Оглавление

В В Е Д Е Н И Е 2

*КОМПЬЮТЕРНЫЕ ПРАВОНАРУШЕНИЯ 3*

*Методы защиты информации в сетях. 11*

*Обзор методов защиты информации 12*

*Заключение 15*

****

## В В Е Д Е Н И Е

Информационные технологии, основанные на новейших достижениях электронно-вычислительной техники, которые получили название новых информационных технологий (НИТ), находят все большее применение в различных сферах деятельности.

Новые информационные технологии создают новое информационное пространство и открывают совершенно новые, ранее неизвестные и недоступные возможности, которые коренным образом меняют представления о существовавших ранее технологиях получения и обработки информации, в большей степени повышают эффективность функционирования различных организаций, способствуют их большей стабильности в конкурентном соперничестве.

Однако, вместе с положительными и, безусловно, необходимыми моментами компьютеры и НИТ привносят и новую головную боль, как бы еще раз констатируя правило, в котором утверждается, что за все надо платить. Эта боль, прежде всего, связана с проблемами обеспечения информационной безопасности.

Предоставляя огромные возможности, информационные технологии, вместе с тем, несут в себе и большую опасность, создавая совершенно новую, мало изученную область для возможных угроз, реализация которых может приводить к непредсказуемым и даже катастрофическим последствиям. Ущерб от возможной реализации угроз можно свести к минимуму только приняв меры, которые способствуют обеспечению информации.

Специалисты считают, что все компьютерные преступления имеют ряд отличительных особенностей. Во-первых, это высокая скрытность, сложность сбора улик по установленным фактам. Отсюда сложность доказательств при рассмотрении в суде подобных дел. Во-вторых, даже единичным преступлением наносится весьма высокий материальный ущерб. В-третьих, совершаются эти преступления высоко квалифицированными системными программистами, специалистами в области телекоммуникаций.

# КОМПЬЮТЕРНЫЕ ПРАВОНАРУШЕНИЯ

Комплексное рассмотрение и решение вопросов безопасности информации в компьютерных системах и сетях принято именовать архитектурой безопасности. В этой архитектуре безопасности выделяются угрозы безопасности, службы безопасности и механизм обеспечения безопасности.

Под угрозой безопасности понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, обрабатываемую информацию, а также программные и аппаратные средства.

Угрозы подразделяются на случайные (непреднамеренные) и умышленные. Источником первых могут быть ошибочные действия пользователей, выход из строя аппаратных средств и др.

Умышленные угрозы преследуют цель нанесения ущерба пользователем сетей и подразделяются на пассивные и активные. Пассивные угрозы не разрушают информационные ресурсы и не оказывают влияния на функционирование сетей. Их задача - несанкционированно получить информацию.

Активные угрозы преследуют цель нарушать нормальный процесс функционирования сетей путем разрушения или радиоэлектронного подавления линий, сетей, вывода из строя компьютеров, искажения баз данных и т.д. Источниками активных угроз могут быть непосредственные действия физических лиц, программные вирусы и т.д.

К основным угрозам безопасности относится раскрытие конфиденциальной информации, компрометация информации, несанкционированное использование ресурсов систем и сетей, отказ от информации.[[1]](#footnote-1)

Компьютерные преступления условно можно подразделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства.

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

1. **Несанкционированный доступ к информации, хранящейся в компьютере,**

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.

Хэккеры, «электронные корсары», «компьютерные пираты» -так называют людей, осуществляющих несанкционированный доступ в чужие информационные сети для забавы. Набирая наудачу один номер за другим, они дожидаются, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приемнику сигналов в собственной ЭВМ, и связь установлена. Если теперь угадать код (а слова, которые служат паролем, часто банальны и берутся обычно из руководства по использованию компьютера), то можно внедриться в чужую компьютерную систему.

Несанкционированный доступ к файлам законного пользователя осуществляется также нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может неспеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз.

Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки.

Авторы больших сложных программ могут не заметить некоторых слабостей логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Например, не все комбинации букв используются для команд, указанных в руководстве по эксплуатации компьютера.

Все эти небрежности, ошибки, слабости логики приводят к появлению «брешей». Обычно они все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавиться от них невозможно. Иногда программисты намеренно делают «бреши» для последующего использования.

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 без защиты против этого приема. Самый простейший путь его осуществления - получить коды и другие идентифицирующие шифры законных пользователей.

Это может делаться:

* приобретением (подкупом персонала) списка пользователей со всей необходимой информацией;
* обнаружением такого документа в организациях, где не налажен достаточный контроль за их хранением;
* подслушиванием через телефонные линии.

Иногда случается, как, например, с ошибочными телефонными звонками, что пользователь с удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой , с какой и намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени и таким образом получить некоторую информацию, в частности коды.

Несанкционированный доступ может осуществляться и в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных.

1. **Ввод в программное обеспечение « логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят компьютерную систему.**

«Временная бомба» - разновидность «логической бомбы», которая срабатывает по достижении определенного момента времени.

Способ «троянский конь» состоит в тайном введении в чужую программу таких команд, которые позволяют осуществить новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. С помощью «троянского коня» преступники, например, отчисляют на свой счет определенную сумму с каждой операции.

Компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен, тысяч, а иногда и миллионов команд. Поэтому «троянский конь» из нескольких десятков команд вряд ли может быть обнаружен, если, конечно, нет подозрений относительного этого. Но и в последнем случае экспертам-программистам потребуется много дней и недель, чтобы найти его.

Есть еще одна разновидность «троянского коня». Ее особенность состоит в том, что в безобидно выглядящий кусок программы вставляются не команды, собственно выполняющие «грязную» работу, а команды, формирующие эти команды и после выполнения уничтожающие их. В этом случае программисту, пытающемуся найти «троянского коня», необходимо искать не его самого, а команды, его формирующие.

В США получила распространение форма компьютерного вандализма, при которой «троянский конь» разрушает через какой-то промежуток времени все программы, хранящиеся в памяти машины. Во многих поступивших в продажу компьютерах оказалась «временная бомба», которая «взрывается» в самый неожиданный момент, разрушая всю библиотеку данных.

1. **Разработка и распространение компьютерных вирусов.**

Вирусы - главная опасность для сетевого программного обеспечения, особенно в сетях предприятий с существенным объемом удаленной связи, включая электронные доски объявлений.

Вирусы - это самовоспроизводящиеся фрагменты машинного кода, которые прячутся в программах. Они цепляются к программам и «ездят» на них по всей сети.[[2]](#footnote-2)

Выявляется вирус не сразу: первое время компьютер «вынашивает инфекцию», поскольку для маскировки вирус нередко используется в комбинации с «логической бомбой» или «временной бомбой». Пользователь ничего не заметит, так как его компьютер находится в состоянии «здорового носителя вируса». Обнаружить этот вирус можно, только обладая чрезвычайно развитой программистской интуицией, поскольку никакие нарушения в работе ЭВМ в данный момент не проявляют себя. А в один прекрасный день компьютер «заболевает».

По оценке специалистов в «обращении» находится более 100 типов вирусов. Но все их можно разделить на две разновидности, обнаружение которых различно по сложности: «вульгарный вирус» и «раздробленный вирус». Программа «вульгарного вируса» написана единым блоком, и при возникновении подозрений в заражении ЭВМ эксперты могут обнаружить ее в самом начале эпидемии (размножения).

Программа «раздробленного вируса» разделена на части, на первый взгляд, не имеющие между собой связи. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, чтобы воссоздать и, следовательно, размножить вирус. Таким образом, он почти все время находится в «распределенном» состоянии, лишь на короткое время своей работы собираясь в единое целое.

Варианты вирусов зависят от целей, преследуемых их создателем. Признаки их могут быть относительно доброкачественными, например, замедление в выполнении программ или появление светящейся точки на экране дисплея. Признаки могут быть эволютивными, и «болезнь» будет обостряться по мере своего течения.

Наконец, эти проявления могут быть катастрофическими и привести к стиранию файлов и уничтожению программного обеспечения.

Способы распространения компьютерного вируса основываются на способности вируса использовать любой носитель передаваемых данных в качестве «средства передвижения».

Таким образом, дискета или магнитная лента, перенесенные на другие ЭВМ, способны заразить их. И наоборот, когда «здоровая» дискета вводится в зараженный компьютер, она может стать носителем вируса. Удобными для распространения обширных эпидемий оказываются телекоммуникационные сети. Достаточно одного контакта, чтобы персональный компьютер был заражен или заразил тот, с которым контактировал. Однако самый частый способ заражения - это копирование программ, что является обычной практикой у пользователей персональных ЭВМ. Так скопированными оказываются и зараженные программы.

Против вирусов были приняты чрезвычайные меры, приведшие к созданию тестовых программ-антивирусов. Защитные программы подразделяются на три вида: фильтрующие (препятствующие проникновению вируса), противоинфекционные (постоянно контролирующие процессы в системе) и противовирусные (настроенные на выявление отдельных вирусов). Однако развитие этих программ пока не успевает за развитием компьютерной эпидемии.

Следует отметить, что распространение компьютерных вирусов имеет и некоторые положительные стороны. В частности, они являются лучшей защитой от похитителей программного обеспечения. Зачастую разработчики сознательно заражают свои дискеты каким-либо безобидным вирусом, который хорошо обнаруживается любым антивирусным тестом. Это служит достаточно надежной гарантией, что никто не рискнет копировать такую дискету.

1. **Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.**

Особенностью компьютерной неосторожности является то, что 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.

1. **Подделка компьютерной информации.**

Этот вид компьютерной преступности является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, причем имеющий достаточно высокую квалификацию.

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер.

К подделке информации можно отнести также подтасовку результатов выборов, голосований, референдумов и т.п.

1. **Хищение компьютерной информации.**

Проблема хищения информации очень сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться.

Рассмотрим теперь вторую категорию преступлений, в которых компьютер является «средством» достижения цели. Здесь можно выделить разработку сложных математических моделей, входными данными, в которых являются возможные условия проведения преступления, а выходными данными - рекомендации по выбору оптимального варианта действий преступника.

Классическим примером служит дело собственника компьютерной службы, бухгалтера по профессии, служившего одновременно бухгалтером пароходной компании в Калифорнии (США), специализировавшейся на перевозке овощей и фруктов. Он обнаружил пробелы в деятельности ревизионной службы компании и решил использовать этот факт. На компьютере своей службы он смоделировал всю бухгалтерскую систему компании. Прогнав модель вперед и обратно, он установил, сколько фальшивых счетов ему необходимо и какие операции следует проводить.

Он организовал 17 подставных компаний и, чтобы создать видимость реальности ситуации, обеспечил каждую из них своим счетом и начал денежные операции. Его действия оказались настолько успешными, что в первый год он похитил 250 тыс. долларов.

Другой вид преступлений с использованием компьютеров получил название «воздушный змей».

В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающими суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз до тех пор, пока на счете не оказывается приличная сумма. Тогда деньги быстро снимаются и владелец счета исчезает.[[3]](#footnote-3)

Таким образом, мы видим, что организованная преступность давно приняла на вооружение вычислительную технику.

**Угрозы безопасности информации в компьютерных системах**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ТИП УГРОЗЫ** | | | **Причины или побудительные мотивы** | |
| **Преднамеренные**  **угрозы** | **Непреднамеренные**  **угрозы** |  | |
| Хищение носителей информации |  | Стремление использовать конфиденциальную информацию в своих целях | |
| Применение программных ловушек |  | Те же | |
|  | Неисправность аппаратуры, которая может инициировать  несанкционированное  считывание информации | Недостаточная квалификация обслуживающего персонала, применение несертифицированных технических средств | |
| Использование программ «Троянский  конь» |  | Нанесение ущерба путем несанкционированного доступа в систему | |
| Ошибки в программах обработки информации |  | Нанесение ущерба путем внесения программных закладок в процессе разработки программных систем | |
| Внедрение компьютерного вируса |  | Разрушение информационной системы в целях нанесения ущерба | |
|  | Ошибки в программах обработки информации | Применение несертифицированного программного продукта | |
|  | Внедрение компьютерного вируса | Обслуживающий персонал не соблюдает требования безопасности, нарушает технологическую последовательность работы с системой | |
| Ошибочная коммутация в сети ЭВМ |  | В целях создания канала для утечки конфиденциальной информации | |
|  | Ошибочная коммутация в сети ЭВМ | Низкая квалификация обслуживающего персонала | |
|  | Паразитное электромагнитное излучение (ЭМИ) | Недостаточный учет требований безопасности на этапе проектирования информационной системы или ее создания | |
|  | Перекрестные наводки за счет ЭМИ | Те же | |
| Принудительное электромагнитное облучение |  | Вывод из строя информационной системы в целях нанесения ущерба | |
| Использование акустических излучений |  | Получение конфиденциальной информации | |
| Копирование с помощью визуального и слухового контроля |  | Те же | |
| Маскировка под пользователя, подбор пароля |  | Несанкционированное вмешательство в работу системы в преступных целях | |
|  | Ошибка в работе оператора | Низкая квалификация оператора, применение несертифицированного программного продукта | |
| Ошибки программиста описание и искажение программной защиты,раскрытие кодов паролей |  | В целях извлечения личной выгоды или нанесения ущерба | |
| Ошибки эксплуатационщика, описание и искажение схем защиты, ошибочная коммутация |  | Те же | |
|  | Ошибки эксплуатационщика, описание и искажение схем защиты, ошибочная коммутация | Недостаточная квалификация, нарушение технологии | |
|  | Ошибки пользователя | Использование недостаточной защиты | |

# Методы защиты информации в сетях.

Одной из самых больших сложностей оказывается установление факта совершения преступления. При компьютерных преступлениях редко наносится какой-либо видимый материальный ущерб. Например, незаконное копирование информации чаще всего остается необнаруженным, введение в компьютер вируса обычно списывается на непреднамеренную ошибку пользователя, который не смог его «отловить» при общении с внешним компьютерным миром.

Ввиду сложности математического и аппаратного обеспечения, уровень раскрываемости компьютерных преступлений в настоящее время довольно низок. По оценкам западногерманских специалистов, только 10% раскрытых компьютерных преступлений могут быть своевременно обнаружены с помощью систематических ревизионных проверок, а 90% преступлений выявляются только благодаря случайности.

Более того, при очевидно корыстных преступлениях пострадавшие часто не торопятся заявлять в правоохранительные органы.В раскрытии факта совершения преступления очень часто не заинтересованы должностные лица, в обязанности которых входит обеспечение компьютерной безопасности, т.к. признание факта несанкционированного доступа в подведомственную им систему ставит под сомнение их профессиональную квалификацию, а несостоятельность мер по компьютерной безопасности, принимаемых руководством, может вызвать серьезные осложнения. Банковские служащие, как правило, тщательно скрывают обнаруженные ими преступления, которые совершены против компьютеров банка, т.к. это может пагубно отразится на его престиже и привести к потере клиентов. Жертва может отказаться от расследования, опасаясь, что ее финансовые и другие служебные тайны могут стать достоянием во время суда.[[4]](#footnote-4)

# Обзор методов защиты информации

**1. Ограничение доступа к информации.**

Главная задача средств ограничения доступа - исключить случайный или преднамеренный доступ на территорию размещения КСА (к комплексам технических средств автоматизации) и непосредственно к аппаратуре посторонних лиц. С этой целью создается защитный контур с двумя видами преград: физической и контрольно-пропускной.

Контрольно-пропускной вид преграды может быть реализован различными способами: на основе аутентификации по обычным пропускам, аутентификации специальными магнитными карточками, кодовой аутентификации и биометрической аутентификации (отпечатки пальцев, голос, личная подпись и т.п.).

Физическая преграда защитного контура снабжается охранной сигнализацией.

**2. Контроль доступа к аппаратуре.**

В целях контроля доступа к внутреннему монтажу, линиям связи и технологическим органам управления используются устройства контроля вскрытия аппаратуры. На все закрытые дверцы, крышки, лючки или кожуха устройств устанавливаются специальные датчики. При вскрытии аппаратуры датчики срабатывают и выдают сигнал на центральное устройство контроля. Контроль вскрытия аппаратуры необходим не только в интересах защиты информации от несанкционированных действий, но и для соблюдения технологической дисциплины.

**3. Разграничение и контроль доступа к информации.**

Разграничение доступа предполагает такую организацию функционирования информационной системы, при которой должностным лицом может быть получена лишь та информация, которая необходима ему в силу функциональных обязанностей и к которой оно допущено.

**4. Разделение привилегий на доступ.**

Его суть заключается в том, что из числа допущенных к информации лиц выделяется группа, которой предоставляется право на доступ к информации только при одновременном предъявлении своих полномочий всеми членами группы. Такой способ имеет высокую эффективность защиты. Как правило, он реализуется с помощью кодов паролей.

5. Идентификация и аутентификация (установление подлинности) субъекта.

Идентификация - это присвоение субъекту (или объекту) уникального образа, имени или числового кода.

Аутентификация - это определение, является ли проверяемый субъект (объект) тем, за кого он себя выдает.

Одним из распространенных способов идентификации и установления подлинности личности является присвоение лицу или объекту уникального имени или числового кода-пароля и хранение его значения в вычислительной системе. При необходимости входа в систему пользователь вводит с терминального устройства свой код пароля, который затем сравнивается со значениями в списке паролей, хранимом в вычислительной системе. В случае совпадения кодов система открывает доступ к разрешенной информации.

6. Установление подлинности технических средств.

Важной ступенью организации системы защиты информации является идентификация и установление подлинности терминала, с которого входит в систему пользователь. Это действие также осуществляется с помощью паролей.

7. Установление подлинности документов.

Подлинность документов, являющихся продуктом информационной системы рассматривается с двух позиций:

* получение документов, сформированных на локальной вычислительной установке;
* получение готового документа с удаленных объектов вычислительной сети.

В первом случае подлинность документа гарантируется вычислительной системой, имеющей средства защиты от НСД и расположенной на контролируемой территории.

При передаче документа по каналам связи, которые расположены на неконтролируемой территории, условия передачи документа меняются. В таких случаях при передаче данных по каналам связи в вычислительной сети применяется криптографическое преобразование информации

8. Защита информации от утечки за счет побочного электромагнитного излучения.

Средства вычислительной техники являются электротехническими устройствами, при работе которых возникают электромагнитные излучения (ЭМИ) и, как следствие, электромагнитные наводки на цепи электропитания, линии телефонной и другой проводной связи. Существуют технические радиоэлектронные средства, которые позволяют восстановить информацию путем приема и анализа электромагнитных излучений. Особенно просто восстанавливается информация при анализе электромагнитного излучения дисплея (монитора на электронно-лучевой трубке), поэтому он является самым слабым звеном вычислительной установки с точки зрения безопасности информации.

Для защиты информации от побочных ЭМИ применяют следующие меры:

* для зашумления электромагнитных сигналов устанавливают специальные генераторы помех;
* на цепи питания устанавливают специальные устройства, которые осуществляют развязку по высокочастотной составляющей и тем самым препятствуют выходу электромагнитного излучения за пределы контролируемой зоны;
* изготовление специальных металлических кожухов , в которые помещаются устройства, а также ограждение экранов мониторов металлизированными сетками. Они выполняют роль экранов, которые препятствуют выходу электромагнитного излучения за пределы контролируемой зоны.

9. Защита информации от случайных воздействий.

Причинами случайных воздействий являются сбои и отказы аппаратуры, т.е. возникновение неисправностей, которые могут возникать в случайные моменты времени и вызывать нарушения в системе защиты информации.

Эффективным способом защиты от случайных воздействий является повышение надежности аппаратуры и вычислительной системы в целом.

10. Защита информации от аварийных ситуаций.

Защита информации от аварийных ситуаций заключается в создании и поддержании в работоспособном состоянии различных средств предупреждения, организации контроля и мероприятий по исключению НСД на средствах вычислительной техники в условиях отказа их жизнеобеспечения людей на объекте размещения и при возникновении стихийных бедствий.

**Заключение**

Компьютер стал любимым детищем человека. Уровень развития страны во многом определяется по уровню компьютеризации. С вычислительной техникой человечество связывало надежды на резкий скачок в интеллектуальной и духовной областях, информатике, сервисе, обороноспособности и многое другое, что может сделать нашу жизнь беззаботнее.

Но к сожалению, далеко не всем надеждам удалось осуществиться. Наряду с несомненными благами компьютеризация еще более нарушила нашу безопасность. Количество ошибок, связанных с неправильным использованием вычислительной техники, с переоценкой ее надежности и защищенности, постоянно растет.

В ПК и в вычислительных сетях сосредотачивается информация, исключительное пользование которой принадлежит определенным лицам или группам лиц, действующем в порядке личной инициативы или в соответствии с должностными обязанностями.

Такая информация должна быть защищена от всех видов постороннего вмешательства. К тому же в вычислительных сетях должны принимать меры по защите вычислительных ресурсов сети от их несанкционированного использования, т.е. доступа к сети лиц, не имеющих на это права. Физическая защита более надежна в отношении компьютеров и узлов связи, но оказывается уязвимой для каналов передачи данных большой протяженности.

Защита сетей приобретает все более важное значение, однако, не все считают, что это наилучшее решение проблемы защиты. Эту проблему следует рассматривать глобально. Необходимо защищать

информацию на всем пути ее движения от отправителя до получателя.

##### СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Батурин Ю.М., Жодзинский А.М.

Компьютерная преступность и компьютерная безопасность - М.: Юрид. лит.,1991.

1. Косарев В.П. и др. Под ред. Косарева В.П. и Еремина Л.В.

Компьютерные системы и сети: Учеб. Пособие - М.: Финансы и статистика ,1999г.

1. Косарев В.П., Голубева Н.И., Шилиманов К.

Персональные компьютеры (в вопросах и ответах): Учеб. пособие - М.: Фин. Акад.,1998г.

1. Стэн Шатт

Мир компьютерных сетей - Киев,1996г.

1. Косарев В. П., Голубева Н. Н., Шишманов К. «Персональные компьютеры» [↑](#footnote-ref-1)
2. Стен Шатт «Мир компьютерных сетей» [↑](#footnote-ref-2)
3. Батурин Ю. М., Жодзинский А. М. «Компьютерная преступность и компьютерная безопасность» [↑](#footnote-ref-3)
4. Батурин Ю. А., Жодзинский А. М. «Компьютерная преступность и компьютерная безопасность» [↑](#footnote-ref-4)