного доступа к компьютерной информации могут устанавливаться в процессе следственного осмотра компьютерного оборудования и носителей информации анализа баз и банков данных: допросов технического персонала: владельцев информационных ресурсов? Вид и размер ущерба устанавливаются обычно посредством комплексной экспертизы: проводимой с применением специальных познаний в области информатизации: средств вычислительной техники и связи: экономики: финансовой деятельности и товароведения?

**Выявление обстоятельств: способствовавших неправомерному доступу к компьютерной информации?** На заключительном этапе расследования формируется целостное представление об обстоятельствах: способствовавших несанкционированному доступу к компьютерной информации? В данном аспекте важно последовательное изучение различных документов: главным образом относящихся к защите информации? Особое значение при этом могут иметь материалы ведомственного служебного расследования?

Вопросы о способствовавших рассматриваемому преступлению обстоятельствах целесообразно ставить при информационно-технологической и информационно-технической судебных экспертизах? Соответствующие обстоятельства могут устанавливаться также благодаря допросам технического персонала: очным ставкам: следственным экспериментам: осмотрам документов?

Эти обстоятельства состоят главным образом в следующем %

1 **Неэффективность методов защиты компьютерной информации от несанкционированного доступа:** что в значительной мере относится к компьютерным сетям?

2 **Совмещение функций разработки и эксплуатации программного обеспечения** в рамках одного структурного подразделения? Разработчики компьютерной программы нередко сами участвуют в ее промышленной эксплуатации? Они имеют возможность вносить в нее разные изменения: осуществлять доступ к любой информации: в том числе закрытой? Являясь авторами средств защиты и их эксплуатационниками: они подобны главному бухгалтеру: выполняющему также функции кассира?

3 **Неприменение в технологическом процессе всех имеющихся средств и процедур регистрации и протоколирования операций: действий программ и обслуживающего персонала?**

4 **Нарушение сроков изменения паролей пользователей?**

5 **Нарушение установленных сроков хранения копий программ и компьютерной информации либо отсутствие их?**

На допросах лица: обвиняемого в неправомерном доступе

 к компьютерной информации: уточняются и дополняются ранее полученные данные?

### Способы краж в банковских информационно-вычислительных системах

Ввиду существенного финансового ущерба: причиняемого компьютерными преступлениями в данной сфере экономики: целесообразно остановиться на способах краж в банковских информационно-вычислительных системах подробнее?

Под способом краж в информационных системах кредитно-финансовых структур понимают совокупность приемов и средств: обеспечивших несанкционированный доступ к банковским информационным ресурсам и технологиям: которые позволяют совершить модификацию хранимой информации с целью нарушения отношений собственности: выразившегося в противоправном изъятии денежных средств или обращении их в пользу других лиц?**[12]**

Известные на сегодня способы отличаются значительным и постоянно расширяющимся разнообразием?

По своей криминалистической сущности такого рода умышленные действия являются преступлением с четко выраженными этапами развития? Они отличаются друг от друга по характеру действий и степени завершенности криминального деяния? Такое деление на стадии необходимо для правильной правовой оценки? Применяя ст?29 УК: можно выделить следующие три этапа?**[2]**

**Приготовление к преступлению**

Поиск: покупка: получение на время или хищение орудий деяния компьютера: модема и пр?: написание специальной программы: позволяющей преодолеть защиту банковских сетей изготовление и приспособление средств совершения преступления: сбор информации о клиентах банка: системе защиты СЗ: подбор паролей: преодоление СЗ от несанкционированного доступа к данным и компьютерной информации умышленное создание условий для совершения преступления?

**Покушение на преступление**

Производится путем манипуляции данными: хранимыми в памяти банковской информационной системы: и ее управляющими программами для несанкционированного движения денежных средств в пользу злоумышленника или третьего лица?

**Окончание преступления** Заключительная стадия: когда все несанкционированные транзакции завершены и злоумышленник имеет возможность воспользоваться плодами своего деяния?**[12]**

Перечень и распределение по стадиям известных в настоящее время основных приемов и средств совершения преступления приведены в приложении 1?

Вот более подробно некоторые приемы: применяемые в компьютерных преступлениях?

**Изъятие средств вычислительной техники СВТ** производится с целью получения системных блоков: отдельных винчестеров или других носителей информации: содержащих в памяти установочные данные о клиентах: вкладчиках: кредиторах банка и т?д? Такие действия проводятся путем хищения: разбоя: вымогательства и сами по себе содержат состав обычных некомпьютерных преступлений? Они квалифицируются по ст? 158: 161: 162: 163 УК России?

**Перехват негласное получение информации** также служит для снятия определенных сведений с помощью методов и аппаратуры аудио-: визуального и электромагнитного наблюдения? Объектами: как правило: являются каналы связи: телекоммуникационное оборудование: служебные помещения для проведения конфиденциальных переговоров: бумажные и магнитные носители в том числе и технологические отходы? Это компетенция ст? 138: 183

**Несанкционированный доступ НСД** к средствам вычислительный техники? Это активные действия по созданию по созданию возможности распоряжаться информацией без согласия собственника? Они могут быть квалифицированы с использование ст?183: 272 УК? НСД обычно реализуется с использованием следующих основных приемов:

1. за дураком — физическое проникновение в производственные помещения? Злоумышленник ожидает у закрытого помещения: держа в руках предметы: связанные с работой на компьютерной технике элементы маскировки: пока не появится кто-либо: имеющий легальный доступ к СВТ: затем остается только войти внутрь вместе с ним или попросить его помочь занести якобы необходимые для работы на компьютере предметы? Другой вариант — электронное проникновение в СВТ — подключение дополнительного компьютерного терминала к каналам связи с использованием шлейфа шнурка в тот момент времени: когда законный пользователь кратковременно покидает свое рабочее место: оставляя свой терминал или персональный компьютер в активном режиме\*
2. за хвост - злоумышленник подключается к линии связи законного пользователя и дожи дается сигнала: обозначающего конец работы: перехватывает его на себя: а потом: когда законный пользователь заканчивает активный режим: осуществляет доступ к банковской системе? Подобными свойствами обладают телефонные аппараты с функцией удержания номера: вызываемого абонентом\*
3. компьютерный абордаж - злоумышленник вручную или с использованием автоматической программы подбирает код пароль доступа к банковской системе с использованием обычного телефонного аппарата\*
4. неспешный выбор - преступник изучает и исследует систему защиты от НСД: ее слабые места: выявляет участки: имеющие ошибки или неудачную логику программного строения: разрывы программ брешь: люк и вводит дополнительные команды: разрешающие доступ\*
5. маскарад - злоумышленник проникает в банковскую компьютерную систему: выдавая себя за законного пользователя с применением его кодов паролей и других идентифицирующих шифров\*
6. мистификация - злоумышленник создает условия: когда законный пользователь осуществляет связь с нелегальным терминалом? будучи абсолютно уверенным в том: что он работает с нужным ему законным абонентом? Формируя правдоподобные ответы на запросы законного пользователя и поддерживая его заблуждения некоторое время: злоумышленник добывает коды (пароли) доступа или отклик на пароль\*
7. аварийный — злоумышленник создает условия для возникновения сбоев или других отклонений в работе СВТ? При этом включается особая программа: позволяющая в аварийном режиме получать доступ к наиболее ценным данным? В этом режиме возможно «отключение» всех имеющихся в банковской компьютерной системе средств защиты ин формации?

**Асинхронная атака** является одним из приемов подготовительного этапа к совершению преступления? Преступник: используя асинхронную природу операционной системы: заставляет работать банковскую компьютерную систему в ложных условиях: из-за чего управление обработкой частично или полностью нарушается? Данная ситуация используется для внесения изменений в операционную систему: причем эти изменения не будут заметны (ст? 272 УК РФ)?

**Моделирование** - это наиболее сложный и трудоемкий прием подготовки к совершению преступления? Злоумышленник строит модель поведения банковской компьютерной системы в различных условиях и на основе изучения организации движения денежных средств оптимизирует способ манипуляции данными? Например: в нескольких сторонних банках открываются счета на незначительные суммы: моделируется ситуация: при которой деньги переводятся из одного банка в другой и обратно с постепенным увеличением сумм? В ходе анализа выявляются условия: при которых: а в банке обнаружится: что поручение о переводе не обеспечено необходимой суммой\* б когда в банк необходимо прислать извещение из другого банка о том: что общая сумма покрывает требование о первом переводе\* в устанавливается: сколько циклов это нужно повторять: чтобы на затребованном счете оказалась достаточная сумма и число платежных поручений не казалось подозрительным?

**Подмена данных** используется непосредственно для обращения денежных сумм в свою пользу и представляет собой способ модификации сведений: при котором злоумышленником изменяются или вводятся новые данные как правило: на этапе ввода-вывода информации для приписывания банковскому счету чужой истории? Здесь просматривается состав преступления: определенный ст? 272 УК РФ?

**Троянский конь** матрешка: червь: бомба также служит непосредственно для обращения чужих денег в свою пользу? Это такая манипуляция: при которой злоумышленник тайно вводит в прикладное программное обеспечение специальные модули: обеспечивающие отчисление на заранее открытый подставной счет определенных сумм с каждой банковской операции или увеличение суммы на этом счете при автоматическом пересчете рублевых остатков: связанных с переходом к коммерческому курсу соответствующей валюты? Здесь применимы ст? 273 и 158?

**«Салями»** - оригинальная электронная версия методов изъятия «лишних» денежных средств в свою пользу? При использовании этого метода злоумышленник так же: как и в предыдущем случае: «дописывает» прикладное программное обеспечение специальным модулем: который манипулирует с информацией? перебрасывая на подставной счет результаты округления при проведении законных транзакций? Расчет построен на том: что отчисляемые суммы столь малы: что их потери практически незаметны: а незаконное накопление средств проводится за счет суммы совершения большого количества операций (ст? 272? 273: 158 УК РФ)?

 **Сокрытие следов** Особое место занимают методы: которые применяются злоумышленником для сокрытия следов преступления? Эти действия вряд ли можно квалифицировать по статьям Уголовного кодекса: однако они направлены на то: чтобы преступник смог воспользоваться плодами своего неблагородного труда? Эти методы важны при оценке завершенности совершенного преступления? Одним из таких методов является **дробление денежных сумм —** злоумышленник делит полученные в результате несанкционированных манипуляций с банковской информацией денежные средства на неравные долевые части с зачислением на корреспондентские счета сторонних банков: в которых можно было бы впоследствии снять переведенные суммы наличными?

## Расследование создание: распространение и использование вредоносных программ для ЭВМ

Представляется наиболее целесообразной следующая последовательность решения основных задач при расследовании таких преступлений:

1 Установление факта и способа создания вредоносной программы для ЭВМ?

2 Установление факта использования и распространения вредоносной программы?

3 Установление лиц: виновных в создании: использовании и распространении вредоносных программ для ЭВМ?

4 Установление вреда: причиненного данным преступлением?

5 Установление обстоятельств: способствовавших совершению расследуемого преступления?

**Установление факта и способа создания вредоносной программы для ЭВМ?** Вредоносная программа: как правило: обнаруживается в момент: когда уже явно проявляются последствия ее применения: выявляется она также в процессе антивирусной проверки: производимой пользователем компьютерной системы перед началом работы на компьютере: особенно часто практикуемой при использовании чужих дискет и дисков?

Способов создания программ для ЭВМ очень много? Однако разработка вредоносных программ осуществляется обычно одним из двух нижеописанных способов?

1? Создание вредоносной программы ведется непосредственно на одном из рабочих мест автоматизированной информационной системы? Это: как правило: маскируется под правомерную повседневную работу на том или ином участке разработчиком вредоносной программы: который в силу своих служебных обязанностей имеет доступ к информационной системе и функционирующей в ней информации: а иногда и владеет кодами: паролями? Сокрытие преступных действий разработчик осуществляет путем удаления компрометирующих его данных или хранения их на собственных дискетах?

2? Создание такой программы: ведется вне сферы непосредственной деятельности компьютерной системы: для воздействия на которую она предназначена? При этом преступнику необходимы сведения о функционирующей в данной системе информации: способах доступа к ней: методах ее защиты? Для их получения он устанавливает связи с кем-либо из пользователей системы либо внедряет в нее свое доверенное лицо: чаще программиста?

Иногда вредоносная программа создается путем внесения изменений в существующую программу?

На факт создания вредоносной программы косвенно могут указывать следующие обстоятельства:

а повышенная заинтересованность алгоритмами функционирования программ: работой системы информационной защиты: входной и выходной информацией лицами: в круг обязанностей которых это не входит\*

6 внезапная увлеченность программированием лиц: в круг обязанностей которых программирование не входит?

Эти обстоятельства могут устанавливаться как в результате проведения оперативно-розыскных мероприятий: так и следственных действий например: допроса свидетелей из числа пользователей компьютерной системы: в которой обнаружены признаки использования вредоносной программы?

**Установление факта использования и распространения вредоносной программы?** Большинство пользователей компьютерных систем может обнаружить вредоносные программы с помощью антивирусных программ? В процессе расследования факт использования вредоносной программы можно установить посредством осмотра следующих документов: журналов учета рабочего времени доступа к вычислительной технике: сбоев и ремонта: регистрации пользователей компьютерной системы или сети: проведения регламентных работ\* лицензионных соглашений и договоров на пользование программными продуктами и их разработку\* книг паролей\* приказов и других документов: регламентирующих работу учреждения и: в частности: использование компьютерной информации? Надо иметь в виду: что эти документы могут существовать в электронной форме: на машинных носителях? К ознакомлению с ними рекомендуется привлекать специалиста- При изучении таких документов следователь может получить информацию о законности использования того или иного программного обеспечения: системе организации работы учреждения: использования в ней информации: доступа к информации и вычислительной технике: круге лиц: находившихся в определенный момент времени на объекте: где функционирует компьютерная система: или имевших доступ к вычислительной технике?

**При допросе подозреваемого: обвиняемого: свидетелей** необходимо выяснить способы распространения вредоносных программ: то есть предоставления доступа к ним путем продажи: проката: сдачи внаем: предоставления взаймы: включая импорт для любой из этих целей'?

Надо иметь в виду: что применяется множество способов использования и распространения вредоносных программ? В частности: оно осуществляется в случаях запуска программы с другого компьютера или с дискеты: купленной: одолженной: полученной в порядке обмена: или с электронной доски объявлений ВВС Би-Би-Си? Распространение программы вызывающей уничтожение и блокирование информации: нарушение работоспособности ЭВМ: системы ЭВМ или их сети: может осуществляться по компьютерной сети в результате использования нелицензионной и несертифицированной программы или купленной у случайного лица: а также скопированной у кого-либо из знакомых: например: чаще игровых программ?

Важное значение для установления фактов использования и распространения вредоносных программ имеет своевременное производство информационно-технологической экспертизы: которая может определить: какие изменения внесены в исследуемые программы: время внесения изменений: их характер: какие последствия способны вызвать использование и распространение вредоносных программ? Она может также установить примененный преступником способ преодоления программной и аппаратной защиты подбор ключей и паролей: отключение средств защиты: использование специальных программных средств?

**Установление лиц: виновных в создании: использовании и распространении вредоносных программ для ЭВМ?** При решении данной следственной задачи необходимо учитывать: что вредоносную программу может создать человек: обладающий навыками в обращении с компьютером и написании программ? Лучше всего их могут сделать опытные программисты: но они: как правило: не участвуют в их распространении? Нередко вредоносные программы создают и используют лица: сравнительно давно освоившие машинный язык: из чувства самоутверждения: по мотиву корысти или мести: а иногда из потребности в вандализме? Некоторые делают это в форме интеллектуального вызова: стремясь преодолеть систему информационной защиты: считающейся неуязвимой?

Использовать и распространять вредоносные программы может любой человек: умеющий работать на персональном компьютере? Однако наибольшую опасность представляют высококвалифицированные специалисты в области компьютерных технологий: опытные компьютерные взломщики: получившие в литературе название хакеров?

Преступления данной категории иногда совершаются группой лиц: причем один хакер создает вредоносные программы: а остальные члены группы обеспечивают его деятельность в материально-техническом и информационном отношениях? В мировой практике борьбы с компьютерными преступлениями известны случаи осуществления хакерами связей с организованной преступностью: когда преступные сообщества выступают в роли заказчиков компьютерных махинаций: обеспечивая хакеров необходимой техникой: организуя прикрытие: снимая через подставных лиц деньги в банковских компьютерных системах?

Поиск лица: причастного к использованию вредоносных программ: требует значительных затрат времени и средств? В благоприятных случаях установить его можно по следам рук: оставленным на участках дисководов: клавишах: некоторых других частях компьютера?

После установления подозреваемого его задержание должно быть произведено незамедлительно: чтобы не допустить уничтожения компрометирующих его материалов? В случае если вредоносная программа является компьютерным вирусом: от быстроты задержания зависят масштабы его возможного распространения и причинения ущерба?

**Установление вреда: причиненного данным преступлением?** Решая данную задачу: надо иметь в виду: что вредоносная программа в виде вируса может за считанные секунды размножиться в большом количестве экземпляров и за короткий период времени заразить многие компьютерные системы? Компьютерные вирусы могут:

а заполнить весь диск или всю свободную память компьютера своими копиями\*

б переставить местами часть файлов: т? е? смешать их так: что найти их на диске будет практически невозможно\*

в испортить таблицу размещения файлов\*

г отформатировать диск или дискету: уничтожив все ранее записанное на соответствующем носителе\*

д вывести на дисплей то или иное нежелательное сообщение\*

е перегрузить компьютер: то есть осуществить произвольный перезапуск\*

ж замедлить работу компьютера\*

з внести изменения в таблицу определения кодов: делая невозможным пользование клавиатурой\*

и изменить содержание программ и файлов: что может привести к ошибкам в сложных расчетах\*

к привести в негодность персональный компьютер\*

л раскрыть информацию с ограниченным доступом?

Размер ущерба: причиненного преступлением данного вида: устанавливается экспертным путем? Он может быть определен в рамках судебно-бухгалтерской и судебно-экономической экспертиз в комплексе с информационно-технологической и информационно-технической экспертизами?

**Установление обстоятельств: способствовавших совершению преступления?** Полную безопасность компьютерных систем обеспечить нельзя: но снизить опасность вредоносных программ для ЭВМ до определенного уровня возможно: в частности: путем устранения обстоятельств: способствующих созданию: использованию и распространению вредоносных компьютерных программ? К числу таких обстоятельств относятся в основном следующие:

отказ от использования антивирусных средств\*

использование случайного несертифицированного программного обеспечения\*

использование нелегальных копий программ для ЭВМ\*

отсутствие резервных копий программ и системных файлов\*

отсутствие учета и контроля за доступом к компьютерным системам\*

использование компьютеров не по назначению для компьютерных игр: обучения посторонних: написания программ лицами: в обязанности которых это не входит\*

игнорирование требования относительно проверки каждой приобретенной программы с целью возможного обнаружения признаков ее заражения компьютерным вирусом\*

незащищенность загрузочных дискет от нежелательных записей посредством специальной прорези\*

нерегулярность записей программ: устанавливаемых в компьютерную систему?

Устанавливаются перечисленные обстоятельства по результатам тщательного анализа всех материалов уголовного дела? Основным средством их установления является судебная информационно-технологическая экспертиза: при назначении которой необходимо ставить вопрос: Что способствовало совершению преступления: связанного с созданием: использованием и распространением вредоносных программ для ЭВМ;?

## Расследование нарушения правил эксплуатации ЭВМ: системы ЭВМ или их сети

Серьезный ущерб компьютерной системе или сети может нанести нарушение правил их эксплуатации: что обычно приводит к сбоям в обработке информации и в конечном счете дестабилизации деятельности соответствующего предприятия или учреждения?

При расследовании по делам данной категории необходимо прежде всего доказать факт нарушения определенных правил: повлекший уничтожение: блокирование или модификацию охраняемой законом компьютерной информации и причинивший существенный вред? Кроме того: необходимо установить и доказать:

место и время период времени нарушения правил эксплуатации ЭВМ\*

характер компьютерной информации: подвергшейся уничтожению: блокированию или модификации вследствие нарушения правил эксплуатации компьютерной системы или сети\*

способ и механизм нарушения правил\*

характер и размер ущерба: причиненного преступлением\*

факт нарушения правил определенным лицом\*

виновность лица: допустившего преступное нарушение правил эксплуатации ЭВМ\*

обстоятельства: способствовавшие совершению расследуемого преступления?

При **установлении факта преступного нарушения правил** эксплуатации ЭВМ необходимо тщательно изучить нормативные документы: предусматривающие правила эксплуатации данной компьютерной системы или сети: их характер и назначение: имея в виду: что соответствующие правила направлены на обеспечение информационной безопасности компьютерных систем и сетей? Они могут определять порядок создания: сбора: обработки: накопления: хранения: поиска: распространения и представления потребителю компьютерной информации: ее защиту?

Ст? 274 УК предусматривает охраняемую законом информацию: то есть главным образом информацию ограниченного доступа: которая по условиям ее правового режима использования подразделяется на информацию: отнесенную к государственной тайне: и конфиденциальную? Именно эти два вида информации: циркулирующие в компьютерных системах и сетях: нуждаются в особых средствах защиты?

Порядок накопления: обработки: защиты и предоставления пользователю информации с ограниченным доступом определяется органами государственной власти либо ее собственником? Такие правила существуют: например: в государственных архивах: органах государственной исполнительной власти: в информационных системах которых функционирует конфиденциальная информация или составляющая государственную тайну?

Степень секретности и конфиденциальности информации имеет существенное значение для определения размера ущерба: причиненного преступным нарушением правил эксплуатации ЭВМ?

Факт нарушения правил эксплуатации ЭВМ становится известным в первую очередь обычно владельцам и пользователям компьютерной системы или сети вследствие обнаружения отсутствия необходимой информации или ее существенного изменения: негативно отразившегося на деятельности предприятия: организации: учреждения?

Факт нарушения правил эксплуатации ЭВМ может быть установлен по материалам служебного административного расследования: если таковое имело место? Оно проводится обычно службой информационной безопасности объекта: на котором имел место соответствующий инцидент? В этих материалах можно найти ответы на многие из вопросов: перечисленных выше?

По материалам служебного расследования могут быть установлены также место: время преступного нарушения правил и другие обстоятельства: подлежащие доказыванию? Если служебное расследование не проводилось: подлежащие доказыванию обстоятельства устанавливаются лишь следственным путем?

При осмотре автоматизированных рабочих мест пользователя ЭВМ: системы ЭВМ или их сети можно установить конкретное место нарушения правил эксплуатации ЭВМ?

Необходимо различать место нарушения правил и место наступления вредных последствий? Нередко они не совпадают: особенно при нарушении правил эксплуатации компьютерных сетей: которые: как известно: представляют собой объединение ряда персональных компьютеров: расположенных в различных местах: подчас на значительных расстояниях друг от друга?

При расследовании нарушения правил эксплуатации компьютерной сети очень важно установить: где расположена обычная станция: эксплуатация которой осуществлялась с грубым нарушением правил информационной безопасности? В первую очередь необходимо определить места: где по схеме развертывания сети расположены рабочие станции: имеющие собственные дисководы: так как на них значительно больше возможностей для преступных нарушений правил эксплуатации компьютерной сети? Это: например: возможность для нарушителя копирования данных с файлового сервера на свою дискету или использования дискеты с различными программами: в том числе с компьютерными вирусами? Такие действия: ставящие под угрозу целостность информации: содержащейся и центральных файловых серверах: исключены на бездисковых рабочих станциях? Рекомендуется производить следственный осмотр учетных данных: в которых могут быть отражены сведения о расположении конкретной рабочей станции: использующей файловый сервер?

Кроме того: могут быть допрошены в качестве свидетелей администратор сети и специалисты: обслуживающие файловый сервер: в котором произошло уничтожение: блокирование или модификация компьютерной информации?

Им могут быть заданы примерно следующие вопросы %

На какой рабочей станции могли быть нарушены правила эксплуатации компьютерной сети: где она расположена;

Могли ли быть нарушены правила эксплуатации данной локальной вычислительной сети на рабочей станции: расположенной там-то;

Если правила нарушаются непосредственно на файловом сервере: то место нарушения этих правил может совпадать с местом наступления вредных последствий?

Место нарушения правил может быть установлено и по результатам информационно-технической экспертизы: перед экспертами которой могут быть поставлены вопросы %

1? На какой рабочей станции локальной вычислительной сети могли быть нарушены правила ее эксплуатации: в результате чего наступили вредные последствия;

2? Могли ли быть нарушены правила эксплуатации сети на рабочей станции: расположенной там-то;

При определении **времени нарушения правил** эксплуатации ЭВМ необходимо установить и зафиксировать как время нарушения конкретных правил: так и время наступления вредных последствий?

Нарушение правил и наступление вредных последствий могут произойти одновременно? Например: при отключении электропитания в результате нарушения установленных правил обеспечения информационной безопасности может быть мгновенно уничтожена с трудом введенная в компьютер очень важная информация: которую не успели записать на дискету в случае отсутствия запасных источников автономного питания: которые обычно автоматически подключаются при отключении основного?

Но возможен также значительный разрыв во времени между моментом нарушения правил и временем наступления вредных последствий? Так: например: в определенный момент времени вносятся изменения в программу или базу данных в нарушение установленных правил и значительно позже наступают вредные последствия этого?

Время нарушения правил обычно устанавливается по учетным данным: которые фиксируются в процессе эксплуатации ЭВМ? К ним относятся сведения о результатах применения средств автоматического контроля компьютерной системы: регистрирующих ее пользователей и моменты подключения к ней абонентов: содержание журналов учета сбойных ситуаций: передачи смен операторами ЭВМ: распечатки выходной информации: где: как правило: фиксируется время ее обработки? Указанные данные могут быть получены благодаря осмотру места происшествия: выемке и осмотру необходимых документов? Осмотр места происшествия и документов целесообразно проводить с участием специалиста? Время нарушения правил можно установить также путем допроса свидетелей из числа лиц: участвующих в эксплуатации ЭВМ? Допрашиваемым могут быть заданы примерно следующие вопросы %

Каким образом в данной компьютерной системе фиксируются факты и время отклонения от установленных правил порядкаэксплуатации ЭВМ;

Когда могло быть нарушено определенное правило эксплуатации ЭВМ: вследствие чего наступили вредные последствия;

При необходимости может быть назначена судебная информационно-техническая экспертиза: перед которой для установления времени преступного нарушения правил можно сформулировать следующие вопросы %

Как технически осуществляется автоматическая фиксация времени обращения пользователей к данной компьютерной системе или сети и всех изменений: происходящих в их информационных массивах;

Можно ли по представленным машинным носителям информации установить время нарушения определенных правил эксплуатации ЭВМ: если да: то когда нарушение произошло;

Время наступления вредных последствий устанавливается по материалам служебного расследования: по результатам осмотра места происшествия: а также путем допроса свидетелей и производства судебных экспертиз?

При осмотре места происшествия могут быть обнаружены машинные носители информации: на которых ранее хранились важные: охраняемые законом данные: которые вследствие нарушения правил эксплуатации ЭВМ оказались уничтоженными или существенно измененными либо заблокированными? На них может быть зафиксировано время наступления таких последствий: которое можно выявить при следственном осмотре: с помощью специалиста?

Указанные последствия часто обнаруживаются пользователями компьютерной системы или сети: а также администраторами базы данных? Поэтому при допросе их в качестве свидетелей следует выяснить: когда они впервые обнаружили отсутствие или существенное изменение той информации: которая находилась в определенной базе данных?

Время наступления вредных последствий может быть установлено в и результате производства информационно-технической экспертизы: при назначении которой перед экспертами целесообразно ставить следующие вопросы %

Как технически осуществляется автоматическая фиксация времени уничтожения или изменения базы данных либо блокирования отдельных файлов;

Можно ли по стертым или измененным вследствие нарушения правил эксплуатации ЭВМ базам данных установить время наступления вредных последствий и если да: то когда они наступили;

**Способ нарушения правил эксплуатации ЭВМ** может быть как активным: так и пассивным? Первый выражается в самовольном выполнении непредусмотренных операций при компьютерной обработке информации: а второй - в невыполнении предписанных действий?

**Механизм нарушения таких правил** связан с технологией обработки информации на ЭВМ? Это: например: неправильное включение и выключение ЭВМ: использование посторонних дискет без предварительной проверки на наличие в ней компьютерного вируса: невыполнение требования об обязательном копировании информации для ее сохранения на случай уничтожения первого экземпляра?

Способ и механизм нарушения правил устанавливается путем допросов свидетелей: подозреваемых и обвиняемых желательно с участием специалистов: проведения следственного эксперимента: производства информационно-технической экспертизы?

При допросах выясняется последовательность той или иной операции на ЭВМ: которая привела к нарушению правил?

**Характер ущерба:** наносимого преступным нарушением правил эксплуатации ЭВМ: в общих чертах обозначен в диспозиции ст? 274 УК? Он может заключаться в уничтожении: блокировании или модификации охраняемой законом информации? Ущерб либо носит чисто экономический характер: либо вредит интересам государства вследствие утечки сведений: составляющих государственную тайну? Разглашение или утрата такой информации может нанести серьезный ущерб внешней безопасности Российской Федерации: что влечет также уголовную ответственность по статьям 283 и 284 УК?

Размер ущерба устанавливается посредством информационно-экономической экспертизы: перед которой целесообразно ставить вопрос: Какова стоимость информации: уничтоженной или измененной вследствие нарушения правил эксплуатации ЭВМ?

Степень секретности информации устанавливается в соответствии с Законом О государственной тайне?

При **установлении лица**: допустившего преступное нарушение правил эксплуатации ЭВМ: следует иметь в виду: что виновным может быть согласно ч? 1 ст? 274 УК лицо: имеющее доступ к ЭВМ: системе ЭВМ или их сети? При этом необходимо различать лицо: имеющее доступ к ЭВМ: и лицо: имеющее доступ к компьютерной информации? кое лицо: допущенное к ЭВМ: имеет доступ к компьютерной информации? Доступ к ЭВМ: системе ЭВМ или сети: как правило: имеют определенные лица в силу выполняемой ими работы: связанной с применением средств компьютерной техники? Среди них и следует устанавливать нарушителей правил? В отношении каждого из них устанавливается:

фамилия: имя: отчество\*

занимаемая должность относимость к категории должностных лиц: ответственных за информационную безопасность и надежность работы компьютерного оборудования: либо к категории непосредственно отвечающих за обеспечение выполнения правил эксплуатации данной компьютерной системы или сети\*

образование\*

специальность\*

стаж работы по специальности и на данной должности\*

уровень профессиональной квалификации\*

конкретные обязанности по обеспечению информационной безопасности и нормативные акты: которыми они установлены договор: проектная документация на автоматизированную систему и пр?\*

причастность к разработке: внедрению в опытную и промышленную эксплуатацию данной компьютерной системы или сети\*

наличие и объем доступа к базам и банкам данных\*

данные: характеризующие лицо по месту работы\*

наличие домашнего компьютера и оборудования к нему?

Все это устанавливается посредством допросов свидетелей: обвиняемого: осмотра эксплуатационных документов на данную компьютерную систему: осмотра компьютера: оборудования к нему: машинных носителей информации: распечаток?

**Виновность лица**: совершившего преступное нарушение правил эксплуатации ЭВМ: устанавливается на основе анализа результатов всех проведенных в ходе расследования следственных действий? Соответствующие правила могут быть нарушены как умышленно: так и неосторожно? В отношении же последствий вина может быть только неосторожной? При умышленном нарушении рассматриваемых правил и наличии умысла на вредные последствия нарушения должна наступать ответственность за совокупность преступлений: например: при нарушении правил с целью повреждения компьютерного оборудования - по ст? 274 и 167 УК?

**Обстоятельство: способствовавшие совершению данного преступления**: выявляются путем изучения как общего состояния охраны информационной безопасности в определенной системе или сети: так и факторов: непосредственно обусловивших расследуемое событие?

Многие обстоятельства: способствовавшие нарушению правил эксплуатации ЭВМ: но установить по материалам служебного расследования?

Так: в связи с покушением на хищение более 68 млрд? рублей из Центрального банка РФ служебным расследованием: проведенным до возбуждения уголовного дела: были установлены причины: способствовавшие этому преступлению: главными их которых явились нарушения правил эксплуатации компьютерной системы осуществления безналичных расчетов: среди которых фигурировали: в частности: следующие %

ведение обработки платежных документов без использования сертифицированных средств защиты\*

слабые руководство и контроль за технологическими процессами компьютерной обработки платежных документов со стороны Управления безопасности??

Установлению криминогенных факторов могут способствовать судебные экспертизы?

По уголовному делу о хищении валютных средств во Внешэкономбанке: совершенных путем использования компьютерных расчетов: комплексной судебно-бухгалтерской и информационно-технической экспертизой были установлены следующие нарушения порядка эксплуатации компьютерной системы %

отсутствие организации работ по обеспечению информационной безопасности\*

нарушение технологического цикла проектирования: разработки: испытаний и сдачи в эксплуатацию программного обеспечения системы автоматизации банковских операций\*

совмещение функций разработки и эксплуатации программного обеспечения в рамках одного структурного подразделения: что позволяло разработчикам после сдачи компьютерной системы в промышленную эксплуатацию иметь доступ к закрытой информации в нарушение установленных правил под предлогом доводки программного обеспечения\*

использование незарегистрированных в установленном порядке программ\*

неприменение в технологическом процессе всех имеющихся средств и процедур регистрации операций по обработке компьютерной информации и лиц: эксплуатирующих ЭВМ? **[9]**

ЗАКЛЮЧЕНИЕ

В ходе изучения действующего уголовного законодательства в области регулирования компьютерного права и специфики расследования преступлений в сфере компьютерной информации были сделаны определенные обобщения:

Преступления в области компьютерной информации являются частью информационных преступлений: объединенных единым инструментом обработки информации — компьютером? Практически все преступления относятся к преступлениям средней тяжести? Исключением является лишь преступления: квалифицируемые ч?2 ст?273: относящиеся к тяжким преступлениям? Для всех преступлений данного вида необходимо наличие вины в форме умысла? Субъектом преступления может стать любой человек старше 16 лет: особенно если учесть всевозрастающую компьютерную грамотность населения?

Известные на сегодня способы совершения компьютерных преступлений отличаются значительным: и постоянно расширяющимся разнообразием? Совершают преступления данной категории чаще всего люди со специальной подготовкой в области автоматизированной обработки информации: причем более половины из их числа в составе преступных групп? Основная опасность исходит от внутренних пользователей — ими совершается более 90 преступлений?

Типичными следственными действиями: применяющимися при расследовании преступлений в сфере компьютерной информации являются следственный осмотр: допрос свидетеля: потерпевшего: обвиняемого: подозреваемого: производство судебных информационно-технических экспертиз: обыск и выемка: а также следственный эксперимент?

При расследовании преступлений в сфере компьютерной информации следственные задачи решаются в следующей последовательности:

1. Установление факта совершения преступления: времени его совершения: способа и других обстоятельств: знание которых необходимо для успешного проведения расследования?
2. установление лица или лиц: совершившего преступное деяние: виновности и мотивов преступления
3. установление вредных последствий преступления и выявление обстоятельств: способствовавших преступлению

На основе вышесказанного считаю необходимым принять следующие выводы:

1 При производстве следственных осмотра объектов преступления в целях обнаружения следов преступления: выяснения обстановки происшествия и иных значимых для дела обстоятельств целесообразно привлекать к ним технических специалистов с достаточно высокой степенью компетенции? Соответствующие специалисты призываются также для участия при производстве обыска последующего осмотра изъятого и следственного эксперимента? Вышеуказанные участники следственных действий должны оказать помощь следователю при установлении факта совершения преступления: времени его совершения: способа совершения: обстоятельств: способствовавших преступлению? Весьма важно значение проведения судебных информационно-технических экспертиз?

2 Поскольку совершение преступлений: квалифицирующихся статьями 272 и 273 УК РФ является технологически весьма сложным действием: круг подозреваемых значительно сужается? Он охватывает весьма ограниченное количество людей? Эти люди: а имеют достаточно высокую квалификацию в области обработки компьютерной информации: разработки: создания и эксплуатации высокоинтеллектуальной компьютерной техники\* б с большой степенью вероятности имеют легальный доступ как к самим компьютерам: компьютерной системе или сети: так и к конфиденциальной информации: хранящейся в них\*

3 В соответствии с источниками рекомендуется предусмотреть в форме плана расследования следующие данные: 1 наименование дела\* 2 дату его возбуждения\* 3 срок окончания расследования\* 4 графы: а доверсионные вопросы нуждающиеся в выяснении еще до выдвижения какой-либо версии\* б версии\* в подлежащие выяснению вопросы\* г необходимые мероприятия применительно к каждой версии и каждому выясняемому вопросу\* д срок выполнения каждого мероприятия\* е исполнитель каждого мероприятия\* ж отметка о выполнении мероприятия?

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Конституция Российской Федерации% Принята всенародным голосованием 12 декабря 1993 г?—Москва%изд-во БЕК: 1996? 62 с?
2. Уголовный Кодекс Российской Федерации% Федеральный закон РФ от 1 января 1997 г? — Йошкар-Ола% Изд?-комп? центр МПИК: 1996? 237 с?
3. Правоохранительные органы? Учебник для юридических вузов и факультетов 2-е изд?: испр? и доп? Гуценко К?Ф?: Ковалев М?А??? М?% Зерцало: ТЕИС: 1996?- 328 с?
4. Российское уголовное право? Особенная часть №Под редакцией В?Н? Кудрявцева: А?В? Наумова?- М?: Юрист: 1997?- 496 с?
5. Уголовное право России? Особенная часть: Учебник №Отв? ред? доктор юридических наук: профессор Б?В? Здравомыслов?- М?: Юрист: 1996?- 560 с?
6. Уголовный процесс: Учебник для студентов юридических вузов и факультетов М?% Зерцало: ТЕИС: 1996?- 509 с?
7. Уголовное право России? Особенная часть: Учебник №Под ред? проф? А? И? Рарога?- М?: Институт международного права и экономики? Издательство “Триада: Лтд”: 1996?- 480 с?
8. Уголовное право Российской Федерации? Особенная часть: Учебник №Под ред? Г?Н? Борзенкова и В?С? Комиссарова?- М?: Олимп\* ООО “Издательство АСТ”: 1997?- 752 с?
9. Руководство для следователей №Под ред? Н?А? Селиванова: В?А? Снеткова?- М?: ИНФРА - М: 1997?- IV: 732 с?
10. Белкин Р?С? Криминалистическая энциклопедия?- М?% Издательство БЕК: 1997?- 342 с?
11. Беззубцев О?А?: Ковалев А?К? ФАПСИ% Законодательное регулирование в области защиты информации Технологии и средства связи:—1997?—май-июнь: с? 94-96
12. Вихорев С?В?: Герасименко В?Г? Борьба с преступлениями в банковских вычислительных системах Технологии и средства связи:—1997?—ноябрь-декабрь: с? 92-93
13. Волчинская Е?К? Есть ли в России компьютерное право; Российская юстиция?— 1997?— 6: с? 9-19
14. Гостев И?М? Информационное право? Вопросы законодательного регулирования Технологии и средства связи:—1997?—май-июнь: с? 98-100
15. Гульбин Ю? Преступления в сфере компьютерной информации Российская юстиция?— 1997?— 10: с? 24-25
16. Крылов В?Г? Информационные преступления — новый криминалистический объект Российская юстиция?— 1997?— 4: с? 22
17. Комиссаров В?С? Преступления в сфере компьютерной информации% понятие и ответственность Юридический мир?— 1998?— февраль: с? 9-19
18. Ляпунов Ю?: Максимов В? Ответственность за компьютерные преступления Юридический консультант?— 1997?— 10: с? 9-15
19. Симкин Л? Как остановить компьютерное пиратство; Российская юстиция?— 1996?— 10: с? 37-39
20. Чечко Л? Компьютерные хищения Российская юстиция?—1996?— 5: с? 45
21. Шахов А?В? Электронные взломщики-преступники под маской ромнатиков Технологии и средства связи:—1997?—март-апрель: с? 88-89
22. Справочник следователя (Практическая криминалистика% следственные действия(? Выпуск первый?- М?% Юрид? лит?: 1990?- 228 с?
23. Баев О? Я? Тактика следственных действий% Учебное пособие? - Воронеж% НПО “МОД ЭК”: 1995?- 224 с
24. Криминалистика №под редакцией д?ю?н? проф? В?А? Образцова? -М?% Юристъ: 1995? - 592 с?

Приложение 1

Способы совершения преступлений в банковских информационных сетях

|  |
| --- |
| **Стадии совершения преступления** |
| **Приготовление** | **Покушение** | **Окончание** |
| **Подготовка орудий преступления** | **Создание условий для преступления** | **Манипуляции с банковской информацией** | **Маскировка следов преступления** | **Получение и пользование деньгами** |
|  |
| **Основные приемы и методы действий** |
| **покупка СВТ** | **изъятие СВТ** | **подмена данных** | **дробление сумм** | **снятие со счетов** |
| **аренда СВТ** | **НСД к СВТ** | **троянский конь** | **прогон по цепочке** | **легальный перевод** |
| **хищение СВТ** | **перехват информации** | **салями** | **блокирование** | **приобретение имущества** |
| **составление программ** | **моделирование** |  |  |  |
|  | **асинхронная атака** |  |  |  |
|  | **моделирование** |  |  |  |

КОМИТЕТ ПО ДЕЛАМ НАУКИ И ВЫСШЕЙ ШКОЛЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЧУВАШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

 ИМЕНИ И? Н? УЛЬЯНОВА

Институт экономики: финансов и права

Юридический факультет

**ДИПЛОМНАЯ РАБОТА**

**ТЕМА% РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

|  |
| --- |
| Выполнил% студент группы ВЮ-32-96 Петров Александр Владимирович |
| Научный руководитель% доцент Сироткин Леонид Иванович |
| Заведующий кафедрой% доктор юридических наук: профессор Малюткин Валентин Алексеевич |