СРЕДНЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

О.Э.ЗГАДЗАЙ, С.Я.КАЗАНЦЕВ, Л.А.КАЗАНЦЕВА

ИНФОРМАТИКА ДЛЯ ЮРИСТОВ

Под редакцией С.Я.Казанцева

Допущено
Министерством образования Российской Федерации
в качестве учебника для студентов Образовательных учреждений
среднего профессионального образования, обучающихся
по специальностям правоведческого профиля

Москва
Издательство Мастерство
2001

ББК 67.404.3
УДК65.012.45
З-46

Рецензенты:
начальник факультета информационных технологий Московского института МВД России, д-р техн. наук, полковник внутренней службы *А. С. Овчинский;*
ученый секретарь Института среднего профессионального образования РАО, доцент кафедры маркетинга Казанского социально-юридического института, канд. пед. наук *Г. И. Кирилова.*

Згадзай О.Э. и др.
З-46 Информатика для юристов: Учебник / О.Э. Згадзай, С.Я. Казанцев, Л.А. Казанцева; Под ред. С.Я. Казанцева. — М.: Мастерство, 2001. — 256 с.
ISBN 5-294-00070-9

Рассмотрены аппаратное, программное и математическое обеспечение современной информационной технологии применительно к юридической деятельности. Раскрыта сущность информационных процессов в системах различной природы. Приведены примеры информационных процессов и систем; методы построения простейших информационных моделей и алгоритмов.

Для студентов средних профессиональных учебных заведений юридических специальностей.

ББК 67.404.3
УДК 65.012.45

ISBN 5-294-00070-9

Глава 9. КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

Процесс информатизации общества наряду с положительными последствиями имеет и ряд отрицательных сторон. Так, например, объединение компьютеров в глобальные сети с одной стороны, дало возможность большому количеству людей приобщиться к огромному массиву накопленной в мире информации, а с другой стороны, породило проблемы с охраной интеллектуальной собственности, помещаемой в сеть и хранящейся в ней.

Широкое распространение и внедрение во все сферы жизни общества компьютеров и компьютерных технологий привело и к тому, что изменился сам характер многих преступлений, появились новые их виды.

Преступные группы и сообщества также начали активно использовать в своей деятельности новые информационные технологии. Для достижения прежде всего корыстных целей преступники стали активно применять компьютеры и специальную технику, создавать системы конспирации и скрытой связи в рамках системного подхода при планирования своих действий. Одновременно наблюдается резкое нарастание криминального профессионализма — количества дерзких по замыслу и квалифицированных по исполнению преступлений.

Очевидно, что рассматриваемые проблемы не могли не затронуть и сферу деятельности правоохранительных органов. Возникла необходимость в разработке подходов к исследованию новых видов преступлений, методов их расследования и профилактики.

9.1. ПОНЯТИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ И ИХ КЛАССИФИКАЦИЯ

Негативным последствием информатизации общества является появление так называемой компьютерной преступности. В литературе до настоящего времени ведется полемика о том, какие действия следует относить к разряду компьютерных преступлений. Сложность решения вопроса заключается также и в том, что диапазон противоправных действий, совершаемых с использованием средств компьютерной техники, чрезвычайно широк — от преступлений традиционного типа до преступлений, требующих высокой математической и технической подготовки.

Появление на рынке в 1974 г. компактных и сравнительно недорогих персональных компьютеров дало возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контроле доступа к информации, ее сохранности и целостности. Организационные меры, а также программные и технические средства защиты информации оказались недостаточно эффективными.

Особенно остро проблема несанкционированного вмешательства в работу компьютерных систем дала о себе знать в странах с развитой информационной инфраструктурой. Вынужденные прибегать к дополнительным мерам безопасности, они стали активно использовать правовые, в том числе и уголовно-правовые средства защиты. Так, например, в Уголовном кодексе Франции в 1992 г. система преступлений против собственности пополнилась специальной главой «О посягательствах на системы автоматизированной обработки данных». В ней предусмотрена ответственность за незаконный доступ ко всей или к части системы автоматизированной обработки данных, воспрепятствование работе или нарушение правильности работы системы или ввод в нее обманным способом информации, уничтожение или изменение базы данных. Изучить и разработать проект специальной конвенции, посвященной проблеме правонарушений в сфере компьютерной информации, счел необходимым и Совет Европы.

Развивалась компьютерная преступность и в СССР. Так, одно из первых в нашей стране компьютерных преступлений, совершенное в 1979 г. в Вильнюсе — хищение 78 584 руб. — удостоилось занесения в международный реестр подобных правонарушений. Российские правоведы уже давно ставили вопрос о необходимости законодательного закрепления правоотношений, вытекающих из различных сфер применения средств автоматизированной обработки информации. Определенным этапом стало принятие в 1992 г. Закона РФ «О правовой охране программ для электронно-вычислительных машин и баз данных». Закон содержал положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных, либо незаконное воспроизведение или распространение таковых влечет уголовную ответственность. Однако соответствующих изменений в УК РФ внесено не было. В 1994 г. был принят Гражданский кодекс, который содержит ряд норм, связанных с компьютерной информацией, а в 1995 г. — Федеральный закон об информации, информатизации и защите информации. Логическим развитием правовой системы, создающей условия безопасности автоматизированной обработки информации, стало включение в УК РФ 1996 г. группы статей, предусматривающих основания уголовной ответственности за нарушения в сфере компьютерной информации.

Хотя действующее в большинстве стран уголовное законодательство является достаточно гибким, чтобы квалифицировать правонарушения этого типа, социальные и технические изменения создают все новые и новые проблемы. Поэтому некоторые из известных мировой практике компьютерных посягательств не подпадают под действие уголовного законодательства и в юридическом смысле не могут считаться преступными. Так, существует точка зрения, что компьютерных преступлений, как преступлений специфических в юридическом смысле, не существует и следует говорить лишь о компьютерных аспектах преступлений[1].

Вместе с тем, специалисты в данной области исследований пришли к выводу, что к разряду компьютерных следует отнести те преступления, у которых *объектом* преступного посягательства является *информация,* обрабатываемая и хранящаяся в компьютерных системах, а *орудием* посягательства служит *компьютер.* По этому пути пошло и российское законодательство.

Следует заметить, что с точки зрения уголовного законодательства охраняется *компьютерная информация,* которая определяется как информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ. Вместо термина «компьютерная информация» можно использовать и термин «машинная информация», под которой подразумевается информация, запечатленная на машинном носителе, в памяти электронно-вычислительной машины, системе ЭВМ или их сети. В качестве предмета или орудия преступления, согласно законодательству, может выступать компьютерная информация, компьютер, компьютерная система или компьютерная сеть.

При рассмотрении вопросов о классификации компьютерных преступлений и их криминалистической характеристике целесообразно исходить из определения компьютерного преступления в широком смысле слова. В этом случае под компьютерным преступлением следует понимать предусмотренные законом общественно-опасные деяния, совершаемые с использованием средств компьютерной техники. Правомерно также использовать термин «компьютерное преступление» в широком значении как социологическую категорию, а не как понятие уголовного права.

Классификация компьютерных преступлений может быть проведена по различным основаниям. Так, например, можно условно подразделить все компьютерные преступления на две большие категории: преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства. При этом не принимаются во вни-

---

[1] *Батурин Ю. М.* Право и политика в компьютерном круге. — М.: Наука, 1987.

Появление на рынке в 1974 г. компактных и сравнительно недорогих персональных компьютеров дало возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контроле доступа к информации, ее сохранности и целостности. Организационные меры, а также программные и технические средства защиты информации оказались недостаточно эффективными.

Особенно остро проблема несанкционированного вмешательства в работу компьютерных систем дала о себе знать в странах с развитой информационной инфраструктурой. Вынужденные прибегать к дополнительным мерам безопасности, они стали активно использовать правовые, в том числе и уголовно-правовые средства защиты. Так, например, в Уголовном кодексе Франции в 1992 г. система преступлений против собственности пополнилась специальной главой «О посягательствах на системы автоматизированной обработки данных». В ней предусмотрена ответственность за незаконный доступ ко всей или к части системы автоматизированной обработки данных, воспрепятствование работе или нарушение правильности работы системы или ввод в нее обманным способом информации, уничтожение или изменение базы данных. Изучить и разработать проект специальной конвенции, посвященной проблеме правонарушений в сфере компьютерной информации, счел необходимым и Совет Европы.

Развивалась компьютерная преступность и в СССР. Так, одно из первых в нашей стране компьютерных преступлений, совершенное в 1979 г. в Вильнюсе — хищение 78 584 руб. — удостоилось занесения в международный реестр подобных правонарушений. Российские правоведы уже давно ставили вопрос о необходимости законодательного закрепления правоотношений, вытекающих из различных сфер применения средств автоматизированной обработки информации. Определенным этапом стало принятие в 1992 г. Закона РФ «О правовой охране программ для электронно-вычислительных машин и баз данных». Закон содержал положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных, либо незаконное воспроизведение или распространение таковых влечет уголовную ответственность. Однако соответствующих изменений в УК РФ внесено не было. В 1994 г. был принят Гражданский кодекс, который содержит ряд норм, связанных с компьютерной информацией, а в 1995 г. — Федеральный закон об информации, информатизации и защите информации. Логическим развитием правовой системы, создающей условия безопасности автоматизированной обработки информации, стало включение в УК РФ 1996 г. группы статей, предусматривающих основания уголовной ответственности за нарушения в сфере компьютерной информации.

Хотя действующее в большинстве стран уголовное законодательство является достаточно гибким, чтобы квалифицировать правонарушения этого типа, социальные и технические изменения создают все новые и новые проблемы. Поэтому некоторые из известных мировой практике компьютерных посягательств не подпадают под действие уголовного законодательства и в юридическом смысле не могут считаться преступными. Так, существует точка зрения, что компьютерных преступлений, как преступлений специфических в юридическом смысле, не существует и следует говорить лишь о компьютерных аспектах преступлений[1].

Вместе с тем, специалисты в данной области исследований пришли к выводу, что к разряду компьютерных следует отнести те преступления, у которых *объектом* преступного посягательства является *информация,* обрабатываемая и хранящаяся в компьютерных системах, а *орудием* посягательства служит *компьютер.* По этому пути пошло и российское законодательство.

Следует заметить, что с точки зрения уголовного законодательства охраняется *компьютерная информация,* которая определяется как информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ. Вместо термина «компьютерная информация» можно использовать и термин «машинная информация», под которой подразумевается информация, запечатленная на машинном носителе, в памяти электронно-вычислительной машины, системе ЭВМ или их сети. В качестве предмета или орудия преступления, согласно законодательству, может выступать компьютерная информация, компьютер, компьютерная система или компьютерная сеть.

При рассмотрении вопросов о классификации компьютерных преступлений и их криминалистической характеристике целесообразно исходить из определения компьютерного преступления в широком смысле слова. В этом случае под компьютерным преступлением следует понимать предусмотренные законом общественно-опасные деяния, совершаемые с использованием средств компьютерной техники. Правомерно также использовать термин «компьютерное преступление» в широком значении как социологическую категорию, а не как понятие уголовного права.

Классификация компьютерных преступлений может быть проведена по различным основаниям. Так, например, можно условно подразделить все компьютерные преступления на две большие категории: преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства. При этом не принимаются во вни-

---

[1] *Батурин Ю.М.* Право и политика в компьютерном круге. — М: Наука, 1987.

мание так называемые «околокомпьютерные» преступления, связанные с нарушением авторских прав программистов, незаконным бизнесом на вычислительной технике, а также физическим уничтожением компьютеров и т. п.

Одна из наиболее общих классификаций была предложена в 1983 г. группой экспертов Организации экономического сотрудничества и развития. В соответствии с ней выделяются следующие криминологические группы компьютерных преступлений:

• экономические преступления;

• преступления против личных прав и частной сферы;

• преступления против государственных и общественных интересов.

Экономические компьютерные преступления являются наиболее распространенными. Они совершаются по корыстным мотивам и включают в себя компьютерное мошенничество, кражу программ («компьютерное пиратство»), кражу услуг и машинного времени, экономический шпионаж.

Компьютерными преступлениями *против личных прав и частной сферы* являются незаконный сбор данных о лице, разглашение частной информации (например, банковской или врачебной тайны), незаконное получение информации о расходах и т.д.

Компьютерные преступления *против государственных и общественных интересов* включают в себя преступления, направленные против государственной и общественной безопасности, угрожающие обороноспособности государства, а также злоупотребления с автоматизированными системами голосования и т. п.

Подходить к классификации компьютерных преступлений наиболее оправданно с позиций составов преступлений, которые могут быть отнесены к разряду компьютерных. Хотя состав компьютерных преступлений в настоящее время четко не определен, можно выделить ряд видов противоправных деяний, которые могут быть в него включены. Перечислим некоторые основные виды преступлений, связанных с вмешательством в работу компьютеров:

• *несанкционированный доступ в корыстных целях к информации, хранящейся в компьютере или информационно-вычислительной сети.* Несанкционированный доступ осуществляется, как правило, с использованием чужого-имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных. Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т.п.), оказываются беззащитны про-

тив этого приема. Самый простой путь его осуществления — получить коды и другие идентифицирующие шифры законных пользователей. Несанкционированный доступ может осуществляться и в результате системной поломки. Например, если некоторые файлы одного пользователя остаются открытыми, то другие пользователи могут получить доступ к не принадлежащим им частям банка данных. Все происходит так, словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В таком случае он может проникнуть в чужие сейфы и похитить все, что в них хранится:

• *разработка и распространение компьютерных вирусов.* Программы-вирусы обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание;

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

• *халатная небрежность при разработке, создании и эксплуатации программно-вычислительных комплексов компьютерных сетей, приведшая к тяжким последствиям.* Проблема небрежности в области компьютерной техники сродни вине по неосторожности при использовании любого другого вида техники. Особенностью компьютерных систем является то, что абсолютно безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима;

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

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

• *хищение программного обеспечения.* Если «обычные» хищения подпадают под действие существующего уголовного закона, то

проблема хищения программного обеспечения значительно более сложна. Значительная часть программного обеспечения в России распространяется путем кражи и обмена краденым;

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

• *несанкционированный просмотр или хищение информации из банков данных, баз данных и баз знаний.* В данном случае под базой данных следует понимать форму представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Приходится констатировать, что процесс компьютеризации общества приводит к увеличению количества компьютерных преступлений, возрастанию их удельного веса в общей доле материальных потерь от различных видов преступлений. Потери же отдельно взятого государства в таких случаях могут достигать колоссальных размеров. Один из характерных примеров — уголовное дело о хищении 125,5 тыс. долл. США и подготовке к хищению еще свыше 500 тыс. долл. во Внешэкономбанке СССР в 1991 г., рассмотренное московским судом. По материалам другого уголовного дела, в сентябре 1993 г. было совершено покушение на хищение денежных средств в особо крупных размерах из Главного расчетно-кассового центра Центрального Банка России по г. Москве на сумму 68 млрд. 309 млн. 768 тыс. руб.

Имели также место следующие факты: хищение в апреле 1994 г. из расчетно-кассового центра (РКЦ) г. Махачкалы на сумму 35 млрд. 1 млн. 557 тыс. руб.; хищения в московском филиале Инкомбанка; в филиалах Уникомбанка; в коммерческом банке Красноярского края, откуда было похищено 510 млн. руб.; хищения в акционерном коммерческом банке г. Волгограда на сумму 450 млн. руб.; в Сбербанке г. Волгограда на сумму 2 млрд. руб.

По данным МВД России, с 1992—1994 гг. из банковских структур преступниками по фальшивым кредитным авизо и поддельным ордерам было похищено более 7 трлн. руб. В связи с ростом подобных хищений еще в конце 1993 г. в ЦБ России и региональных РКЦ были установлены компьютерные системы защиты от фальшивых платежных документов. По данным Центрального Банка России, ежеквартально выявляется фиктивных платежей на десятки миллиардов рублей, которые преступники внедряют в сети подразделений банка.

Парадоксальная особенность компьютерных преступлений состоит и в том, что трудно найти другой вид преступления, после совершения которого его жертва не выказывает особой заинтере-

сованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность на поприще компьютерного взлома, мало что утаивая от представителей правоохранительных органов. Психологически этот парадокс вполне объясним.

Во-первых, жертва компьютерного преступления совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты своей репутации) существенно превосходят уже причиненный ущерб.

И, во-вторых, преступник приобретает широкую известность в деловых и криминальных кругах, что в дальнейшем позволяет ему с выгодой использовать приобретенный опыт.

9.2. СПОСОБЫ СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Важнейшим и определяющим элементом криминалистической характеристики любого, в том числе и компьютерного, преступления является совокупность данных, характеризующих способ его совершения.

Под способом совершения преступления обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, которое оставляет различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить оптимальные методы решения задач раскрытия преступления.

Ю.М.Батурин разделил способы совершения компьютерных преступлений на пять основных групп[1]. Методологический подход Ю.М.Батурина и ряд предложенных им классификаций следует считать достаточно удачными, поскольку в своей основе этот подход опирается на систематизацию способов совершения компьютерных преступлений, применяющуюся в международной практике. В качестве основного классифицирующего признака выступает метод использования преступником тех или иных действий, направленных на получение доступа к средствам компьютерной техники. Руководствуясь этим признаком, Ю. М. Батурин выделил следующие общие группы по отношению к способу совершения компьютерных преступлений:

- изъятие средств компьютерной техники;
- перехват информации;

[1] *Батурин Ю.М.* Проблемы компьютерного права. — М: Юрид. лит., 1991.

• несанкционированный доступ;
• манипуляция данными и управляющими командами;
• комплексные методы.

К первой группе относятся традиционные способы совершения обычных видов преступлений, в которых действия преступника направлены на изъятие чужого имущества. Характерной отличительной чертой данной группы способов совершения компьютерных преступлений является тот факт, что в них средства компьютерной техники всегда выступают только в качестве предмета преступного посягательства. Например, прокуратурой г. Кургана в 1997 г. расследовалось уголовное дело по факту убийства частного предпринимателя. В ходе обыска на квартире убитого следователем был изъят персональный компьютер. По имеющейся оперативной информации в памяти компьютера убитый мог хранить фамилии, адреса своих кредиторов и должников. В дальнейшем этот компьютер по решению следователя был передан в одну из компьютерных фирм для производства исследования содержимого его дисков памяти. В ту же ночь из помещения упомянутой компьютерной фирмы путем отгиба решеток была произведена кража данного компьютера. В результате того, что изъятие и передача ЭВМ были произведены следователем с рядом процессуальных нарушений, данное преступление осталось нераскрытым.

Ко второй группе относятся способы совершения компьютерных преступлений, основанные на действиях преступника, направленных на получение данных и машинной информации посредством использования методов аудиовизуального и электромагнитного перехвата. Далее в скобках будут приводиться оригинальные названия способов на английском языке

Активный перехват (interception) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера, например линии принтера или телефонному проводу канала связи либо непосредственно через соответствующий порт персонального компьютера.

Пассивный (электромагнитный) *перехват (electromagnetic pickup)* основан на фиксации электромагнитных излучений, возникающих при функционировании многих средств компьютерной техники, включая и средства коммуникации. Так, например, излучение электронно-лучевой трубки дисплея можно принимать с помощью специальных приборов на расстоянии до 1000 м.

Аудиоперехват или снятие информации по виброакустическому каналу является опасным и достаточно распространенным способом и имеет две разновидности. Первая заключается в установке подслушивающего устройства в аппаратуру средств обработки информации, вторая — в установке микрофона на инженерно-технические конструкции за пределами охраняемого помещения (стены, оконные рамы, двери и т.п.).

Видеоперехват осуществляется путем использования различной видеооптической техники.

«Уборка мусора» *(scavening)* представляет собой достаточно оригинальный способ перехвата информации. Преступником неправомерно используются технологические отходы информационного процесса, оставленные пользователем после работы с компьютерной техникой. Например, даже удаленная из памяти и с жестких дисков компьютера, а также с дискет информация может быть восстановлена и несанкционированно изъята с помощью специальных программных средств.

К третьей группе способов совершения компьютерных преступлений относятся действия преступника, направленные на получение несанкционированного доступа к информации. В эту группу входят следующие способы.

«Компьютерный абордаж» (hacking) — несанкционированный доступ в компьютер или компьютерную сеть без права на то. Этот способ используется хакерами для проникновения в чужие информационные сети.

Преступление осуществляется чаще всего путем случайного перебора абонентного номера компьютерной системы с использованием модемного устройства. Иногда для этих целей используется специально созданная программа автоматического поиска пароля. Алгоритм ее работы заключается в том, чтобы, учитывая быстродействие современных компьютеров, перебирать все возможные варианты комбинаций букв, цифр и специальных символов и в случае совпадения комбинаций символов производить автоматическое соединение указанных абонентов.

Эксперименты по подбору пароля путем простого перебора показали, что 6-символьные пароли подбираются примерно за 6 дней непрерывной работы компьютера. Элементарный подсчет свидетельствует о том, что уже для подбора 7-символьных паролей потребуется от 150 дней для английского языка и до 200 дней для русского. А если учитывать регистр букв, то эти числа надо умножить еще на 2. Таким образом, простой перебор представляется чрезвычайно трудновыполнимым.

Поэтому в последнее время преступниками стал активно использоваться метод «интеллектуального перебора», основанный на подборе предполагаемого пароля, исходя из заранее определенных тематических групп его принадлежности. В этом случае *программе-взломщику* передаются некоторые исходные данные о личности автора пароля. По оценкам специалистов, это позволяет более чем на десять порядков сократить количество возможных вариантов перебора символов и на столько же — время на подбор пароля.

Практика расследования компьютерных преступлений свидетельствует о том, что взломанные хакерами пароли оказывались

на удивление простыми. Среди них встречались такие как: 7 букв «А»; имя или фамилия автора или его инициалы; несколько цифр, например, «57»; даты рождения, адреса, телефоны или их комбинации.

Одно из громких компьютерных преступлений было совершено группой петербургских программистов. Несколько жителей г. Санкт-Петербурга с компьютера, стоящего в квартире одного из них, проникли в базу данных известной канадско-американской информационной компьютерной сети Sprint Net.

Российские хакеры действовали по накатанному пути. Узнав телефонный номер входа в информационную сеть, они написали оригинальную программу эффективного подбора паролей и с ее помощью узнали коды входа в Sprint Net. Используя их, они получили доступ к конфиденциальным базам данных американских и канадских клиентов.

Не удалось установить, какие конкретно цели преследовали хакеры, поскольку воспользоваться ценной коммерческой информацией они не успели. Никакой ответственности за свои действия хакеры не понесли. Единственным «наказанием» для них стала оплата сетевого времени, затраченного на вскрытие компьютерной системы и перебор паролей.

«Успехи» хакеров настолько велики, что США, например, намерены использовать их в информационной войне. С момента официального признания в 1993 г. военно-политическим руководством США «информационной войны» в качестве одной из составляющих национальной военной стратегии, ускоренными темпами идут поиски методов, форм и средств ее ведения. Так, в последние годы все чаще говорят о целесообразности привлечения хакеров на различных стадиях «информационной войны».

Хакеры наиболее эффективно могут быть использованы на этапе сбора разведывательной информации и сведений о компьютерных сетях и системах вероятного противника. Они уже накопили достаточный опыт в угадывании и раскрытии паролей, использовании слабых мест в системах защиты, обмане законных пользователей и вводе вирусов, «троянских коней» и т.п. в программное обеспечение компьютеров. Искусство проникновения в компьютерные сети и системы под видом законных пользователей дает хакерам возможность стирать все следы своей деятельности, что имеет большое значение для успешной разведывательной деятельности. Имитация законного пользователя дает возможность хакеру-разведчику сформировать систему слежения в сети противника на правах законного пользователя информации.

Не менее эффективным может быть применение опыта хакеров в электронной войне при решении задач дезинформирования и пропаганды через информационные системы и сети противника. Для хакеров не составляет проблемы манипулирование данными,

находящимися в базах данных противника. Им также нетрудно лишить противника возможности доступа к жизненно важным информационным ресурсам. Для этого могут использоваться способы загрузки информационных систем большим количеством сообщений, передаваемых по электронной почте, или же заражение систем противника компьютерными вирусами.

По сообщениям зарубежных СМИ, проблема использования хакеров в интересах информационной войны в настоящее время не ограничивается только изучением их опыта, но и реализуется на практике. Спецслужбы США и некоторых европейских стран уже прибегают к услугам этой категории компьютерных «специалистов».

• *«За дураком» (piggybacking).* Этот способ используется преступником путем подключения компьютерного терминала к каналу связи через коммуникационную аппаратуру в тот момент времени, когда сотрудник, отвечающий за работу средства компьютерной техники, кратковременно покидает свое рабочее место, оставляя терминал в активном режиме.

• *«За хвост» (between-the-lines entry).* При этом способе съема информации преступник подключается к линии связи законного пользователя и дожидается сигнала, обозначающего конец работы, перехватывает его и осуществляет доступ к системе.

• *«Неспешный выбор» (browsing).* При данном способе совершения преступления преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите.

Этот способ чрезвычайно распространен среди хакеров. *В Internet* и других глобальных компьютерных сетях идет постоянный поиск, обмен, покупка и продажа взломанных хакерами программ. Существуют специальные телеконференции, в которых проходит обсуждение программ-взломщиков, вопросов их создания и распространения.

• *«Брешь» (trapdoor entry).* В отличие от «неспешного выбора», когда производится поиск уязвимых мест в защите компьютерной системы, при данном способе преступником осуществляется конкретизация поиска: ищутся участки программ, имеющие ошибку или неудачную логику построения. Выявленные таким образом «бреши» могут использоваться преступником многократно, пока не будут обнаружены законным пользователем.

• *«Люк» (trapdoor).* Данный способ является логическим продолжением предыдущего. В месте найденной «бреши» программа «разрывается» и преступником туда дополнительно вводится одна или несколько команд. Такой «люк» «открывается» по необходимости, а включенные команды автоматически выполняются.

Люки часто бывают оставлены самими создателями программ, иногда с целью внесения возможных изменений. Подобные *«чер-*

ные входы» в защищенную систему обычно имеются в любой сертифицированной программе, но об этом не принято распространяться вслух.

В качестве примера можно привести компьютерную систему управления самолетов «Мираж». Во время войны в Персидском заливе ее «стопроцентная» защита от несанкционированного доступа была сломана одним кодовым сигналом, пущенным в обход системы защиты. Бортовые системы самолетов были отключены, и Ирак остался без авиации.

К четвертой группе способов совершения компьютерных преступлений относятся действия преступников, связанные с использованием методов манипуляции данными и управляющими командами средств компьютерной техники. Эти методы наиболее часто используются преступниками для совершения различного рода противоправных деяний и достаточно хорошо известны сотрудникам подразделений правоохранительных органов, специализирующихся на борьбе с компьютерными преступлениями.

Наиболее часто встречаются следующие способы совершения компьютерных преступлений, относящихся к этой группе:

• *«Троянский конь» (trojan horse).* Данный способ заключается в тайном введении в чужое программное обеспечение специально созданных программ, которые, попадая в информационно-вычислительные системы, начинают выполнять новые, не планировавшиеся законным владельцем действия, с одновременным сохранением прежних функций. В соответствии со ст. 273 Уголовного кодекса Российской Федерации под такой программой понимается «программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети». По существу, «троянский конь» — это модернизация рассмотренного выше способа «люк» с той лишь разницей, что люк «открывается» не при помощи непосредственных действий преступника, а автоматически, с использованием специально подготовленной для этих целей программы и без непосредственного участия самого преступника. С помощью такого способа преступники обычно отчисляют на заранее открытый счет определенную сумму с каждой банковской операции. Возможен и вариант увеличения преступниками избыточных сумм на счетах при автоматическом пересчете рублевых остатков, связанных с переходом к коммерческому курсу соответствующей валюты. Разновидностями такого способа совершения компьютерных преступлений является внедрение в программы *«логических бомб» {logic bomb)* и *«временных бомб» {time bomb).*

• *компьютерный вирус (virus).* С уголовно-правовой точки зрения, согласно ст. 273 Уголовного кодекса РФ, под компьютерным вирусом следует понимать вредоносную для ЭВМ программу, спо-

собную самопроизвольно присоединяться к другим программам («заражать» их) и при запуске последних выполнять различные нежелательные действия: порчу файлов, искажение, стирание данных и информации, переполнение машинной памяти и создание помех в работе ЭВМ. К этой же группе относят и некоторые другие способы совершения компьютерных преступлений, которые иногда выделяются в самостоятельные группы: компьютерное мошенничество; незаконное копирование. *Компьютерное мошенничество* чаще всего осуществляется способом *«подмены данных» (data digging)* или *«подмены кода» (code change).* Это наиболее простой и поэтому очень часто применяемый способ совершения преступления. Действия преступников в этом случае направлены на изменение или введение новых данных, и осуществляются они, как правило, при вводе-выводе информации. Некоторые из таких способов совершения преступлений возникли и получили распространение только с появлением компьютеров. В качестве примера можно привести перебрасывание на подставной счет мелочи, являющейся результатом округления (операция типа «салями» *(salami)).* Расчет построен на том, что компьютер совершает сотни тысяч операций в секунду и обрабатывает при этом сотни тысяч счетов клиентов. Заниматься подобным мошенничеством вручную не имеет никакого смысла. *Незаконное копирование* (тиражирование) программ с преодолением программных средств защиты предусматривает незаконное создание копии ключевой дискеты, модификацию кода системы защиты, моделирование обращения к ключевой дискете, снятие системы защиты из памяти ЭВМ и т.п.

Не секрет, что подавляющая часть программного обеспечения, используемого в России, представляет собой пиратские копии взломанных хакерами программ. Самой популярной операционной системой в России является Microsoft Windows 95. По статистике, на долю этой платформы приходится свыше 77 % отечественного рынка операционных систем. Своим бесспорным успехом на российском рынке Windows 95 обязана деятельности компьютерных пиратов. По данным международной организации BSA, занимающейся вопросами охраны интеллектуальной собственности, свыше 90 % используемых в России программ установлены на компьютеры без лицензий, тогда как в США таких не более 24%.

В качестве примера незаконного тиражирования программ можно привести и компьютерную базу российского законодательства «КонсультантПлюс». Несмотря на постоянную работу специалистов фирмы по улучшению системы защиты, тысячи нелегальных копий программы имеют хождение на территории России. Последняя, шестая версия «Консультанта», была «привязана» к дате создания компьютера, записанной в его постоянной памяти. Однако не прошло и двух недель после выхода этой версии, как хакерами

была создана программа, эмулирующая нужную дату на любом компьютере. В настоящее время желающий может найти такую программу в компьютерной сети Internet и с ее помощью установить на свой компьютер базу данных по законодательству, стоимость которой превышает 1000 долл. США.

Пятая группа способов — комплексные методы — включает в себя различные комбинации рассмотренных выше способов совершения компьютерных преступлений.

Следует заметить, что рассмотренная выше классификация не является, как уже говорилось выше, единственно возможной. Так, по международной классификации в отдельную группу принято выделять такие способы, как *компьютерный саботаж* с аппаратным или программным обеспечением, которые приводят к выходу из строя компьютерной системы. Наиболее значительные компьютерные преступления совершаются посредством порчи программного обеспечения, причем часто его совершают работники, недовольные своим служебным положением, отношениями с руководством и т.д.

Примером такого компьютерного преступления может служить получивший широкую огласку случай с программистом, остановившим главный конвейер Волжского автозавода в г. Тольятти. Занимаясь отладкой программного кода автоматизированной системы, управляющей подачей механических узлов на конвейер, он умышленно внес изменения в программу. В результате, после прохождения заданного числа деталей система «зависала» и конвейер останавливался. Пока программисты устраняли источник сбоев, с конвейера автозавода сошло не более двухсот машин.

Существует также ряд способов совершения преступлений, которые крайне сложно отнести к какой либо группе. К таким способам относятся асинхронная атака, моделирование, мистификация, маскарад и т.д.

Асинхронная атака (Asynchronous attack). Сложный способ, требующий хорошего знания операционной системы. Используя асинхронную природу функционирования большинства операционных систем, их заставляют работать при ложных условиях, из-за чего управление обработкой информации частично или полностью нарушается. Если лицо, совершающее «асинхронную атаку», достаточно профессионально, оно может использовать ситуацию, чтобы внести изменения в операционную систему или сориентировать ее на выполнение своих целей, причем извне эти изменения не будут заметны.

Моделирование (Simulation). Создается модель конкретной системы, в которую вводятся исходные данные и учитываются планируемые действия. На основании полученных результатов методом компьютерного перебора и сортировки выбираются возможные подходящие комбинации. Затем модель возвращается к исходной

точке и выясняется, какие манипуляции с входными данными нужно проводить для получения на выходе желаемого результата. В принципе, «прокручивание» модели вперед-назад может происходить многократно, чтобы через несколько итераций добиться необходимого итога. После этого остается осуществить задуманное на практике.

Мистификация {spoofing). Возможна, например, в случаях, когда пользователь удаленного терминала ошибочно подключается к какой-либо системе, будучи абсолютно уверенным, что работает именно с той самой системой, с которой намеревался. Владелец системы, к которой произошло подключение, формируя правдоподобные отклики, может поддержать контакт в течение определенного времени и получать конфиденциальную информацию, в частности коды пользователя и т.д.

9.3. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Можно выделить следующие типичные преступные *цели* совершения компьютерных преступлений:

• хищение денег (подделка счетов и платежных ведомостей, фальсификация платежных документов, вторичное получение уже произведенных выплат, перечисление денег на подставные счета и т.д.);

• приписка сверхурочных часов работы;

• хищение вещей (совершение покупок с фиктивной оплатой, добывание запасных частей и редких материалов);

• хищение машинной информации;

• внесение изменений в машинную информацию;

• кража машинного времени;

• подделка документов (получение фальшивых дипломов, фиктивное продвижение по службе);

• несанкционированная эксплуатация системы;

• саботаж;

• шпионаж (политический и промышленный).

Мотивами совершения компьютерных преступлений, как показали исследования зарубежных и российских исследователей, являются следующие[1]:

• корыстные соображения — 66,%;

• политические цели — 17%;

• исследовательский интерес — 7%;

• хулиганство — 5%;

• месть — 5%.

[1] *Вехов В. Б.* Компьютерные преступления. — М.: Право и Закон, 1996.

Для подавляющего большинства преступлений характерны корыстные мотивы — это 52 % всех компьютерных преступлений; с разрушением и уничтожением средств компьютерной техники сопряжено 16% преступлений, с подменой исходных данных — 12%, с хищением данных и программ — 10%, с хищением услуг — 10%[1]. В этой связи интересными представляются результаты опроса, проведенного в 1988 г. среди 1600 специалистов по информационной безопасности в 50 странах мира[2].

Результаты опроса свидетельствуют, что самой распространенной угрозой безопасности были компьютерные вирусы — важнейшим этот тип угрозы назвали 60% опрошенных. В 1991 и 1992 гг. эти цифры составляли 22 и 44% соответственно.

Что касается финансовых потерь из-за нарушений в области защиты информации, то в полном их отсутствии уверены 28% опрошенных. Среди тех, кто признает наличие таких потерь, их доли распределились так, как показано на диаграмме:

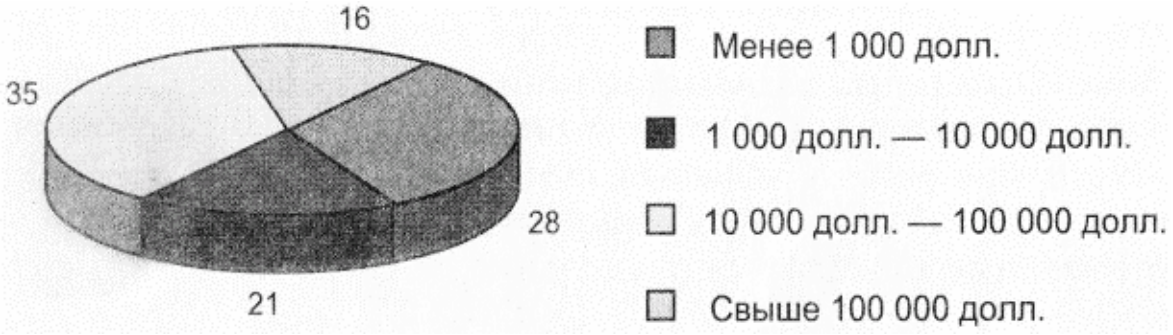

Рис. 9.1. Финансовые потери в результате нарушений безопасности (%)

Опрос показал также, что основная часть угроз по-прежнему исходит от персонала компаний. На то, что хотя бы один из авторизованных пользователей был уличен в компьютерном злоупотреблении, указало 58 % респондентов (в 1991 г. 75 %). Опасность от внешних злоумышленников не так велика, как это представляется средствами массовой информации. Неавторизованные пользователи проникали в корпоративные сети только в 24% случаев. Поставщики и покупатели являлись источниками атак лишь в 12% случаев.

В этой связи особый интерес приобретает характеристика личности преступника. С криминалистической точки зрения можно выделить несколько самостоятельных обособленных групп компьютерных преступников.

К первой группе можно отнести лиц, сочетающих определенные черты профессионализма с элементами изобретательности и развлечения. Такие люди, работающие с компьютерной техникой, весьма любознательны, обладают острым умом, а также склонно-

---

[1] *Вехов В. Б.* Компьютерные преступления. - М.: Право и Закон, 1996. - С. 42.

[2] PC WEEK/RE. № 1, 19 января, 1999.

стью к озорству. Они воспринимают меры по обеспечению безопасности компьютерных систем как вызов своему профессионализму и стараются найти технические пути, которые доказали бы их собственное превосходство. При этом они не прочь поднять свой престиж, похвастаться перед коллегами умением найти слабости в компьютерной системе защиты, а иногда и продемонстрировать, как эти слабости можно использовать. Постепенно они набирают опыт, приобретают вкус к такого рода деятельности и пытаются совмещать свои занятия с получением некоторой материальной выгоды. Такой путь проходит большинство хакеров.

Вторую группу составляют лица, страдающие особого рода информационными болезнями, развившимися на почве взаимодействия со средствами компьютерной техники.

Компьютерные системы действуют на основе строго определенных правил и алгоритмов, ограниченных рамками задачи. Человек часто руководствуется чувствами, старается пояснить свою цель, аргументировать постановку задачи, ввести при необходимости новые данные и т.п. Некоторые люди попадают в такие ситуации, когда не могут адаптироваться к требованиям современной компьютерной технологии. У них развивается болезненная реакция, приводящая к неадекватному поведению. Чаще всего она трансформируется в особый вид компьютерного преступления — *компьютерный вандализм.*

Обычно он принимает форму физического разрушения компьютерных систем, их компонентов или программного обеспечения. Часто этим занимаются из чувства мести уволенные сотрудники, а также люди, страдающие компьютерными неврозами.

К третьей группе, представляющей наибольший интерес, относятся специалисты или профессиональные компьютерные преступники. Эти лица обладают устойчивыми навыками, действуют расчетливо, маскируют свои действия, всячески стараются не оставлять следов. Цели их преимущественно корыстные. Особенно опасно, если лица такой направленности оказываются среди сотрудников организации или среди авторизованных пользователей информационной системы.

В 1998 г. в Экспертно-криминалистическом центре МВД был проведен классификационный анализ лиц, замешанных в применении компьютеров для совершения противоправных деяний. Обобщенный портрет отечественного хакера, созданный на основе уголовного преследования такого рода лиц, выглядит примерно так: это мужчина в возрасте от 15 до 45 лет, либо имеющий многолетний опыт работы на компьютере, либо, напротив, почти не обладающий таким опытом; в прошлом к уголовной ответственности не привлекался; является яркой, мыслящей личностью, способной принимать ответственные решения; хороший, добросовестный работник, по характеру нетерпим к насмешкам и к потере

своего социального статуса в рамках группы окружающих его людей; любит уединенную работу; приходит на службу первым и уходит последним; часто задерживается на работе после окончания рабочего дня и очень редко использует отпуска и отгулы.

Существенную роль в структуре криминалистической характеристики компьютерных преступлений играют также *сведения о потерпевшей стороне.* Изучение жертв компьютерных преступлений часто дает больше информации для решения вопросов компьютерной безопасности, чем изучение лиц, совершающих компьютерные преступления. По опубликованным данным, относящимся к группе развитых стран, среди жертв собственники системы составляли 79%; клиенты — 13%; третьи лица — 8%[1].

Организации-жертвы компьютерных преступлений с неохотой сообщают об этом в правоохранительные органы. Латентность компьютерных преступлений чрезвычайно высока. Часто виновные лица просто увольняются или переводятся в другие структурные подразделения. Иногда с виновного взыскивается ущерб в гражданском порядке. Принимая решение, жертва компьютерного преступления руководствуется одним или несколькими из указанных ниже факторов:

• компьютерный преступник, как правило, не рассматривается как типичный уголовный преступник;

• расследование компьютерных преступлений может нарушить нормальное функционирование организации, привести к приостановке ее деятельности;

• расследование компьютерных преступлений, в том числе и силами самой фирмы, является делом весьма дорогостоящим;

• будучи разоблаченными, компьютерные преступники в большинстве случаев отделываются легкими наказаниями, зачастую условными — для пострадавших это является одним из аргументов за то, чтобы не заявлять о преступлении;

• законодательство не всегда применимо к компьютерным преступлениям, что приводит к серьезным затруднениям при правильной их квалификации;

• правоохранительные органы не склонны относить многие из компьютерных правонарушений к категории преступлений и, соответственно, отказывают в возбуждении уголовного дела;

• компьютерный преступник воспринимается как незаурядная личность;

• жертва боится серьезного, компетентного расследования, так как оно может вскрыть неблаговидную, если не незаконную, механику ведения дел в организации;

• расследование компьютерных преступлений может выявить несостоятельность мер безопасности, принимаемых ответствен-

---

[1] PC WEEK/RE. № 1, 19 января, 1999.

ным за них персоналом организации, привести к нежелательным осложнениям, постановке вопросов о профессиональной пригодности и т.д.;

• опасение увеличения размеров страховых взносов, если компьютерные преступления становятся для организации регулярными;

• боязнь потери клиентов вследствие утраты репутации;

• раскрытие компьютерных преступлений сопряжено, как правило, с открытием финансовых, коммерческих и других служебных тайн, которые могут стать достоянием гласности во время судебного рассмотрения дел.

Вопросы предотвращения и раскрытия компьютерных преступлений сегодня касаются каждой организации. Важно, чтобы администрация хорошо понимала, какие условия делают возможными такие посягательства. Руководителям не обязательно быть экспертами в области информационной безопасности, но они должны четко представлять себе возможные проблемы и последствия, связанные с потерей критичной информации.

Существует много косвенных признаков того, что в организации, учреждении готовится или осуществляется компьютерное преступление. Выявление указанных признаков не требует специальных знаний и, учитывая это обстоятельство, можно предусмотреть дополнительные меры по совершенствованию компьютерной безопасности и предотвращению преступлений.

Наиболее общие индикаторы выглядят следующим образом: сотрудники дают подозрительные объяснения по поводу распределения денежных и материальных средств; производится перезапись данных без серьезных на то причин; данные заменяются, изменяются или стираются; данные не обновляются; на ключевых документах появляются подделанные подписи; появляются фальшивые записи; персонал системы без видимых на то оснований начинает работать сверхурочно; персонал возражает против осуществления контроля за записью данных; у работников, непосредственно работающих с компьютерами, появляется ненормальная реакция на рутинные вопросы; некоторые сотрудники отказываются уходить в отпуск; отдельные работники начинают слоняться без дела в других подразделениях; жалобы клиентов становятся хроническими и др.

9.4. ТЕНДЕНЦИИ РАЗВИТИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В РОССИИ

Уровень компьютерной преступности определяется во многом объективными причинами и напрямую зависит от общего уровня информатизации общества. Большинством зарубежных и отечественных исследователей отмечается отставание России в вопросах компьютеризации от развитых стран в среднем на 20 лет. Если в США

первое компьютерное преступление было зафиксировано в 1966 г., то в бывшем СССР — в 1979 г. Поэтому тенденции развития компьютерной преступности в России могут заметно отличаться от таковых в развитых странах. По мнению экспертов в данной области, следует прежде всего ожидать значительного количественного роста компьютерных преступлений. Этому способствует ряд причин, среди которых основными можно считать: во-первых, резкий рост безработицы и падение уровня жизни среди так называемой «беловоротничковой» прослойки населения на фоне общего экономического кризиса и кризиса неплатежей; во-вторых, массовая неконтролируемая компьютеризация и использование новейших электронных средств во всех сферах деятельности, прежде всего финансовых, банковских и кредитных учреждениях всех форм собственности; в-третьих, отсутствие соответствующей правовой базы, препятствующей в сколько-нибудь заметной мере распространению и пресечению компьютерных преступлений. Если в США на сегодня действует более 2000 законов и подзаконных актов, в той или иной мере касающихся компьютерных преступлений и связанных с ними явлений, а аналогичные нормы действуют также в ФРГ, Великобритании и Франции, то в России их число не превышает и 10, включая рассмотренные выше три статьи нового Уголовного Кодекса РФ.

На наш взгляд, преимущественное внимание на фоне ожидаемого количественного роста компьютерных преступлений следует обратить на выявление качественных изменений и основных тенденций развития компьютерной преступности в России с целью их возможной профилактики и пресечения. К таким тенденциям можно отнести следующие:

• перенос центра тяжести на совершение компьютерных преступлений с использованием компьютерных сетей, что вызвано широким применением межбанковской системы электронных платежей и компьютерных систем связи, в рамках которой, по различным оценкам, совершается около 40 % всех банковских операций в России;

• преимущественный рост компьютерных преступлений, совершаемых в сфере экономики и денежного обращения, к которым относятся финансовые хищения, мошенничества, подлоги и т.д. Это вызвано прежде всего большим количеством финансовых средств, находящихся в данной сфере при отсутствии надежных средств защиты информации и устойчивой дезорганизации платежной системы России;

• перерастание компьютерной преступности в разряд транснациональных преступлений, чему способствует относительная легкость преодоления систем защиты в компьютерных сетях и доступа к коммерческим секретам крупнейших мировых корпораций и банков, включая всемирную компьютерную сеть Internet. Компью-

терные преступления позволяют наиболее простым способом отмывать «грязные» капиталы (наркобизнес, незаконный оборот оружия и др.) и переводить крупные суммы денег на оффшорные счета за рубежом;

• существенное омоложение в ближайшие годы компьютерной преступности за счет притока молодого поколения профессионалов-компьютерщиков, чему способствует раннее знакомство учащейся молодежи с компьютерами, понимание их роли в современном обществе и отсутствие при этом устойчивых моральных принципов;

• одна из самых опасных тенденций — сращивание компьютерной преступности с организованной преступностью. Современные компьютерные преступления носят в своей массе организованный характер, требуют специальной подготовки и больших материальных и финансовых затрат на их проведение. Интеграция в международные преступные сообщества и коррупция в среде должностных лиц также способствуют этому положению;

• значительный количественный рост, особенно характерного для России такого вида компьютерных преступлений, как кражи и незаконное тиражирование программного обеспечения, что является следствием массовой компьютеризации при сложившейся психологии потребителей российского компьютерного рынка. По некоторым оценкам специалистов, доля «пиратского» программного обеспечения составляет около 95 % и не имеет пока тенденции к сокращению (для сравнения, его доля в США не превышает 30%);

• рост такого вида компьютерных преступлений, как незаконное пользование услугами телефонных и телекоммуникационных компаний в России. К этому приводит широкое распространение модемной связи при существовании высоких цен на данные виды услуг. Так например, одна их крупнейших компаний США «America On Line» вынуждена была отказать в предоставлении услуг российским пользователям ввиду многочисленных случаев неуплаты и махинаций в Сети, приносивших многомиллионные убытки компании и ее пользователям в других странах;

• появление и распространение таких компьютерных преступлений, как компьютерный экономический и политический шпионаж, шантаж и преступления против личности, чему способствует повсеместная компьютеризация атомной энергетики, здравоохранения, систем транспорта и оборонной промышленности, в особенности ракетной сферы;

• появление таких новых для России видов компьютерных преступлений, как например, кража и подделка кредитных карточек.

Среди положительных тенденций можно прогнозировать сокращение числа краж собственно компьютерной техники и периферии, ввиду существенного падения цен на них и относительной

доступности, а также сокращение незаконного использования машинных ресурсов и машинного времени.

На современном этапе развития ИТ в России назрела необходимость детального изучения проблемы основ криминалистического исследования компьютерной преступности. Следует отметить, что при совершении компьютерных преступлений, так же как и при совершении любых других общеизвестных видов преступлений, остаются «следы», обнаружение, фиксация и исследование которых является непременным условием при расследовании и раскрытии как данного вида преступлений, так и в борьбе с «техногенной» преступностью в целом.

9.5. КОМПЬЮТЕРНЫЕ ВИРУСЫ

Общие сведения. Пользователи ПК наиболее часто сталкиваются с одной из разновидностей компьютерной преступности — компьютерными вирусами. Последние являются особого типа вредоносными программами, доставляющими пользователям и обслуживающему ПК персоналу немало неприятностей[1].

Компьютерным вирусом называется способная к самовоспроизводству и размножению программа, внедряющаяся в другие программы.

Очевидна аналогия понятий компьютерного и биологического вирусов. Однако не всякая могущая саморазмножаться программа является компьютерным вирусом. *Вирусы всегда наносят ущерб* — препятствуют нормальной работе ПК, разрушают файловую структуру и т.д., поэтому их относят к разряду так называемых вредоносных программ.

Исторически появление компьютерных вирусов связано с идеей создания самовоспроизводящихся механизмов, в частности программ, которая возникла в 50-х гг. Дж.фон Нейман еще в 1951 г. предложил метод создания таких механизмов, и его соображения получили дальнейшее развитие в работах других исследователей. Первыми появились игровые программы, использующие элементы будущей вирусной технологии, а затем уже на базе накопленных научных и практических результатов некоторые лица стали разрабатывать самовоспроизводящиеся программы с целью нанесения ущерба пользователям компьютера.

Создатели вирусов сосредоточили свои усилия в области ПК вследствие их массовости и практически полного отсутствия эффективных средств защиты как на аппаратном уровне, так и на уровне ОС. Среди побудительных мотивов, движущих авторами вирусов, можно назвать следующие:

• стремление «насолить» кому-либо;

---

[1] *Безруков Н.Н.* Компьютерные вирусы. — М.: Наука, 1991.

• неестественная потребность в совершении преступлений;

• желание самоутвердиться, озорство и одновременно недопонимание всех последствий распространения вируса;

• невозможность использовать свои знания в конструктивном русле (это в большей степени экономическая проблема);

• уверенность в полной безнаказанности (в ряде стран отсутствуют нормы правовой ответственности за создание и распространение вирусов).

Основными каналами проникновения вирусов в персональный компьютер являются накопители на сменных носителях информации и средства сетевой коммуникации, в частности сеть Internet.

Первые случаи массового заражения ПК вирусами были отмечены в 1987 г., когда появился так называемый Пакистанский вирус, созданный братьями Амджатом и Базитом Алви. Таким образом они решили наказать американцев, покупавших дешевые незаконные копии программного обеспечения в Пакистане, которые братья стали инфицировать разработанным вирусом. Вирус заразил в США более 18 тыс. компьютеров и, проделав кругосветное путешествие, попал в СССР. Следующим широко известным вирусом стал вирус Lehigh (Лехайский вирус), распространившийся в одноименном университете США. В течение нескольких недель он уничтожил содержимое нескольких сотен дискет из библиотеки вычислительного центра университета и личных дискет студентов. К февралю 1989 г. в США этим вирусом было поражено около 4 тыс. ПК.

В дальнейшем количество вирусов и число зараженных ими компьютеров стало лавинообразно увеличиваться, что потребовало принятия срочных мер как технического, так и организационного и юридического характера. Появились различные антивирусные средства, вследствие чего ситуация стала напоминать гонку вооружений и средств защиты от них. Определенный эффект был достигнут в результате принятия рядом развитых стран законодательных актов о компьютерных преступлениях, среди которых были и статьи, касающиеся создания и распространения компьютерных вирусов.

В настоящее время в мире насчитывается более 20 тыс. вирусов, включая штаммы, т.е. разновидности вирусов одного типа. Вирусы не признают границ, поэтому большинство из них курсирует и по России. Более того, проявилась тенденция увеличения числа вирусов, разработанных отечественными программистами. Если ситуация не изменится, то в будущем Россия сможет претендовать на роль лидера в области создания вирусов.

Классификация вирусов. Жизненный цикл компьютерных вирусов, как правило, включает в себя следующие фазы:

• латентный период, в течение которого вирусом никаких действий не предпринимается;

• инкубационный период, в пределах которого вирус только размножается;

• активный период, в течение которого наряду с размножением выполняются несанкционированные действия, заложенные в алгоритме вируса.

Первые две фазы служат для того, чтобы скрыть источник вируса, канал его проникновения и инфицировать как можно больше файлов до выявления вируса. Длительность этих фаз может определяться предусмотренным в алгоритме временным интервалом, наступлением какого-либо события в системе, наличием определенной конфигурации аппаратных средств ПК (в частности, наличием НЖМД) и т.д.

Компьютерные вирусы классифицируются в соответствии со следующими признаками:

• средой обитания;

• способом заражения среды обитания;

• способом активизации;

• способом проявления (деструктивные действия или вызываемые эффекты);

• способом маскировки.

Вирусы могут внедряться только в программы, которые, в свою очередь, могут содержаться или в файлах, или в некоторых компонентах системной области диска, участвующих в процессе загрузки операционной системы. В соответствии со *средой обитания* различают:

• *файловые* вирусы, инфицирующие исполняемые файлы;

• *загрузочные* вирусы, заражающие компоненты системной области, используемые при загрузке ОС;

• *файлово-загрузочные* вирусы, интегрирующие черты первых двух групп.

Файловые вирусы могут инфицировать:

• позиционно-независимые перемещаемые машинные программы находящиеся в COM-файлах;

• позиционно-зависимые перемещаемые машинные программы, размещаемые в EXE-файлах;

• драйверы устройств (SYS- и BIN-файлы);

• файлы с компонентами DOS;

• объектные модули (OBJ-файлы);

• файлы с программами на языках программирования (в расчете на компиляцию этих программ);

• командные файлы (BAT-файлы);

• объектные и символические библиотеки (LIB- и другие файлы);

• оверлейные файлы (OVL-, PIF- и другие файлы). Наиболее часто файловые вирусы способны внедряться в COM

и/или EXE-файлы.

Загрузочные вирусы могут заражать:

• загрузочный сектор на дискетах;

• загрузочный сектор системного логического диска, созданного на винчестере;

• внесистемный загрузчик на жестком диске. Загрузочные вирусы распространяются на дискетах в расчете на

то, что с них будет осуществлена попытка загрузиться, что происходит не так часто. У файловых вирусов инфицирующая способность выше.

Файлово-загрузочные вирусы обладают еще большей инфицирующей способностью, так как могут распространяться как в программных файлах, так и на дискетах с данными.

Способы заражения среды обитания, зависят от типа последней. Зараженная вирусом среда называется вирусоносителем. При имплантации тело файлового вируса может размещаться:

• в конце файла;

• в начале файла;

• в середине файла;

• в хвостовой (свободной) части последнего кластера, занимаемого файлом.

Наиболее легко реализуется внедрение вируса в конец COM-файла. При получении управления вирус выбирает файл-жертву и модифицирует его следующим образом:

1. Дописывает к файлу собственную копию (тело вируса).

2. Сохраняет в этой копии оригинальное начало файла.

3. Заменяет оригинальное начало файла на команду передачи управления на тело вируса.

При запуске инфицированной описанным способом программы первоначально инициируется выполнение тела вируса, в результате чего:

• восстанавливается оригинальное начало программы (но не в файле, а в памяти!);

• возможно, отыскивается и заражается очередная жертва;

• возможно, осуществляются несанкционированные пользователем действия;

• производится передача управления на начало программы-вирусоносителя, в результате чего она выполняется обычным образом.

Имплантация вируса в начало COM-файла производится иначе: создается новый файл, являющийся объединением тела вируса и содержимого оригинального файла. Два описанных способа внедрения вируса ведут к увеличению длины оригинального файла.

Имплантация вируса в середину файла наиболее сложна и специализирована. Сложность состоит в том, что в этом случае вирус должен «знать» структуру файла-жертвы (например, command.com), чтобы можно было внедриться, в частности, в область стека. Описанный способ имплантации не ведет к увеличению длины файла.

Проявлением (деструктивными действиями) вирусов могут быть:

• влияние на работу ПК;

• искажение программных файлов;

• искажение файлов с данными;

• форматирование диска или его части;

• замена информации на диске или его части;

• искажения системного или несистемного загрузчика диска;

• разрушение связности файлов путем искажения таблицы FAT;

• искажение данных в CMOS-памяти.

Большую часть вирусов первой группы, вызывающих визуальные или звуковые эффекты, неформально называют «иллюзионистами». Другие вирусы этой же группы могут замедлять работу ПК или препятствовать нормальной работе пользователя, модифицируя и блокируя функции выполняемых программ, а также операционной системы. Вирусы всех остальных групп часто называют «вандалами» из-за наносимого ими непоправимого, как правило, ущерба.

В соответствии со *способами маскировки* различают:

• немаскирующиеся вирусы;

• самошифрующиеся вирусы;

• стелс-вирусы.

Авторы первых вирусов уделяли особое внимание механизмам размножения (репликации) с внедрением тел в другие программы. Маскировка же от антивирусных средств не осуществлялась. Такие вирусы называются немаскирующимися.

В связи с появлением антивирусных средств разработчики вирусов сосредоточили усилия на обеспечении маскировки своих изделий. Сначала была реализована идея самошифрования вируса. При этом лишь небольшая его часть является доступной для осмысленного чтения, а остальная расшифровывается непосредственно перед началом работы вируса. Такой подход затрудняет как обнаружение вируса, так и анализ его тела специалистами.

Появились также стелс-вирусы, названные по аналогии с широкомасштабным проектом по созданию самолетов-невидимок. Методы маскировки, используемые стелс-вирусами, носят комплексный характер, и могут быть условно разделены на две категории: маскировка наличия вируса в программе-вирусоносителе; маскировка присутствия резидентного вируса в ОЗУ.

К первой категории относятся:

• автомодификация тела вируса;

• реализация эффекта удаления тела вируса из вирусоносителя при чтении последнего с диска, в частности, отладчиком (это осуществляется путем перехвата прерывания, конечно, в случае наличия резидентного вируса в ОЗУ);

• имплантация тела вируса в файл без увеличения его размера;

• эффект неизменности длины инфицированного файла (осуществляется аналогично п. 2);

• сохранение неизменным оригинального начала программных файлов.

Например, при чтении каталога средствами DOS резидентный вирус может перехватить соответствующее прерывание и искусственно уменьшить длину файла. Конечно, реальная длина файла не меняется, но пользователю выдаются сведения, маскирующие ее увеличение. Работая же с каталогами непосредственно (в обход средств DOS), можно получить истинную информацию о характеристиках файла. Такие возможности предоставляет, в частности, оболочка Norton Commander.

Ко второй категории методов маскировки можно отнести:

• занесение вируса в специальную зону резидентных модулей DOS, в хвостовые части кластеров, в CMOS-память, видеопамять и т.п.;

• модификацию списка несистемного загрузчика, о чем уже говорилось;

• манипулирование обработчиками прерываний, в частности, специальные методы их подмены, с целью обойти резидентные антивирусные средства;

• корректировку общего объема ОЗУ.

При повседневной работе пользователь в состоянии обнаружить вирус *по его симптомам.* Естественно, что симптомы вируса непосредственно определяются реализованными в нем способами проявления, а также другие характеристиками вируса. В качестве симптомов вирусов выделяют следующие:

• увеличение числа файлов на диске;

• уменьшение объема свободной оперативной памяти;

• изменение времени и даты создания файла;

• увеличение размера программного файла;

• появление на диске зарегистрированных дефектных кластеров;

• ненормальная работа программы;

• замедление работы программы;

• загорание лампочки дисковода в то время, когда не должны происходить обращения к диску;

• заметное возрастание времени доступа к жесткому диску;

• сбои в работе операционной системы, в частности, ее зависание;

• невозможность загрузки операционной системы;

• разрушение файловой структуры (исчезновение файлов, искажение каталогов).

Наряду с компьютерными вирусами существуют и другие опасные программы, например, так называемые «черви», формально именуемые *репликаторами.* Их основная особенность состоит в способности к размножению без внедрения в другие программы. Репликаторы создаются с целью распространения по узлам вычислительной сети и могут иметь начинку, состоящую, в частности, из вирусов. В этом отношении можно провести аналогию между «червем» и шариковой бомбой.

Примером репликатора является программа Christmas Tree, рисующая на экране дисплея рождественскую елку, а затем рассылающая свои копии по всем адресам, зарегистрированным средствами электронной почты.

Классификация антивирусных средств. В настоящее время имеется большое количество антивирусных средств. Однако все они не обладают свойством универсальности: каждое рассчитано на конкретные вирусы либо перекрывает некоторые каналы заражения ПК или распространения вирусов. В связи с этим перспективной областью исследований можно считать применение методов искусственного интеллекта к проблеме создания антивирусных средств.

Антивирусным средством называют программный продукт, выполняющий одну или несколько из следующих функций:

• защиту файловой структуры от разрушения;

• обнаружение вирусов;

• нейтрализацию вирусов.

Вирус-фильтром (сторожем) называется резидентная программа, обеспечивающая контроль выполнения характерных для вирусов действий и требующая от пользователя подтверждения на производство действий. Контроль осуществляется путем подмены обработчиков соответствующих прерываний. В качестве контролируемых действий могут выступать:

• обновление программных файлов;

• прямая запись на диск (по физическому адресу);

• форматирование диска;

• резидентное размещение программы в ОЗУ. *Детектором* называется программа, осуществляющая поиск

вирусов как на внешних носителях информации, так и в ОЗУ. Результатом работы детектора является список инфицированных файлов и/или областей, возможно, с указанием конкретных вирусов, их заразивших.

Детекторы делятся на универсальные (ревизоры) и специализированные. *Универсальные* детекторы проверяют целостность файлов путем подсчета контрольной суммы и ее сравнения с эталоном. Эталон либо указывается в документации на программный продукт, либо может быть определен в самом начале его эксплуатации.

Специализированные детекторы настроены на конкретные вирусы, один или несколько. Если детектор способен обнаруживать несколько различных вирусов, то его называют *полидетектором.* Работа специализированного детектора основывается на поиске строки кода, принадлежащей тому или иному вирусу, возможно заданной регулярным выражением. Такой детектор не способен обнаружить все возможные вирусы.

Дезинфектором (доктором, фагом) называется программа, осуществляющая удаление вируса как с восстановлением, так и без

восстановления среды обитания. Ряд вирусов искажает среду обитания таким образом, что ее исходное состояние не может быть восстановлено.

Наиболее известными полидетекторами-фагами являются программные пакеты Antiviral Toolkit Pro Евгения Касперского и DrWeb фирмы Диалог.

Иммунизатором (вакциной) называют программу, предотвращающую заражение среды обитания или памяти конкретными вирусами. Иммунизаторы решают проблему нейтрализации вируса не посредством его уничтожения, а путем блокирования его способности к размножению. Такие программы в настоящее время практически не используются.

Методы защиты от компьютерных вирусов. При защите от компьютерных вирусов как никогда важна комплексность проводимых мероприятий как организационного, так и технического характера. На переднем крае «обороны» целесообразно разместить средства защиты данных от разрушения, за ними — средства обнаружения вирусов и, наконец, средства нейтрализации вирусов.

Средства защиты данных от возможной потери и разрушения должны использоваться всегда и регулярно. Дополнительно к этому следует придерживаться следующих рекомендаций организационного характера, чтобы избавиться от заражения вирусами:

• гибкие диски использовать всегда, когда это возможно, с заклеенной прорезью защиты от записи;

• без крайней необходимости не пользоваться неизвестными дискетами;

• не передавать свои дискеты другим лицам;

• не запускать на выполнение программы, назначение которых непонятно; использовать только лицензионные программные продукты;

• ограничить доступ к ПК посторонних лиц.

При необходимости использования программного продукта, полученного из неизвестного источника, рекомендуется:

• протестировать программный продукт специализированными детекторами на предмет наличия известных вирусов. Нежелательно размещать детекторы на жестком диске — для этого нужно использовать защищенную от записи дискету;

• осуществить резервирование файлов нового программного продукта;

• провести резервирование тех своих файлов, наличие которых требуется для работы нового программного обеспечения;

• организовать опытную эксплуатацию нового программного продукта на фоне вирус-фильтра с обдуманными ответами на его сообщения.

Защита от компьютерных вирусов должна стать частью комплекса мер по защите информации как в отдельных компьютерах, так и в автоматизированных информационных системах в целом.

СПИСОК ЛИТЕРАТУРЫ

1. *Андреев В.Б.* Правовая информатика: Учеб. пособ. — М: ИМП, 1998.

2. *Баранов А.К., Карпычев В.Ю., Минаев В.А.* Компьютерные экспертные технологии в органах внутренних дел: Учебное пособие. — М.: Академия МВД РФ, 1992.

3. *Батурин Ю.М.* Право и политика в компьютерном круге. — М.: Наука, 1987.

4. *Батурин Ю.М.* Проблемы компьютерного права. — М.: Юрид. лит., 1991.

5. *Батурин Ю.М., Жодзишский А. М.* Компьютерные преступления и компьютерная безопасность. — М.: Юрид. лит., 1991.

6. *Бауэр Ф.Л., Гооз Г.* Информатика. Вводный курс: В 2 ч. — М.: Мир, 1990. - Ч. 1.

7. *Безруков Н.Н.* Компьютерные вирусы. — М.: Наука, 1991.

8. *Боровков В.П.* Популярное введение в программу «Statistica». — М.: Компьютер пресс, 1998.

9. *Вехов Б.В.* Компьютерные преступления: способы совершения, методика расследования. — М.: Право и Закон, 1996.

10. *Воскресенский Г.М., Дударев Г.И., Масленников Э.П.* Статистические методы обработки и анализа социальной информации в управленческой деятельности органов внутренних дел. — М.: Академия МВД СССР, 1986.

11. *Гудков П.Б.* Компьютерные преступления в сфере экономики. — М.: МИ МВД России, 1995.

12. *Гульбин Ю.* Преступления в сфере компьютерной информации // Российская юстиция. — 1997. — № 10. — С. 24—25.

13. *Демидов В.Н.* Криминологическая характеристика преступности в России и Татарстане: Учебное пособие. — М.: ВНИИ МВД России, 1998.

14. *Дьяконов В.П.* Справочник по расчетам на микрокалькуляторах. — 3-е изд. — М.: Наука, 1989.

15. *Дьяконов В.П.* Справочник по алгоритмам и программам на языке БЕЙСИК для персональных ЭВМ. — М.: Наука, 1989.

16. *Женило В.Р.* Информатика и вычислительная техника в деятельности органов внутренних дел. Часть 3. Программное обеспечение компьютерной технологии: Учеб. пособ. / Под ред. В.А. Минаева. — М.: ГУК МВД РФ, 1996.

17. *Женило В.Р., Минаев В.А.* Компьютерные технологии в криминалистических фоноскопических исследованиях и экспертизах: Учебное пособие. — М.: Академия МВД РФ, 1994.

18. *Ивахненко А.Г., Юрачковски Ю.П.* Моделирование сложных систем по экспериментальным данным. — М.: Радио и связь, 1987.

19. Информатика. Базовый курс: Учеб. для вузов / Под ред. С. В. Симоновича. — СПб.: Питер, 1999.

20. Информатика и математика для юристов. Краткий курс в таблицах и схемах: Учеб. пособ. / Под ред. В. А. Минаева. — М.: МЮИ МВД России; Приор, 1998.

21. Информатика и вычислительная техника в деятельности органов внутренних дел. Часть 2. Аппаратные средства компьютерной техники: Учеб. пособ. / Под ред. В. А. Минаева. — М.: ГУК МВД РФ, 1995.

22. Информатика и вычислительная техника в деятельности органов внутренних дел. Часть 4. Автоматизация решения практических задач в органах внутренних дел: Учеб. пособ. / Под ред. В. А. Минаева. — М.: ГУК МВД РФ, 1996.

23. Информатика и вычислительная техника в деятельности органов внутренних дел. Часть 5. Аналитическая деятельность и компьютерные технологии: Учеб. пособ. / Под ред. В.А. Минаева. — М.: ГУК МВД РФ, 1996.

24. Информатика и вычислительная техника в деятельности органов внутренних дел. Часть 6. Информационно-вычислительные сети в органах внутренних дел: Учеб. пособ. / Под ред. В.А. Минаева. — М.: ГУК МВД РФ, 1997.

25. Информационные технологии управления в органах внутренних дел / Под ред. В.А. Минаева. — М.: Академия управления МВД РФ, 1997.

26. *Исаков С.А.* Информационно-техническое обеспечение органов внутренних дел: Учеб. пособ. — М.: Юридический институт МВД РФ, 1994.

27. *Казанцев С.Я., Мазуренко П.И.* Использование ЭВМ в деятельности правоохранительных органов. — Казань: Казанский филиал Юридического института МВД РФ, 1997.

28. Каталог программных средств, рекомендуемых к внедрению в практику СЭУ МЮ СССР. - М., 1989.

29. *Кидмайер М.* Мультимедиа. — СПб.: «BHV-Санкт-Петербург», 1994.

30. Комментарий к Уголовному кодексу Российской Федерации / Под ред. А. В. Наумова. — М.: Юристъ, 1996.

31. Компьютерные технологии обработки информации: Учеб. пособ. / Под ред. С. В. Назарова. — М.: Финансы и статистика, 1995.

32. Компьютерные технологии в юридической деятельности. Учеб. и практ. пособие / Под. ред. Н. Полевого, В. Крылова. — М.: Изд-во БЕК, 1994.

33. Концепция развития системы информационного обеспечения органов внутренних дел в борьбе с преступностью. Утверждена приказом МВД РФ № 229 от 12.05.93 г.

34. *Коршунов Ю.М.* Математические основы кибернетики. — М.: Энергоатомиздат, 1987.

35. Криминалистика и компьютерная преступность: Материалы научно-практического семинара // Сб. статей. — М.: ЭКЦ МВД России, 1993.

36. *Крылов В.В.* Расследование преступлений в сфере информации. М.: Городец. 1998.

37. *Левин А.* Самоучитель работы на компьютере. — 5-е изд. — М.: Нолидж, 1999.

38. Локальные вычислительные сети: Справочник: В 3 кн. Кн. 1. Принципы построения, архитектура, коммуникационные средства / Под ред. С. В. Назарова. — М.: Финансы и статистика, 1994.

39. *Ляпунов Ю., Максимов В.* Ответственность за компьютерные преступления // Законность. — 1997. — № 1. — С. 8—15.

40. *Мак-Кланг Кр.Дж., Герриери Дж.А., Мак-Кланг К.А.* Микрокомпьютеры для юристов / Пер. с англ. А. П. Полежаева. — М.: Юридическая литература, 1988.

41. *Маркарян А.А.* Интеграция достижений естественных и технических наук в криминалистику. — Ижевск: УдГУ, 1996.

42. *Мельников В.В.* Защита информации в компьютерных системах. — М.: Финансы и статистика, 1997.

43. Методология и методика прогнозирования в сфере борьбы с преступностью: Труды Академии МВД СССР. — М.: Академия МВД СССР, 1989.

44. *Минаев В.А.* Кадровые ресурсы органов внутренних дел: современные подходы к управлению. — М.: Академия МВД СССР, 1991.

45. *Минин А.Я.* Основы управления и информатики: Курс лекций. — Екатеринбург: Екатеринбургская высшая школа МВД России, 1993.

46. *Минин А.Я.* Информатизация криминологических исследований: теория и методология. — Екатеринбург: Изд-во Урал. Ун-та, 1992.

47. Наука и техника на службе следствия // Информационный бюллетень следственного управления МВД РТ. — Вып. 5. — Казань, 1996.

48. Об информации, информатизации и защите информации. Федеральный закон от 22 февраля 1995 г. // Российская газета. — 1995. — 22 февраля.

49. Организация деятельности информационных работников горрайлинорганов внутренних дел: Сб. материалов для занятий в системе служебной подготовки / Под ред. Ю.А. Буничева. — М.: ГИЦ МВД РФ, 1995.

50. Основы автоматизации управления в органах внутренних дел: Учеб. / Под ред. В. А. Минаева, А. П. Полежаева. — М.: Академия МВД РФ, 1993.

51. Основы математического моделирования в деятельности органов внутренних дел: Учеб. пособ. / Под ред. В. А. Минаева. — М.: Академия МВД РФ, 1993.

52. *Першиков В. И., Савинков В. М.* Толковый словарь по информатике. — 2-е изд. — М.: Финансы и статистика, 1995.

53. *Петровский А., Леонтьев Б.* Эффективный хакинг для начинающих и не только. — М.: Познавательная книга плюс, 1999.

54. *Полевой Н. С.* Криминалистическая кибернетика: Учебное пособие. - 2-е изд. - М.: МГУ, 1989.

55. Правовая информатика и кибернетика: Учеб. / Под ред. Н. С. Полевого. — М.: Юридическая литература, 1993.

56. Проблемы программирования, организации и информационного обеспечения предварительного следствия // Межвуз. межвед. сб. науч. трудов. — Уфа, 1989.

57. Программа компьютеризации органов внутренних дел РФ на 1991 г. и ближайшую перспективу. Утверждена приказом МВД РФ № 104 от 05.07.91 г.

58. Расследование неправомерного доступа к компьютерной информации / Под ред. И.Г. Шурухнова. — М.: Изд-во Щит, 1999.

59. *Симонович С.В., Евсеев Г.А.* Практическая информатика: Учебное пособие. Универсальный курс. — М.: АСТ-Пресс, 1998.

60. *Симонович С.В., Евсеев Г.А., Алексеев А.Г.* Специальная информатика: Учебное пособие. — М.: АСТ-Пресс, 1998.

61. *Сойер Б., Фостер Д.Л.* Программирование экспертных систем на Паскале: Перевод с англ. — М.: Финансы и статистика, 1990.

62. *Соковых Ю.Ю.* Квалификация преступлений и информатика // Информационный бюллетень следственного комитета МВД РФ, 1993, № 4 (46).

63. Статистическое моделирование и прогнозирование: Учеб. пособ. / Под ред. А. Г. Гранберга. — М.: Финансы и статистика, 1990.

64. Техническое задание на создание информационной вычислительной сети органов внутренних дел РФ. Утверждено Министром ВД 22.02.92 г.

65. Федеральные учеты ГИЦ в борьбе с преступностью. В помощь работникам органов внутренних дел / Под ред. Г. Л. Лежикова. — М.: ГИЦ МВД РФ, 1994.

66. *Фигурнов В.Э.* IBM PC для пользователя. — 6-е изд. — М.: Инфра-М, 1995.

67. *Щербинин А.И., Игнатов Л.Н., Пучков С.И., Котов И.А.* Сравнительный анализ программных средств автоматизации уголовно-процессуальной деятельности // Информационный бюллетень Следственного комитета МВД РФ. — 1993. — № 3 (46). - С. 73 — 82.

68. *Щербинин А.И., Ильин С.К, Игнатов Л.Н.* Использование персональных ЭВМ в расследовании сложных многоэпизодных дел о хищениях в банковской сфере // Информационный бюллетень Следственного комитета МВД РФ. — 1993. — № 4 (46).

69. Экспертные системы. Принцип работы и примеры. — М.: Радио и связь, 1987.

70. *Яромич С.А.* Информатика вокруг нас: Словарь-справочник. — Одесса: Маяк, 1991.

ОГЛАВЛЕНИЕ

Учебное издание

Згадзай Олег Эдуардович,
Казанцев Сергей Яковлевич,
Казанцева Людмила Александровна

Информатика для юристов

Под редакцией Сергея Яковлевича Казанцева

Учебник

Редактор *Е.Б. Стефанова*
Технический редактор *Е.Ф. Коржуева*
Компьютерная верстка: *И.В. Земскова*
Корректор *А.П. Сизова*

Подписано в печать 07.08.2001. Формат 60x90/16. Бумага тип. № 2 Печать офсетная. Усл. печ. л. 16,0. Тираж 30 000 экз. (1-й завод 1 -7 500 экз.). Заказ **№816.**

Лицензия ИД № 02025 от 13.06.2000. Издательский центр «Академия». 111399 Москва, ул. Мартеновская, 7. Тел./факс (095)330-1092, 305-2387.

Лицензия ИД № 00520 от 03.12.1999. Издательство «Мастерство». 111399 Москва, ул. Мартеновская, 7. Тел./факс (095)330-1092, 305-2387.

Отпечатано на Саратовском полиграфическом комбинате. 410004 г. Саратов, ул. Чернышевского, 59.