Амелин Р. В.

Информационная безопасность

Оглавление

Глава 1. Введение в информационную безопасность

1.1. Основные понятия

Под *информационной безопасностью* понимают состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, (в том числе владельцам и пользователям информации).

Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Существует также одноименная учебная (научная) дисциплина — сравнительно молодая, но динамично развивающаяся отрасль информационных технологий, занимающаяся изучением (разработкой) средств, методов и моделей защиты информации.

Самая распространенная модель информационной безопасности базируется на обеспечении трех свойств информации: конфиденциальность, целостность и доступность.

Конфиденциальность информации означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем. Если доступ к информации получает неуполномоченное лицо, происходит утрата конфиденциальности.

Для некоторых типов информации конфиденциальность является одним из наиболее важных атрибутов (например, данные стратегических исследований, медицинские и страховые записи, спецификации новых изделий и т. п.). В определенных случаях важно сохранить конфиденциальность сведений о конкретных лицах (например, сведения о клиентах банка, о кредиторах, налоговые данные; сведения медицинских учреждений о состоянии здоровья пациентов и т. д.).

Целостность информации определяется ее способностью сохраняться в неискаженном виде. Неправомочные, и не предусмотренные владельцем изменения информации (в результате ошибки оператора или преднамеренного действия неуполномоченного лица) приводят к потере целостности. Целостность особенно важна для данных, связанных с функционированием объектов критических инфраструктур (например, управления воздушным движением, энергоснабжения и т. д.), финансовых данных.

Достаточно показателен пример, когда злоумышленник вторгся в компьютерную систему исследовательской лаборатории ядерной физики в Швейцарии и изменил один знак в значении числа «пи», в результате чего из-за ошибок в расчетах был сорван важный эксперимент, а организация понесла миллионные убытки[1].

Доступность информации определяется способностью системы предоставлять своевременный беспрепятственный доступ к информации субъектам, обладающим соответствующими полномочиями. Уничтожение или блокирование информации (в результате ошибки или преднамеренного действия) приводит к потере доступности.

Доступность — важный атрибут для функционирования информационных систем, ориентированных на обслуживание клиентов (системы продажи железнодорожных билетов, распространения обновлений программного обеспечения). Ситуацию, когда уполно-

[1] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография — М.: Норма, 2004. С. 21.

моченный пользователь не может получить доступ к определенным услугам (чаще всего сетевым), называют *отказом в обслуживании*.

Кроме перечисленых трех свойств дополнительно выделяют еще два свойства, важных для информационной безопасности: аутентичность и апеллируемость.

Аутентичность — возможность достоверно установить автора сообщения.

Апеллируемость — возможность доказать, что автором является именно данный человек и никто другой.

Как учебная и научная дисциплина информационная безопасность исследует природу перечисленных свойств информации, изучает угрозы этим свойствам, а также методы и средства противодействия таким угрозам (защита информации).

Как прикладная дисциплина информационная безопасность занимается обеспечением этих ключевых свойств, в частности, путем разработки защищенных информационных систем.

1.2. Угрозы информационной безопасности

Угроза – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Соответственно *угрозой информационной безопасности* называется потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или компоненты АИС может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений.

Атака — попытка реализации угрозы.

Нарушение — реализация угрозы.

Определение, анализ и классификация возможных угроз безопасности АИС является одним из важнейших аспектов проблемы обеспечения ее безопасности. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты.

Классификацию угроз ИБ можно выполнить по нескольким критериям:

1. По аспекту ИБ: угрозы конфиденциальности, угрозы целостности, угрозы доступности. Дополнительно можно выделить угрозы аутентичности и апеллируемости.

2. По компонентам АИС, на которые нацелена угроза: данные, программное обеспечение, аппаратное обеспечение, поддерживающая инфраструктура).

3. По расположению источника угроз: внутри или вне рассматриваемой АИС. Угрозы со стороны инсайдеров являются наиболее опасными.

4. По природе возникновения: естественные (объективные) и искусственные (субъективные). *Естественные угрозы* — это угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека. *Искусственные угрозы* — угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить *непреднамеренные* (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п., и *преднамеренные* (умышленные) угрозы, связанные с целенаправленными устремлениями злоумышленников.

Рассмотрим перечень конкретных угроз, приведенный в [3].

Основные непреднамеренные искусственные угрозы АС (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

1) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

2) неправомерное отключение оборудования или изменение режимов работы устройств и программ;

3) неумышленная порча носителей информации;

4) запуск программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование носителей информации, удаление данных и т.п.);

5) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

6) заражение компьютера вирусами;

7) неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;

8) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

9) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

10) игнорирование организационных ограничений (установленных правил) при работе в системе;

11) вход в систему в обход средств защиты (загрузка посторонней операционной системы с внешних носителей и т.п.);

12) некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

13) пересылка данных по ошибочному адресу абонента (устройства);

14) ввод ошибочных данных;

15) неумышленное повреждение каналов связи.

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

1) физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

2) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

3) действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);

4) внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

5) вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;

6) применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;

7) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);

8) перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

9) хищение носителей информации;

10) несанкционированное копирование носителей информации;

11) хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

12) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

13) чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки операционных систем и других приложений;

14) незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);

15) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;

16) вскрытие шифров криптозащиты информации;

17) внедрение аппаратных спецвложений, программных «закладок» и вирусов (троянских коней), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

18) незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

19) незаконное подключение к линиям связи с целью подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

1.3. Каналы утечки информации

При ведении переговоров и использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

— акустическое излучение информативного речевого сигнала;

— электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы КЗ (контролируемая зона — это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств);

— виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;

— несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;

— воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;

— побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;

— наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;

— радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;

— радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом;

— радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

— прослушивание ведущихся телефонных и радиопереговоров;

— просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;

— хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

Перехват информации или воздействие на нее с использованием технических средств могут вестись:

— из-за границы КЗ из близлежащих строений и транспортных средств;

— из смежных помещений, принадлежащих другим учреждениям (предприятиям) и расположенным в том же здании, что и объект защиты;

— при посещении учреждения (предприятия) посторонними лицами;

— за счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через информационные сети общего пользования.

1.4. Неформальная модель нарушителя

Нарушитель — лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Для того, чтобы определить вероятные источники угроз информационной безопасности АИС и показатели риска для этих угроз строится *неформальная модель нарушителя*. Такая модель отражает потенциальные возможности и знания нарушителя, время и место действия, необходимые усилия и средства для осуществления атаки и т.п. и в идеале должны быть адекватна реальному нарушителю для данной АИС.

Модель нарушителя включает следующие (обоснованные) предположения:

1. О категориях лиц, к которым может принадлежать нарушитель: пользователи системы, обслуживающий персонал, разработчики АИС, сотрудники службы безопасности, руководители — внутренние нарушители; клиенты, посетители, конкуренты, случайные лица — внешние нарушители.

2. О мотивах нарушителя. Основными мотивами считаются три: безответственность, самоутверждение или корыстный интерес. В первом случае нарушения вызываются некомпетентностью или небрежностью без наличия злого умысла. Во втором случае нарушитель, преодолевая защиту АИС и получая доступ к системным данным, самоутверждается в собственных глазах или в глазах коллег (такой нарушитель рассматривает свои действия как игру «пользователь — против системы»). Наибольшей опасностью обладает третий тип нарушителя, который целенаправленно преодолевает систему защиты, движимый корыстным интересом.

3. Об уровне знаний нарушителя: на уровне пользователя АИС, на уровне администратора АИС, на уровне программиста, на уровне специалиста в области информационной безопасности.

4. О возможностях нарушителя (используемых методах и средствах): применяющий только агентурные методы, применяющий только штатные средства доступа к данным (возможно, в несанкционированном режиме), применяющий пассивные средства (возможность перехвата данных), применяющий активные средства (возможность перехвата и модификации данных).

5. О времени действия: во время штатного функционирования АИС, во время простоя АИС, в любое время.

6. О месте действия: без доступа на контролируемую территорию организации, с доступом на контролируемую территорию (но без доступа к техническим средствам), с рабочих мест пользователей, с доступом к базам данных АИС, с доступом к подсистеме защиты АИС.

Неформальная модель нарушителя строится на основе исследования АИС (аппаратных и программных средств) с учетом специфики предметной области и используемой в организации технологии обработки данных. Поскольку определение конкретных значений характеристик возможных нарушителей — в значительной степени субъективный процесс, обычно модель включает несколько обликов возможного нарушителя, по каждому из которых определяются значения всех приведенные выше характеристик. Наличие неформальной модели нарушителя позволяет выявить причины возможных нарушений информационной безопасности и либо устранить эти причины, либо усовершенствовать систему защиты от данного вида нарушений.

1.5. Информационная безопасность на уровне государства

Целеполагающим нормативно-правовым актом РФ в области информационной безопасности является доктрина информационной безопасности, утвержденная указом Президента от 9 сентября 2000 года.

Доктрина информационной безопасности представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Она развивает Концепцию национальной безопасности РФ применительно к информационной сфере и служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Под *информационной безопасностью Российской Федерации* доктрина понимает состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Доктрина информационной безопасности РФ включает следующие разделы:

1. Национальные интересы РФ в информационной сфере и их обеспечение. При этом выделяются четыре основных составляющие:
    1. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.
    2. Информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности

достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

3. Развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.
4. Защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

2. Виды угроз информационной безопасности РФ.
3. Источники угроз информационной безопасности РФ.
4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.
5. Общие методы обеспечения информационной безопасности Российской Федерации. Подразделяются на три группы:
   1. К правовым методам относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.
   2. Организационно-технические методы.
   3. Экономические методы, включающие в себя разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования; совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.
6. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни. В частности, ключевая роль отводится информационной безопасности в сфере экономики. Воздействию угроз ИБ в сфере экономики наиболее подвержены:
   1. система государственной статистики;
   2. кредитно-финансовая система;
   3. информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;
   4. системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;
   5. системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической дея-

тельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Основными мерами по обеспечению информационной безопасности Российской Федерации в сфере экономики являются:

1. организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;
2. коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;
3. разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;
4. разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;
5. совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;
6. совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

2. Международное сотрудничество РФ в области обеспечения информационной безопасности.
3. Основные положения государственной политики обеспечения информационной безопасности РФ.
4. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ.
5. Основные функции системы обеспечения информационной безопасности РФ,
6. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации.

Глава 2. Принципы построения защищенной АИС

2.1. Задачи системы информационной безопасности

Система обеспечения информационной безопасности АИС должна решать следующие задачи с целью противодействия основным угрозам ИБ [3]:

1. Управление доступом пользователей к ресурсам АИС.
2. Защита данных, передаваемых по каналам связи.
3. Регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности.
4. Контроль работы пользователей системы со стороны администрации и оперативное оповещение администратора безопасности о попытках несанкционированного доступа к ресурсам системы.
5. Обеспечение замкнутой среды проверенного программного обеспечения с целью защиты от бесконтрольного внедрения в систему потенциально опасных программ (в которых могут содержаться вредоносные закладки или опасные ошибки) и средств преодоления системы защиты, а также от внедрения и распространения компьютерных вирусов.
6. Контроль и поддержание целостности критичных ресурсов системы защиты; управление средствами защиты.

Различают внешнюю и внутреннюю безопасность АИС. *Внешняя безопасность* включает защиту АС от стихийных бедствий (пожар, землетрясение и т.п.) и от проникновения в систему злоумышленников извне. *Внутренняя безопасность* заключается в создании надежных и удобных механизмов регламентации деятельности всех ее законных пользователей и обслуживающего персонала.

2.2. Меры противодействия угрозам безопасности

По способам осуществления все меры обеспечения безопасности компьютерных систем подразделяются на: законодательные (правовые), административные (организационные), процедурные и программно-технические.

К *законодательным мерам защиты* относятся действующие в стране нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Важное значение имеют стандарты в области защиты информации (в первую очередь, международные). Среди этих стандартов выделяются «Оранжевая книга», рекомендации X.800 и «Общие критерии оценки безопасности информационных технологий» (Common Criteria for IT Security Evaluation).

«Оранжевая книга» — крупнейший базовый стандарт. В ней даются важнейшие понятия, определяются основные сервиса безопасности и предлагается метод классификации информационных систем по требованиям безопасности.

Рекомендации X.800 в основном посвящены вопросам защиты сетевых конфигураций. Они предлагают развитый набор сервисов и механизмов безопасности.

«Общие критерии» описывают 11 классов, 66 семейств и 135 компонентов функциональных требований безопасности. Классам присвоены следующие названия:

Первая группа определяет элементарные сервисы безопасности:

1. FAU — аудит, безопасность (требования к сервису, протоколирование и аудит);
2. FIA — идентификация и аутентификация;
3. FRU — использование ресурсов (для обеспечения отказоустойчивости).

Вторая группа описывает производные сервисы, реализованные на базе элементарных:

4. FCO — связь (безопасность коммуникаций отправитель-получатель);
5. FPR — приватность;
6. FDP — защита данных пользователя;
7. FPT — защита функций безопасности объекта оценки.

Третья группа классов связана с инфраструктурой объекта оценки:

8. FCS — криптографическая поддержка (обслуживает управление криптоключами и крипто-операциями);
9. FMT — управление безопасностью;
10. FTA — доступ к объекту оценки (управление сеансами работы пользователей);
11. FTP — доверенный маршрут/канал;

Кроме этого «Общие критерии» содержат сведения о том, каким образом могут быть достигнуты цели безопасности при современном уровне информационных технологий и позволяют сертифицировать систему защиты (ей присваивается определенный уровень безопасности).

Осенью 2006 года в России был принят национальный стандарт ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология — Практические правила управления информационной безопасностью», соотвествующий международному стандарту ИСО 17799. Стандарт представляет собой перечень мер, необходимых для обеспечения информационной безопасности организации, включая действия по созданию и внедрению системы управления информационной безопасности, которая строится таким же образом и на тех же принципах, что и система менеджмента качества, и совместима с ней.

Административные меры защиты — меры организационного характера, регламентирующие процессы функционирования АИС, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Они включают:

1. Подбор и подготовку персонала системы.
2. Организацию охраны и пропускного режима.
3. Организацию учета, хранения, использования и уничтожения документов и носителей с информацией.
4. Распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.д.).

В составе административных мер защиты важную роль играет формирование программы работ в области информационной безопасности и обеспечение ее выполнения (для этого необходимо выделять необходимые ресурсы и контролировать состояние дел). Основой программы является *политика безопасности организации* — совокупность руково-

дящих принципов, правил, процедур и практических приёмов в области безопасности, которыми руководствуется организация в своей деятельности. Разработка политики безопасности включает определение следующих основных моментов:

— какие данные и насколько серьезно необходимо защищать;
— кто и какой ущерб может нанести организации в информационном аспекте;
— основные риски и способы их уменьшения до приемлемой величины.

С практической точки зрения политику безопасности можно условно разделить на три уровня: верхний, средний и нижний.

К верхнему уровню относятся решения, затрагивающие организацию в целом (как правило, носят общий характер и исходят от руководства). Например, цели организации в области информационной безопасности, программа работ в области информационной безопасности (с назначением ответственных за ее реализацию).

К *среднему уровню* относятся вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией (например, использование на работе персональных ноутбуков, установка непроверенного программного обеспечения, работа с Интернетом и т.д.).

Политика безопасности *нижнего уровня* касается конкретных сервисов и должна быть наиболее детальной. Часто правила достижения целей политики безопасности нижнего уровня заложены в эти сервисы на уровне реализации [см. 4. С. 148—149].

Меры процедурного уровня — отдельные мероприятия, выполняемые на протяжении всего жизненного цикла АИС. Они ориентированы на людей (а не на технические средства) и подразделяются на:

— управление персоналом;
— физическая защита;
— поддержание работоспособности;
— реагирование на нарушения режима безопасности;
— планирование восстановительных работ.

Программно-технические меры защиты основаны на использовании специальных аппаратных средств и программного обеспечения, входящих в состав АИС и выполняющих функции защиты: шифрование, аутентификацию, разграничение доступа к ресурсам, регистрацию событий, поиск и удаление вирусов и т.д. Они будут подробно рассмотрены в следующих главах.

2.3. Основные принципы построения систем защиты АИС

1. Простота механизма защиты. Используемые средства защиты не должны требовать от пользователей специальных знаний или значительных дополнительных трудозатрат. Они должны быть интуитивно понятны и просты в использовании,.

2. Системность. При разработке системы защиты и вводе ее в эксплуатацию необходим учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для обеспечения безопасности. В частности, долж-

ны быть учтены все слабые места АИС, возможные цели и характер атак, возможность появления принципиально новых угроз безопасности.

3. Комплексность. Предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Целесообразно строить эшелонированную систему защиты, обеспечивающую комплексную безопасность на разных уровнях (внешний уровень — физические средства, организационные и правовые меры; уровень ОС; прикладной уровень).

4. Непрерывность. Мероприятия по обеспечению информационной безопасности АИС должны осуществляться на протяжении всего ее жизненного цикла — начиная с этапов анализа и проектирования и заканчивая выводом системы из эксплуатации. При этом наилучший результат достигается, когда разработка системы защиты идет параллельно с разработкой самой защищаемой АИС. Не допускается также никаких перерывов в работе средств защиты.

5. Разумная достаточность. Один из основополагающих принципов информационной безопасности гласит: абсолютно надежная защита невозможна. Любой самый сложный механизм защиты может быть преодолен злоумышленником при затрате соответствующих средств и времени[2]. *Система защиты считается достаточно надежной, если средства, которые необходимо затратить злоумышленнику на ее преодоление значительно превышают выгоду, которую он получит в случае успеха.* Иногда используется обратный принцип: расходы на систему защиты (включая потребляемые ей системные ресурсы и неудобства, возникающие в связи с ее использованием) не должны превышать стоимость защищаемой информации.

6. Гибкость. Система защиты должна иметь возможность адаптироваться к меняющимся внешним условиям и требованиям.

7. Открытость алгоритмов и механизмов защиты. Система должна обеспечивать надежную защиту в предположении, что противнику известны все детали ее реализации. Или иными словами, защита не должна обеспечиваться за счет секретности структуры и алгоритмов системы защиты АИС.

[2] Хотя подбор 2048-битного ключа с использованием самых современных вычислительных мощностей займет у злоумышленника тысячелетия.

Глава 3. Модели безопасности

3.1. Понятие и назначение модели безопасности

Основную роль в методе формальной разработки системы играет так называемая *модель безопасности* (*модель управления доступом, модель политики безопасности*). Целью этой модели является выражение сути требований по безопасности к данной системе. Она определяет потоки информации, разрешенные в системе, и правила управления доступом к информации.

Модель позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты. Так как она является формальной, возможно осуществить доказательство различных свойств безопасности системы.

Хорошая модель безопасности обладает свойствами абстрактности, простоты и адекватности моделируемой системе.

Основные понятия, используемые в моделях разграничения доступа, приведены в руководящем документе Государственной технической комиссии при Президенте РФ «Защита от несанкционированного доступа к информации»:

Доступ к информации — ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации

Объект доступа — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа

Субъект доступа — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

3.2. Модель дискреционного доступа (DAC)

В рамках дискреционной модели контролируется доступ субъектов (пользователей или приложений) к объектам (представляющим собой различные информационные ресурсы: файлы, приложения, устройства вывода и т.д.).

Для каждого объекта существует субъект-владелец, который сам определяет тех, кто имеет доступ к объекту, а также разрешенные операции доступа. Основными операциями доступа являются READ (чтение), WRITE (запись) и EXECUTE (выполнение, имеет смысл только для программ). Таким образом, в модели дискреционного доступа для каждой пары субъект-объект устанавливается набор разрешенных операций доступа.

При запросе доступа к объекту, система ищет субъекта в списке прав доступа объекта и разрешает доступ если субъект присутствует в списке и разрешенный тип доступа включает требуемый тип. Иначе доступ не предоставляется.

Классическая система дискреционного контроля доступа является «закрытой» в том смысле, что изначально объект не доступен никому, и в списке прав доступа описывается набор разрешений. Также существуют «открытые» системы, в которых по умолчанию все имеют полный доступ к объектам, а в списке доступа описывается набор ограничений.

Такая модель реализована в операционных системах Windows (см. рис. 1) и Linux.

В частности, в Linux для каждого файла (все ресурсы в ОС Linux представимы в виде файлов, в том числе устройства ввода-вывода) устанавливаются разрешения доступа для трех категорий субъектов: владелец файла, члены той же группы, что и владелец, и все остальные пользователи. Для каждой из этих категорий устанавливаются права на чтение (r), запись (w) и выполнение (x). Набор прав доступа объекта может быть представлен в виде символьной строки. Например, запись «`rwxr-xr--`» означает, что владелец файла может делать с ним все, что угодно; члены его группы могут читать и исполнять файл, но не могут записывать, а прочим пользователям доступно только чтение.

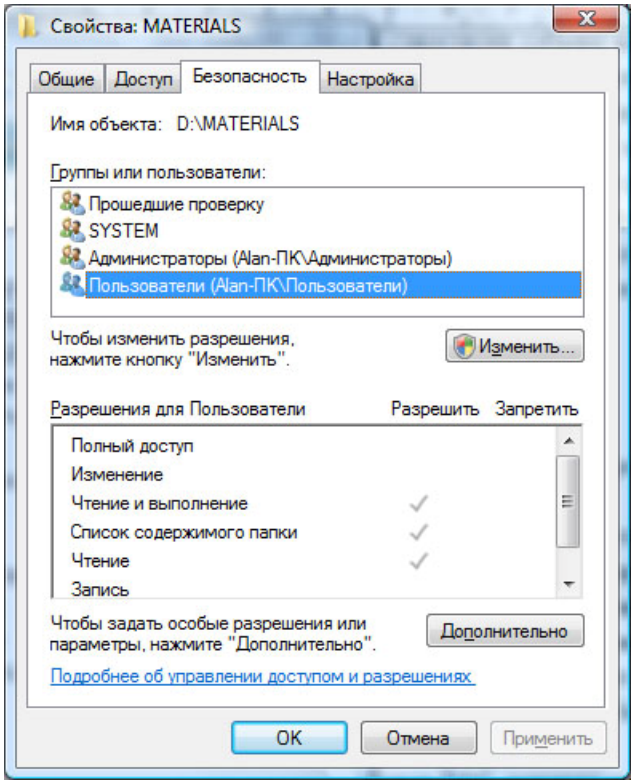

Рис. 1. Дискреционная модель доступа в Windows Vista.

Недостаток модели DAC заключается в том, что субъект, имеющий право на чтение информации может передать ее другим субъектам, которые этого права не имеют, без уведомления владельца объекта. Таким образом, нет гарантии, что информация не станет доступна субъектам, не имеющим к ней доступа. Кроме того, не во всех АИС каждому объекту можно назначить владельца (во многих случаях данные принадлежат не отдельным субъектам, а всей системе).

3.3. Модель безопасности Белла—ЛаПадулы

Одна из наиболее известных моделей безопасности — модель Белла-ЛаПадулы (модель мандатного управления доступом). В ней определено множество понятий, связанных с контролем доступа; даются определения субъекта, объекта и операции доступа, а также математический аппарат для их описания. Эта модель в основном известна двумя основными правилами безопасности: одно относится к чтению, а другое – к записи данных.

Пусть в системе имеются данные (файлы) двух видов: *секретные* и *несекретные,* а пользователи этой системы также относятся к двум категориям: с уровнем допуска к несекретным данным (несекретные) и с уровнем допуска к секретным данным (секретные).

1. Свойство простой безопасности: несекретный пользователь (или процесс, запущенный от его имени) не может читать данные из секретного файла.

*2. *-свойство: пользователь с уровнем доступа к секретным данным не может записывать данные в несекретный файл.* Это правило менее очевидно, но не менее важно. Действительно, если пользователь с уровнем доступа к секретным данным скопирует эти данные в обычный файл (по ошибке или злому умыслу), они станут доступны любому «несекретному» пользователю. Кроме того, в системе могут быть установлены ограничения на операции с секретными файлами (например, запрет копировать эти файлы на другой компьютер, отправлять их по электронной почте и т.д.). Второе правило безопасности гарантирует, что эти файлы (или даже просто содержащиеся в них данные) никогда не станут несекретными и не «обойдут» эти ограничения. Таким образом, вирус, например, не сможет похитить конфиденциальные данные.

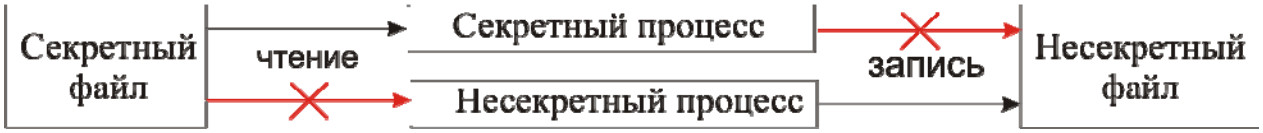

Рис. 2. Модель безопасности Белла-ЛаПадулы.

Рассмотренные правила легко распространить на случай, когда в системе необходимо иметь более двух уровней доступа — например, различаются несекретные, конфиденциальные, секретные и совершенно секретные данные. Тогда пользователь с уровнем допуска к секретным данным может читать несекретные, конфиденциальные и секретные документы, а создавать — только секретные и совершенно секретные.

Общее правило звучит так: *пользователи могут читать только документы, уровень секретности которых не превышает их допуска, и не могут создавать документы ниже уровня своего допуска.* То есть теоретически пользователи могут создавать документы, прочесть которые они не имеют права.

Модель Белла-ЛаПадулы стала первой значительной моделью политики безопасности, применимой для компьютеров, и до сих пор в измененном виде применяется в военной отрасли. Модель полностью формализована математически. Основной упор в модели делается на конфиденциальность, но кроме неё фактически больше ничего не представлено. Кроме того, в модели игнорируется проблема изменения классификации: предполагается, что все сведения относятся к соответствующему уровню секретности, который остается неизменным. Наконец, бывают случаи, когда пользователи должны работать с данными, которые они не имеют права увидеть. «Сведения о том, что самолет несет груз из некоторого количества бомб, возможно, имеют более высокий уровень секретности, чем уровень доступа диспетчера, но диспетчеру тем не менее необходимо знать вес груза.» [1]

3.4. Ролевая модель контроля доступа (RBAC)

Ролевой метод управления доступом контролирует доступ пользователей к информации на основе типов их активностей в системе (ролей). Под *ролью* понимается совокупность действий и обязанностей, связанных с определенным видом деятельности. Примеры ролей: администратор базы данных, менеджер, начальник отдела.

В ролевой модели с каждым объектом сопоставлен набор разрешенных операций доступа для каждой роли (а не для каждого пользователя). В свою очередь, каждому пользователю сопоставлены роли, которые он может выполнять. В некоторых системах пользователю разрешается выполнять несколько ролей одновременно, в других есть ограничение на одну или несколько не противоречащих друг другу ролей в каждый момент времени.

Для формального определения модели RBAC используются следующие соглашения:

S = субъект — человек или автоматизированный агент.

R = роль — рабочая функция или название, определяется на уровне авторизации.

P = разрешения — утверждения режима доступа к ресурсу.

SE = сессия — Соответствие между S, R и/или P.

SA = назначение субъекта (Subject Assignment). $SA \subseteq S \times R$. При этом субъекты назначаются связям ролей и субъектов в отношении «многие ко многим» (один субъект может иметь несколько ролей, а одну роля могут иметь несколько субъектов).

PA = назначение разрешения (Permission Assignment). $PA \subseteq P \times R$. При этом разрешения назначаются связям ролей в отношении «многие ко многим».

RH = частично упорядоченная иерархия ролей (Role Hierarchy). $PH \subseteq R \times R$.

На возможность наследования разрешений от противоположных ролей накладывается ограничительная норма, которая позволяет достичь надлежащего разделения режимов. Например, одному и тому же лицу может быть не позволено создать учетную запись для кого-то, а затем авторизоваться под этой учетной записью.

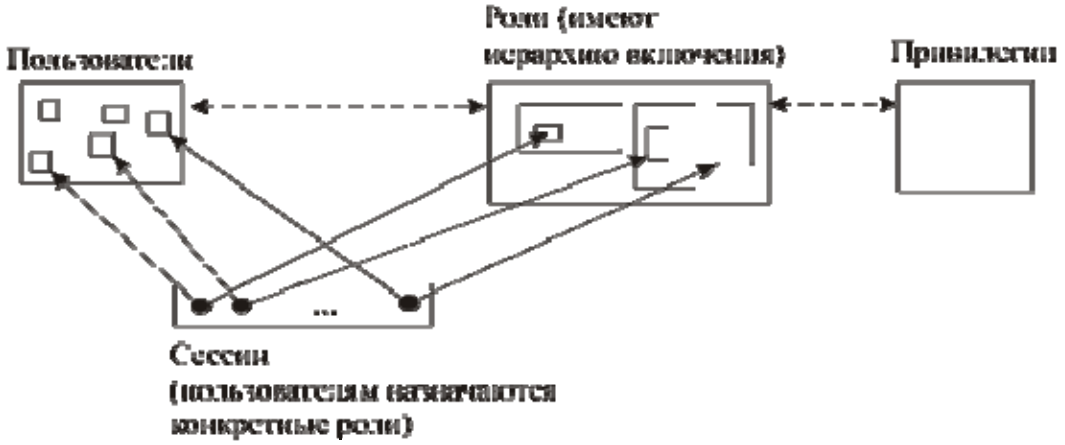

Рис. 3. Схема ролевой модели контроля доступа (RBAC)

Основные достоинства ролевой модели:

1. Простота администрирования. В отличие от модели DAC нет необходимости прописывать разрешения для каждой пары «объект-пользователь». Вместо этого прописываются разрешения для пар «объект-роль» и определяются роли каждого пользователя. При изменении области ответственности пользователя, у него просто изменяются роли. Иерархия ролей (когда роль наряду со своими собственными привилегиями может наследовать привилегии других ролей) также упрощает процесс администрирования.

2. Принцип наименьшей привилегии. Ролевая модель позволяет пользователю регистрироваться в системе ролью, минимально необходимой для выполнения требуемых за-

дач. Запрещение полномочий, не требуемых для выполнения текущей задачи, не позволяет обойти политику безопасности системы.

3. Разделение обязанностей.

RBAC широко используется для управления пользовательскими привилегиями в пределах единой системы или приложения. Список таких систем включает в себя Microsoft Active Directory, SELinux, FreeBSD, Solaris, СУБД Oracle, PostgreSQL 8.1, SAP R/3 и множество других, эффективно применяющих RBAC.

С помощью RBAC могут быть смоделированы дискреционные и мандатные системы управления доступом.

3.5. Системы разграничения доступа

Конкретное воплощение модели разграничения доступа находят в *системе разграничения доступа (СРД).* СРД — это совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

Многие системы разграничения доступа базируются на *концепции диспетчера доступа.* В основе этой концепции лежит понятие *диспетчера доступа* — абстрактной машины, которая выступает посредником при всех обращениях субъектов к объектам. Диспетчер доступа использует *базу данных защиты*, в которой хранятся правила разграничения доступа и на основании этой информации разрешает, либо не разрешает субъекту доступ к объекту, а также фиксирует информацию о попытке доступа в *системном журнале*.

Основными требованиями к реализации диспетчера доступа являются:

- требование полноты контролируемых операций, согласно которому проверке должны подвергаться все операции всех субъектов над всеми объектами системы. Обход диспетчера предполагается невозможным;
- требование изолированности, то есть защищенности диспетчера от возможных изменений субъектами доступа с целью влияния на процесс его функционирования;
- требование формальной проверки правильности функционирования;
- минимизация используемых диспетчером ресурсов [3].

База данных защиты строится на основе матрицы доступа или одного из ее представлений.

Матрица доступа — таблица, в которой строки соответствуют субъектам, столбцы — объектам доступа, а на пересечении строки и столбца содержатся правила (разрешения) доступа субъекта к объекту. Основными недостатками такой матрицы являются ее чрезмерно большая размерность и сложность администрирования: все взаимосвязи и ограничения предметной области приходится учитывать вручную. (Примеры ограничений: права доступа субъекта к файлу не могут превышать его прав доступа к устройству, на котором этот файл размещен; группа пользователей наследует одинаковые полномочия и т.д.). Для преодоления этих сложностей матрица доступа в СРД часто заменяется некоторым ее неявным *представлением*. Рассмотрим основные из них.

1. Списки управления доступом (access control lists, ACL). Для каждого объекта задан список субъектов, имеющих ненулевые полномочия доступа к ним (с указанием этих полномочий). В результате серьезно эконится память, поскольку из матрицы доступа исклю-

чаются все нулевые значения (составляющие большую ее часть). Тем не менее, спискам управления доступом присущ ряд недостатков:

- неудобство отслеживания ограничений и зависимостей по наследованию полномочий субъектов;
- неудобство получения сведений об объектах, к которым имеет какой либо вид доступа данный субъект;
- так как списки управления доступом связаны с объектом, то при удалении субъекта возможно возникновение ситуации, при которой объект может быть доступен несуществующему субъекту.

2. Списки полномочий субъектов. Аналогично ACL с той разницей, что для каждого субъекта задан список объектов, доступ к которым разрешен (с указанием полномочий доступа). Такое представление называется *профилем субъекта*. Оба представления имеют практически идентичные достоинства и недостатки.

3. Атрибутные схемы. Основаны на присвоении субъектам и/или объектам определенных меток, содержащих значения атрибутов. Элементы матрицы доступа не хранятся в явном виде, а динамически вычисляются при каждой попытке доступа для конкретной пары субъект-объект на основе их атрибутов. Помимо экономии памяти достигается непротиворечивость базы данных защиты, а также удобство ее администрирования. Основным недостатком является сложность задания прав доступа конкретного субъекта к конкретному объекту.

Тест для самоконтроля № 1

1. К какой разновидности моделей управления доступом относится модель Белла-ЛаПадулы?

а) модель дискреционного доступа;

б) модель мандатного доступа;

в) ролевая модель.

2. Как называются угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.?

3. К каким мерам защиты относится политика безопасности?

а) к административным;

б) к законодательным;

в) к программно-техническим;

г) к процедурным.

4. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?

а) ACL;

б) списки полномочий субъектов;

в) атрибутные схемы.

5. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?

а) целостность;

б) апеллируемость;

в) доступность;

г) конфиденциальность;

д) аутентичность.

6. К основным принципам построения системы защиты АИС относятся:

а) открытость;

б) взаимозаменяемость подсистем защиты;

в) минимизация привилегий;

г) комплексность;

д) простота.

7. Какие из следующих высказываний о модели управления доступом RBAC справедливы?

а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей;

б) роли упорядочены в иерархию;

в) с каждым объектом доступа ассоциировано несколько ролей ;

г) для каждой пары «субъект-объект» назначен набор возможных разрешений.

8. Диспетчер доступа...

а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;

б) ... использует атрибутные схемы для представления матрицы доступа;

в) ... выступает посредником при всех обращениях субъектов к объектам;

г) ... фиксирует информацию о попытках доступа в системном журнале;

9. Какие предположения включает неформальная модель нарушителя?

а) о возможностях нарушителя;

б) о категориях лиц, к которым может принадлежать нарушитель;

в) о привычках нарушителя;

г) о предыдущих атаках, осуществленных нарушителем;

д) об уровне знаний нарушителя.

10. Что представляет собой доктрина информационной безопасности РФ?

а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;

б) федеральный закон, регулирующий правоотношения в области информационной безопасности;

в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;

г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

11. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности?

а) политика безопасности верхнего уровня;

б) политика безопасности среднего уровня;

в) политика безопасности нижнего уровня;

г) принцип минимизации привилегий;

д) защита поддерживающей инфраструктуры.

12. Какие из перечисленных ниже угроз относятся к классу преднамеренных?

а) заражение компьютера вирусами;

б) физическое разрушение системы в результате пожара;

в) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

е) вскрытие шифров криптозащиты информации.

Глава 4. Введение в криптографию. Симметричное шифрование

4.1. Основные понятия криптографии

До 70-х годов XX века *криптографией* называлась область науки и практической деятельности, связанная с изучением и разработкой методов шифрования данных. В настоящее время это область науки, техники и практической деятельности, связанная с разработкой, применением и анализом криптографических систем защиты информации.

Криптографическая система — это система обеспечения информационной безопасности сети или АИС, использующая криптографические средства. Может включать подсистемы шифрования, идентификации пользователей, электронной цифровой подписи и др.

Криптографические средства — методы и средства обеспечения информационной безопасности, использующие криптографические преобразования информации. В узком смысле под криптографическими средствами могут пониматься отдельные устройства, документы и программы, использующиеся для выполнения функций криптосистемы.

Криптографическое преобразование информации — преобразование информации с использованием одного из криптографических алгоритмов. К *криптографическим алгоритмам* относятся алгоритмы шифрования/дешифрования, хэширования, формирования и проверки электронной цифровой подписи, распределения ключей и множество других алгоритмов, каждый из которых предназначен для противодействия определенным угрозам информационной беопасности со стороны возможного нарушителя (противника, злоумышленника) или нежелательных воздействий естественного характера. Ьольшинство криптографических алгоритмов строятся на математической основе.

Криптография является частью боле общей науки — *криптологии*. Вторая часть криптологии — *криптоанализ.* До 70-х годов XX века эта наука занималась оценкой сильных и слабых стором методов шифрования, а также разработкой методов взлома шифров. В настоящее время криптоанализ — область науки, занимающаяся изучением криптографических систем защиты в поиске способов нарушения информационной безопасности, которую обеспечивает данная система. Таким образом, криптоанализ изучает методы прочтения зашифрованного текста без ключа, методы подделки электронной цифровой подписи (без знания закрытого ключа автора) и т.д. Криптография и криптоанализ — две сильно взаимодействующие науки с противоположными целями. За последние несколько десятилетий они непрерывно и интенсивно развиваются, причем достижения одной из них заставляют другую быстро реагировать совершенствованием своего аппарата.

4.2. Шифрование

Шифрование — это процесс преобразования исходного сообщения M (называемого *открытым текстом*) в форму M' (*зашифрованный текст* или *шифртекст*). При этом провести обратное преобразование M' в M возможно только обладая некоторой дополнительной информацией, называемой *ключом*.

Шифрование нередко путают с *кодированием*, но между двумя этими процессами есть значительная разница. Кодирование также представляет собой преобразование ис-

ходного сообщения в другую форму, но цель этого преобразования — удобство обработки или передачи сообщения. Например, символьный текст кодируется в двоичный (каждый символ заменяется последовательностью нулей и единиц) для того, чтобы его можно было хранить и обрабатывать в ЭВМ, а двоичный текст преобразовывается в последовательность электрических импульсов, для того, чтобы стала возможной его передача по кабелю. Цель шифрования — противоположная. Текст зашифровывается для того, чтобы посторонние лица, не обладающие ключом, не могли бы воспринять заложенную в нем информацию, даже располагая этим зашифрованным текстом. Таким образом, шифрование является *средством обеспечения конфиденциальности* информации.

Алгоритмы шифрования делятся на две большие группы:

1. Симметричное (традиционнное шифрование).
2. Шифрование с открытым ключом.

4.3. Симметричное шифрование

В симметричных алгоритмах шифрования *один и тот же ключ* K используется для того, чтобы зашифровать сообщение и для его последующей расшифровки. Таким образом, и *отправитель* и *получатель* сообщения должны располагать одним и тем же ключом. Схематично это можно записать в виде:

M' = E(M, K)

M = D(M', K),

где E — функция шифрования (encrypt), а D — функция дешифрования (decrypt), обе используют ключ K в качестве одного из параметров.

Исторически симметричное шифрование появилось первым. Более того, до середины XX века это была единственная разновидность шифрования. Симметричные алгоритмы широко применяются и в настоящее время.

Далее мы рассмотрим ряд простых алгоритмов симметричного шифрования, на примере которых легко проанализировать такие их характеристики, как устойчивость к различным видам криптоанализа, а также некоторые базовые принципы криптографии. Затем будут рассмотрены алгоритмы, используемые в современных информационных системах.

Все алгоритмы симметричного шифрования можно разделить на три класса:

1. Подстановочные алгоритмы.
2. Перестановочные алгоритмы.
3. Алгоритмы, использующие и подстановку и перестановку (к этому классу относятся практически все современные алгоритмы, разработанные для защиты информации в ЭВМ).

4.4. Подстановочные алгоритмы

Подстановочные алгоритмы шифрования работают по следующему принципу: *каждый символ (или последовательность символов) исходного сообщения заменяются другим символом (или другой последовательностью символов).*

Рассмотрим конкретные примеры.

1. Шифр Цезаря.

Самым древним и самым простым из известных подстановочных шифров является шифр, использовавшийся Юлием Цезарем. В этом шифре каждая буква исходного сообщения заменяется буквой, находящейся в алфавите на три позиции после нее.

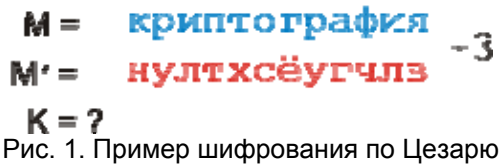

Рис. 1. Пример шифрования по Цезарю

Особенностью шифра Цезаря, как несложно заметить, является отсутствие ключа. Число 3 в данном случае ключом не является, поскольку не выбирается отправителем сообщения, а используется для сдвига по алфавиту постоянно. Во времена Юлия Цезаря это не было слабостью шифра (поскольку сама идея сокрытия информации путем преобразования текста была незнакомой его противникам), но в настоящее время первым правилом криптографии является следующее допущение:

Стойкость любого шифра определяется в предположении, что противнику полностью известен механизм шифрования и единственной информацией, которой он не располагает, является ключ.

Данное допущение особенно актуально для настоящего времени, когда сложность шифров достигла такого уровня, что зашифровывать и расшифровывать сообщения вручную просто невозможно. Для этих целей используется программное обеспечение, которое заинтересованные лица могут детально проанализировать и, таким образом, полностью восстановить алгоритм шифрования.

Это правило имеет тенденцию нарушаться в тех областях, когда криптографиечское программное обеспечение не предназначено для широкого распространения. Например, алгоритмы, использующиеся в системах электронного голосования, правительственной связи и др. Разработчики этих систем считают сокрытие алгоритмов шифрования фактором, усиливающим безопасность. Однако считается научно установленной ошибочность этого предположения. Злоумышленник, серьено заинтересованный в том, чтобы взломать криптографическую защиту и нарушить конфиденциальность данных, почти наверняка найдет способ получить доступ к самой программе, которая по определению не может быть также хорошо защищена, как обрабатываемые ею данные, и изучить используемые алгоритмы. Сокрытие алгоритмов и деталей архитектуры таких систем лишь препятствует их изучению независимыми исследователями и увеличивает опасность того, что алгоритмы, положенные в их основу, будут недостаточно надежными[3].

[3] Так, например, в 2007 году в результате утечки информации оказались обнародованы алгоритмы, используемые в популярной технологии KeeLoq — системы охраны, применяемой в противоугонных средствах автомобильной защиты. После исследования, проведенного независимыми экспертами, оказалось, что при сравнительно скромных затратах времени и вычислительных ресурсов (два дня работы компьютеров общей ценой около 10 000 евро) злоумышленники могут вскрыть сначала секретный ключ какой-либо конкретной машины, а на его основе — но теперь уже за секунды — цифровой ключ любого другого автомобиля этой же компании. Двумя годами раньше аналогичный скандал возник с системой электронного голосования, использовавшейся в США, исходные коды которой оказались случайно выложенными в общий доступ на сайте компании. Исследование показало уязвимость системы к целому спектру популярных атак.

Рассмотрим вариацию шифра Цезаря, при которой число 3 является не жестко заданным, а выбирается произвольно, согласно договоренности между отправителем и получателем сообщения. В этом случае шифр Цезаря становится полноценным шифром с ключом K (потенциально неизвестном противнику).

Однако легко заметить, что в качестве ключа могут быть выбраны лишь числа в диапазоне от 1 до 32 (для русского алфавита). Действительно, шифр является циклическим: Я + 1 = А, но и Я + 34 = А. То есть, число 34, выбранное в качестве ключа, будет эквивалентно ключу 1, ключ 35 — ключу 2 и т.д. Противнику ничего не стоит перебрать все 32 возможных ключа и обнаружить нужный[4].

Таким образом, модифицированный шифр Цезаря является неустойчивым ко взлому *методом перебора возможных ключей* по причине их малого диапазона или, как говорят, *малой длины ключа*.

2. Моноалфавитный шифр (шифр простой замены)

Один из хорошо известных подстановочных шифров. Каждому символу алфавита открытого текста ставится в соответствие некоторый символ другого алфавита. Он может и совпадать с первым (тогда одна буква заменяется другую). При шифровании каждая символ открытого текста заменяется на соответствующий ему другой символ.

Ключом к данному шифру будет являться таблица соответствий, которую удобно представить в виде символов, выписанных в алфавитном порядке тех букв, которые они заменяют. Другими словами, ключом является перестановка символов алфавита зашифрованного текста.

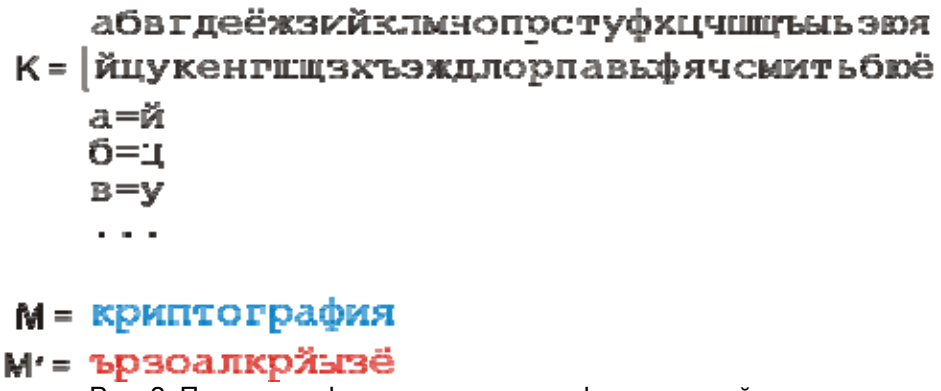

Рис. 2. Пример шифрования текста шифром простой замены

В данном случае число возможных ключей равно числу возможных перестановок из 33 букв, то есть, 33!. Даже при использовании миллиона компьютеров, проверяющих миллион возможных ключей в секунду, перебор всех вариантов займет больше миллиона лет. Таким образом, моноалфавитный шифр является стойким ко взлому методом перебора возможных ключей.

Однако данный шифр достаточно просто поддается криптоанализу, который начинается с подсчета каждого символа шифртекста и определения частоты его встречаемости.

[4] При этом необязательно даже расшифровывать весь текст сообщения: после опробования ключа на первом же десятке символов станет понятно, получаем ли мы бессмысленный набор символов (следовательно, ключ не подходит), или что-то, похожее на настоящий текст.

Для достаточно длинного сообщения (порядка 4—5 предложений) этой информации будет достаточно, чтобы сопоставить ее с таблицей частоты встречамости букв языка.

Все естественные языки имеют характерное частотное распределение символов. Например, буква «О» - встречается в русском языке чаще других, а буква «Ф» — самая редкая (см. табл. 1).

Табл. 1. Таблица частот встречаемости букв русского языка.

Символ	Вероятность	Символ	Вероятность	Символ	Вероятность
пробел	0.175	К	0.028	Ч	0.012
О	0.089	М	0.026	Й	0.010
Е	0.072	Д	0.025	Х	0.009
А	0.062	П	0.023	Ж	0.007
И	0.062	У	0.021	Ю	0.006
Н	0.053	Я	0.018	Ш	0.006
Т	0.053	Ы	0.016	Ц	0.004
С	0.045	З	0.016	Щ	0.003
Р	0.040	Ь	0.014	Э	0.003
В	0.038	Б	0.014	Ф	0.002
Л	0.03	Г	0.013		

На основе частоты встречаемости символов зашифрованного текста можно сделать предположения о некоторых, наиболее часто встречающихся из них, а затем, опираясь на эти предположения, постепенно восстанавливать слова текста, начиная с самых коротких — предлогов и союзов. Так, в английском языке достаточно легко идентифицируется артикль the — самая часто встречающаяся комбинация из трех букв.

Таким образом, моноалфавитные шифры имеют серьезную слабость к криптоанализу *на основе статистических особенностей исходного текста*, которые наследует зашифрованный текст. Противнику даже не нужно целенаправленно подбирать ключ — он сам восстанавливается по ходу дела.

Нетрудно заметить, что шифр Цезаря также является моноалфавитным шифром.

3. Шифр Гронсфельда

Рассмотрим шифр, предсталяющий собой модификацию шифра Цезаря. В качестве ключа используется последовательность цифр произвольной фиксированной длины. Каждая цифра этой последовательности записывается под одним символом открытого текста, причем если длина ключа меньше длины текста, ключ циклически повторяется. Зашифруем слово «информатика» ключом «123».

Рис. 3. Пример шифрования текста шифром Гронсфельда

Данный шифр (описанный Жюль Верном в романе «Жангада») относится к семейству *многоалфавитных шифров* (или *шифров сложной замены*). В многоалфавитном шифре 1-й символ открытого текста шифруется с помощью моноалфавитного шифра, ключом к которому является перестановка K_1, 2-й символ — ключом K_2 и т.д., n-й символ — ключом K_n, а n+1-й — снова ключом K_1, где n — количество используемых алфивитов (или шифров простой замены). В приведенном примере n=3.

Особенности многоалфавитных шифров хорошо демонстрирует шифр Гронсфельда (и, в частности, приведенный пример). Мы видим, что одна и та же буква *«и»* превращается то в *«й»*, то в *«л»* в зависимости от того, какая цифра ключа использовалась для шифрования, а буква *«а»* может быть зашифрована как *«б»* или *«в»*. Более того, буква *«п»*, встречающаяся в зашифрованном тексте три раза, каждый раз означает разные буквы.

Таким образом, хотя статистические особенности исходного текста и будут проявляться с цикличностью n, где n — длина ключа, при достаточно большом n (десять и более цифр, при том, что противнику эта длина неизвестна), таблицы частот дают гораздо большую погрешность, не говоря уже о том, что проверять предположения, восстанавливая фрагменты по смыслу, становится практически невозможным.

Главная слабость шифра Гронсфельда в том, что каждая буква зашифрованного текста отстоит от «своей» буквы открытого текста не более, чем на девять позиций в алфавите, а это дает противику возможность легко проверять различные предположения. Например, предположив, что начало зашифрованного текста «йпчптпбфллв» расшифровывается как «крипто», уже на первом символе, противник отбросит этот вариант, поскольку буква *«к»* не может превратиться в *«й»* после сдвига.

Эта проблема исчезает в модификации шифра Гронфельда, где в качестве ключа выступает не цифровая, а буквенная последовательность. Порядковый номер буквы открытого текста складывается с записанной под ней буквой ключа и получается порядковый номер буквы зашифрованного текста (который берется по модулю мощности алфавита, т.е. Г + Э = 4 + 31 = 35; 35 mod 33 = 2 = Б; Г + Э = Б).

Рис. 4. Модифицированный шифр Гронсфельда

Механизм «сложения» исходного текста с ключом, представляющим собой цифровую или буквенную поседовательность, который мы наблюдали в шифрах Цезаря и Гронсфельда, используется и во многих других шифрах. Особенностью таких шифров яв-

ляется возможность восстановления ключа, если известны открытые и зашифрованный текст. Это делается операцией, обратной «сложению» — «вычитанием»[5].

Таким образом, если противник располагает открытым текстом и соответствующим ему зашифрованным текстом, он может получить ключ и попробовать применить его к другим зашифрованным текстам (поскольку нередко один ключ используется для многих сообщений). Этот метод называется *криптоанализом с известным открытым текстом* и, очевидно, шифр Гронсфельда легко ему поддается.

Для того, чтобы получить пару «открытый текст — зашифрованный текст» противник может вынудить отправителя сообщения зашифровать определенную информацию (например, в истории разведки не раз применялся прием, когда с этой целью нарочно организовывалась утечка информации). Кроме того, противник может делать предположения о словах, которые могут встречаться в тексте исходного сообщения (особенно продуктивны попытки угадать первое слово), и, пробуя эти слова, вычислять фрагменты возможного ключа. Далее эти фрагменты пробуются в других участках зашифрованного текста и, если в результате обратного преобразования получается осмысленная последовательность, криптоаналитик на верном пути.

4. Многобуквенные шифры

В определении подстановочных шифров сказано, что при шифровании может заменяться не каждый отдельный символ исходного сообщения, а сразу группа символов — на другую группу символов. Такие шифры называются *многобуквенными*. Рассмотрим *шифр Плейфейера*, в котором единицей шифрования является биграмма (пара букв), заменяемая другой парой букв.

Шифр предназначен для английского алфавита. Ключом является кодовая фраза, которая записывается в первые ячейки квадратной решетки 5x5 (повторяющиеся буквы пропускаются). Затем квадрат в алфавитном порядке заполняется буквами, которые не вошли в кодовую фразу. I и J считаются одной буквой.

Заполним решетку с ключевым словом MONARCHY.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Рис. 5. Кодовая решетка для шифра Плейфейера

Исходный текст разбивается на биграммы. При этом если две одинаковые буквы открытого текста при разбиении образуют одну биграмму, между ними вставляется символ X. Т.е. вместо BALLOON шифруем BALXLOON.

---

[5] При вычитании одного текста из другого отсчет идет по алфавиту назад. Если получилось отрицательное число, к нему прибавляется мощность (число букв) алфавита. Математически происходит вычитание порядковых номеров букв по модулю мощности алфавита.

Если буквы биграммы стоят в одной строке (столбце), они заменяются их правыми (нижними) соседями с учетом циклического сдвига. В нашем примере OR шифруется как NM, а OP — как HV.

Если буквы биграммы оказываются в разных строках и столбцах, то каждая из пары букв заменяется буквой, находящейся на пересечении ее строки и столбца, в котором находится вторая буква. Например, BE шифруется как CI, а OS — как AP.

Слово INFORMATION будет зашифровано как GAPHMORSFAAW.

Данный шифр сохраняет статистические особенности исходного текста в том смысле, что можно построить таблицу частот биграмм для языка и проанализировать частоты биграмм зашифрованного текста. Однако если букв в английском языке 26, то биграмм уже $26^2 = 676$, поэтому задача существенно усложняется и без весьма значительных объемов зашифрованного текста обречена на провал.

Другой интересный пример многобуквенного шифра — *шифр Хилла*. Он представляет собой систему из *m* линейных уравнений с *m* коэффициентами. Шифр заменяет каждые *m* букв открытого текста на *m* букв зашифрованного текста. Например, при $m = 3$ имеем систему уравнений (где n — мощность алфавита):

$$c_1 = (k_{11} p_1 + k_{12} p_2 + k_{13} p_3) \bmod n$$
$$c_2 = (k_{21} p_1 + k_{22} p_2 + k_{23} p_3) \bmod n$$
$$c_3 = (k_{31} p_1 + k_{32} p_2 + k_{33} p_3) \bmod n$$

Ключом шифрования будет являться матрица коэффициентов K, а само шифрование можно представить как произведение вектора, составленного из порядковых номеров букв открытого текста (первая буква имеет номер 0) на ключевую матрицу K:

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} k_{12} k_{13} \\ k_{21} k_{22} k_{23} \\ k_{31} k_{32} k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$$

Для расшифровки зашифрованный текст необходимо умножить на матрицу, обратную к K (K^{-1}).

Шифр Хилла также хорошо скрывает частоту символов исходного сообщения, но уязвим к криптоанализу с известным открытым текстом. Поскольку система линейная, противнику понадобится m^2 пар «открытый текст — зашифрованный текст», чтобы вычислить ключевую матрицу. Однако наиболее эффективный метод криптоанализа для данного шифра — *криптоанализ с избранным открытым текстом*, когда противник имеет возможность получать зашифрованные образцы специально подобранного им открытого текста[6]. Посмотрите, что будет представлять из себя зашифрованный текст, если зашифровать последовательность БАА ($p_1 = 1$, $p_2 = 0$, $p_3 = 0$).

5. Одноразовый блокнот

[6] Например, имеется система передачи данных по каналу связи в зашифрованном виде, которая использует один и тот же ключ для шифрования всех данных. При этом противник может перехватывать передающиеся по каналу связи зашифрованные сообщения, а также передавать свои собственные. В этом случае он может получить интересующие его пары «открытый текст — зашифрованный текст» и с их помощью провести криптоанализ ключа.

Выше были рассмотрены классические алгоритмы симметричного шифрования, применявшиеся, в докомпьютерную эпоху. Каждый из этих алгоритмов уязвим для определенных видов криптоанализа. Самые совершенные из современных алгоритмов со временем таже обнаруживают свои слабые стороны.

В настоящее время признано существование единственного алгоритма шифрования, который невозможно вскрыть. Этот шифр известен как *шифр Вернама* или *одноразовый блокнот*. Открытый текст складывается с *абсолютно случайным ключом*, совпадающим с ним по размеру[7]. После этого ключ уничтожается (т.е. не используется для шифрования других текстов). Абсолютная криптостойкость шифра доказана Клодом Шенноном.

На практике одноразовые блокноты применяются очень редко (лишь для сообщений высшей секретности). Во-первых, изготоволение такого блокнота достаточно дорого (т.к. абсолютно случайная последовательность не может генерироваться алгоритмически), а блокнот предназначен лишь для одноразового использования. Во-вторых, возникает *проблема передачи ключа:* единственный надежный вариант — личная встреча . Действительно, предположим у отправителя и получателя сообщения есть надежный канал обмена информацией. Тогда почему бы не передавать по этому каналу незашифрованные сообщения. Если же отправить ключ, зашифровав его другим алгоритмом, вся система окажется надежной не более, чем этот алгоритм.

4.5. Перестановочные алгоритмы

В перестановочных алгоритмах *символы открытого текста изменяют порядок следования в соответствии с правилом, которое определяется ключом*.

Простейший пример перестановки: символы открытого текста не слева направо, а сверху вниз, при этом длина столбца ограничена. Результатом будет текст, выписанный по строкам.

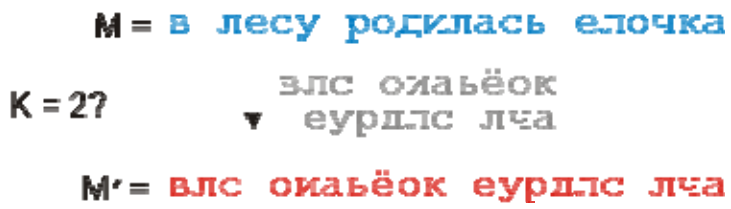

Рис. 6. Простейший перестановочный шифр.

Такой шифр будет весьма уязвим к перебору ключей (в качестве ключа будет выступать длина столбца), поскольку ключ в любом случае не может быть длиннее, чем длина самого сообщения.

Рассмотрим более интересный пример: *решетка Флейберга*. Ключом к этому шифру является квадратная решетка, стороны которой содержат четное число ячеек. Четверть ячеек решетки вырезаются по следующему принципу: если некоторая ячейка вырезана, то

[7] Сложение происходит по модулю мощности алфавита. Если зашифровывается текст, представленный в двоичном виде, то операция шифрования представляет собой исключающее или (XOR), примененное к ключу и открытому тексту.

нельзя вырезать те ячейки, в которые она переходит при повороте решетки на 90, 180 и 270 градусов.

Для того, чтобы зашифровать текст, решетка с прорезями накладывается на расчерченный квадрат, после чего буквы текста последовательно записываются в прорези. Когда все прорези заполнены, решетка поворачивается на 90 градусов, причем, согласно принципу построения решетки, прорези при этом окажутся на месте незаполненных ячеек. В прорези записывается продолжение текста, после чего рештка снова поворачивается и, таким образом, процедура повторяется еще два раза. Если текст не поместился в один квадрат, таким же образом заполняется следующий. Оставшиеся пустыми ячейки последнего квадрата заполняют случайными символами.

Рис. 7. Пример шифрования с помощью решетки Флейберга

Шифр Флейберга, очевидно, уязвим к криптоанализу с известным открытым текстом, причем для двоичного алфавита эта уязвимость значительно меньше, чем для естественно-языковых алфавитов.

4.6. Современные алгоритмы симметричного шифрования

Современные алгоритмы симметричного шифрования используют как подстановку, так и перестановку. Стандартом де-факто являются несколько раундов шифрования с разными ключами, которые генерируются на основе одного общего ключа. Большинство современных алгоритмов имеют структуру, аналогичную структуре шифра Файстеля, разработанного в 1973 году.

Шифр Файстеля создавался как пример практической реализации идеи Клода Шеннона: *надежный алгоритм шифрования должен удовлетворять двум свойствам: диффузии и коффузии.*

Диффузия — каждый бит открытого текста должен влиять на каждый бит зашифрованного текста. Суть диффузии заключается в рассеянии статистических характеристик открытого текста внутри шифрованного текста.

Конфузия — отсутствие статистической взаимосвязи между ключом и зашифрованным текстом. Даже если противник определит какие-то статистические особенности зашифрованного текста, их должно оказаться недостаточно, чтобы получить любую информацию о ключе.

Рассмотрим структуру шифра Файстеля.

Данный шифр относится к категории блочных. *Блочные шифры* предназначены для шифрования небольших блоков определенной длины. Для того, чтобы зашифровать произвольный текст, его необходимо разбить на блоки, после чего каждый блок зашифровывается отдельно (вариации рассматриваются в следующем разделе). Кроме того, как и практически все современные алгоритмы, шифр Файстеля работает с двоичным алфави-

том (т.е. и открытый и зашифрованный текст представлены последовательностью битов) и предназначен для реализации на ЭВМ.

На вход алгоритма шифрования подается блок открытого текста, имеющий четную длину *2l* и ключ *K*. Блок разделяется на две равные части — правую R0 и левую L0. Далее эти части проходят m раундов обработки, после чего снова объединяются в зашифрованный текст.

Каждый *i*-й раунд состоит в генерации подключа K_i (на основе общего ключа K) и применении к блоку R_i некоторого зависящего от ключа преобразования *F*. Результат складывается с блоком L_i с помощью операции XOR (исключающее или) и получается блок R_{i+1}. Блок R_i без изменений берется в качестве блока L_{i+1}.

Процесс дешифрования принципиально ничем не отличается, но на вход подается зашифрованный текст, а ключи K_i вычисляются в обратном порядке.

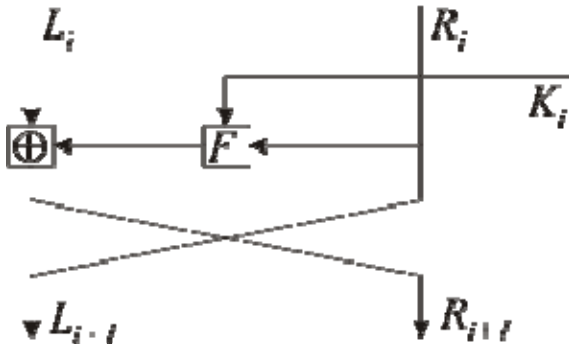

Рис. 8. Схема i-го раунда шифрования шифра Файстеля

Различные алгоритмы, использующие структуру шифра Файстеля могут отличться следующими параметрами:

1. Длина ключа. Чем длиннее ключ, предусмотренный алгоритмом, тем сложнее осуществить перебор. Сейчас надежной считается длина ключа не менее 1024 бита.

2. Размер блока. Чем выше размер блока, тем больше надежность шифра, но скорость операций шифрования/дешифрования при этом снижается.

3. Число раундов обработки. С каждым новым раундом обработки надежность шифра повышается.

4. Функция раунда *F* — чем она сложнее, тем труднее криптоанализ шифра.

5. Алгоритм вычисления промежуточных ключей K_i.

Алгоритм DES

Долгое время самым популярным алгоритмом симметричного шифрования являлся *DES* (Data Encrypting Standart), принятый в 1977 году. Этот алгоритм базируется на структуре шифра Файстеля с размером блока 64 бита и 56-битным ключом.

Функция раунда F использует набор из восьми так называемых S-матриц. Каждая матрица состоит из 4 строк, причем каждая строка представляет собой перестановку чисел от 0 до 15 (соответственно, 16 столбцов). Матрицы жестко заданы[8]. Каждая матрица по-

[8] S-матрицы считались самой сомнительной частью алгоритма DES, поскольку создатели алгоритма не раскрыли принципы их заполнения — почему выбраны именно эти матрицы и не содержит ли алгоритм

лучает на вход шесть бит и выдает четырехбитовый результат. Первый и последний бит входного значения задают строку матрицы, а четыре остальных — столбец. Двоично представление числа, находящегося на их пересечении, и будет результатом преобразования. Собственно же преобразование F заключается в следующем:

1. 32-битовый блок R_i расширяется до 48 битов с помощью специальной таблицы путем дублирования некоторых 16 битов.

2. Полученный результат складывается с 48-битным подключом K_i операцией XOR.

3. Результат сложения разбивается на 8 шестибитовых блоков и каждый из них преобразуется с помощью соответствующей S-матрицы.

4. Получившийся в итоге 32-битный блок подвергается жестко заданной в алгоритме перестановке.

Долгое время DES являлся федеральным стандартом шифрования США. Этот алгоритм показывает хороший *лавинный эффект* (изменение одного бита открытого текста или ключа приводит к изменению многих битов зашифрованного текста) и успешно противостоял многолетним попыткам взлома. Однако длина ключа в 56 битов при возросшей производительности ЭВМ сделала шифр потенциально уязвимым к перебору ключей, поэтому в 1997 году был объявлен конкурс на новый алгоритм, который должен был стать криптостандартом на ближайшие 10-20 лет.

Алгоритм AES

Победитель конкурса был определен в 2000 году — им стал бельгийский шифр RIJNDAEL, который был переименован в AES (Advanced Encryption Standard). Он является нетрадиционным блочным шифром, поскольку не использует сеть Фейштеля. Каждый блок входных данных представляется в виде двумерного массива байт (4x4, 4x6 или 4x8 в зависимости от размера блока, которая может варьироваться). В зависимости от размера блока и длины ключа алгоритм содержит от 10 до 14 раундов, в каждом из которых проводится ряд преобразований — либо над независимыми столбцами, либо над независимыми строками, либо вообще над отдельными байтами в таблице.

Среди других современных алгоритмов симметричного шифрования следует назвать шифры IDEA, Blowfish, RC5, CAST-128.

4.7. Режимы функционирования блочных шифров

Симметричные алгоритмы шифрования можно разделить на две категории: блочные и потоковые. В *потоковых* алгоритмах символы (байты или биты) исходного текста шифруются последовательно. Классическим примером является одноразовый блокнот или шифр простой замены. В *блочных* шифрах единицей шифрования является блок (последовательность бит фиксированной длины), который преобразуется в блок зашифрованного текста такой же длины. Как отмечалось выше, большинство современных симметричных алгоритмов шифрования относятся к категории блочных шифров.

«тайных ходов». Однако за годы попыток взлома этого алгоритма слабости S-матриц так и не были выявлены.

Существует четыре основных режима работы блочных шифров, которые предназначены для их оптимального применения в самых различных областях.

1. *Режим электронной шифровальной книги (ECB)*. Наиболее простой и естественный способ. Текст разбивается на блоки и каждый блок шифруется с одним и тем же ключом. Основной недостаток подхода заключается в том, что одинаковые блоки будут одинаково зашифровано, что снижает защиту в случае больших объемов шифруемой информации.
2. *Режим сцепления шифрованных блоков (CBC)*. Каждый блок открытого текста перед шифрованием объединяется с помощью операции XOR с предыдущим блоком зашифрованного текста. Первый блок объединяется с некоторым заранее заданным *инициализационным вектором*. В результате одинаковые блоки открытого текста в зашифрованном виде будут различаться.
3. *Режим шифрованной обратной связи* (CFB). Похож на предыдущий, но основное назначение состоит в том, чтобы превратить блочный шифр (например, DES с длиной блока 64 бита) в потоковый, т.е. шифрующий по одному символу (размером, например, j = 8 бит). Идея заключается в том, что изначально 64-битовый буфер заполняется значением инициализационного вектора (известного отправителю и получателю), которое шифруется ключом K. Из полученного результата выбираются старшие (левые) j бит, которые объединяются с помощью XOR с первым символом открытого текста. Получаем первый зашифрованный символ. Далее содержимое буфера сдвигается на j бит влево, а в самый младшие (правые) j бит записывается зашифрованный символ. Система готова к шифрованию следующего символа.
4. *Режим обратной связи по выходу (OFB)*. Аналогичен предыдущему, но в младшие j бит буфера после сдвига помещается не зашифрованный символ, а j сташих бит результата шифрования (т.е. до их объединения с символом открытого текста). Такой режим более устойчив к помехам (сбой при передаче одного символа зашифрованного текста не будет влиять на результаты дешифрования других символов).

4.8. Скремблеры

Одним из распространенных потоковых алгоритмов шифрования является скремблер. *Скремблерами* называются программные или аппаратные реализации алгоритма, позволяющего шифровать побитно непрерывные потоки информации. Сам скремблер представляет из себя набор бит, изменяющихся на каждом шаге по определенному алгоритму. После выполнения каждого очередного шага на его выходе появляется шифрующий бит – либо 0, либо 1, который накладывается на текущий бит информационного потока операцией XOR.

Рассмотрим пример простого скремблера. Он задается двумя битовыми последовательностями равной длины, одна из которых называется *ключом* (начальной последовательностью), а вторая собственно скремблером (часто вторая последовательность является фиксированной для конкретной аппаратной или программной реализации, а ключ выбирается как в обычном симметричном шифровании). Чем больше длина ключа (и скремблера), тем более надежным будет алгоритм.

Начальная последовательность (ключ) накладывается на скремблер, представляющий собой маску: выбираются только те биты последовательности, позициям которых соответствует единица в скремблере. Далее выбранные биты складываются между собой операцией XOR. Получается новый бит, который записывается в начало (слева) ключа. Последний (правый) бит ключа становится первым символом кодирующей последовательности и отбрасывается. Таким образом, происходит сдвиг ключа и генерация одного бита. Этот бит накладывается на первый бит исходного текста операцией XOR и получается первый бит зашифрованного текста. После этого цикл повторяется.

Пусть необходимо зашифровать сообщение 00111 скремблером 101 с ключом 011. Вычисляется сумма по модулю 2 первого и третьего бита ключа: $1 \oplus 1 = 0$. Этот бит становится новым первым битом ключа, а последний бит ключа (1) становится битом шифрующей последовательности. Вычисляем первый бит зашифрованного текста: $1 \oplus 0 = 1$. Далее повторям процесс, но уже с ключом 101. Шифрование всего сообщения показано на рисунке.

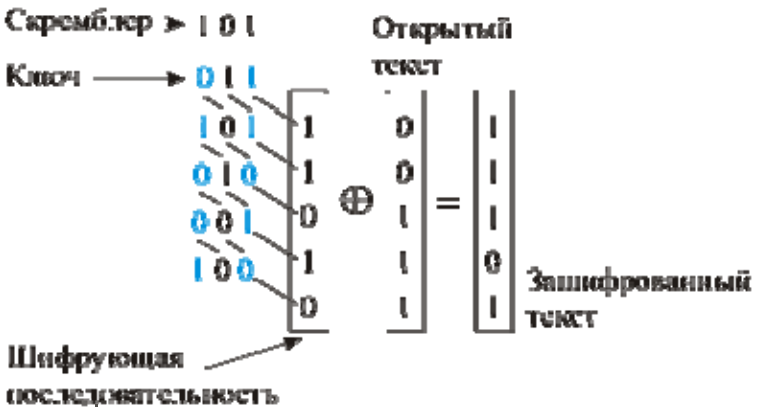

Рис. 9. Скремблирование последовательности 00111 скремблером 101 с ключом 011

4.9. Основные разновидности криптоанализа симметричных шифров

Классическая задача криптоанализа — получение открытого текста по зашифрованному тексту, не располагая при этом ключом. Часто под этим подразумевается нахождение ключа.

Некоторые методы криптоанализа шифров обсуждались выше при рассмотрении соответствующих алгоритмов шифрования.

Одна из популярных классификаций методов криптоанализа — по тем данным, которыми должен располагать аналитик. Соответственно выделяют:

— *Анализ только шифрованного текста*. Криптоаналитику известны алгоритм шифрования и зашифрованный текст.

— *Анализ с известным открытым текстом.* Криптоаналитик дополнительно располагает несколькими парами соответствующих друг другу фрагментов открытого и зашифрованного текста, созданного с одним и тем же ключом.

— *Анализ с избранным открытым текстом.* Криптоаналитик имеет возможность выбирать открытый текст для шифрования (т.е. располагает интересующим его открытым текстом и соответствующим ему зашифрованным).

— *Анализ с избранным зашифрованным текстом.* Криптоаналитик имеет возможность выбирать получать открытый текст для некоторых интересующих его образцов открытого текста.
— *Анализ с избранным текстом.* Возможности криптоаналитика включают два предыдущих случая.

Существуют также отдельные методы криптоанализа, широко применяющиеся для взлома современных шифров. Перечислим наиболее известные из них.

Статистический криптоанализ. Основан на подсчете частоты встречаемости отдельных символов (или групп символов) в зашифрованном тексте. Подходит для взлома симметричных подстановочных алгоритмов.

Дифференциальный криптоанализ. Разновидность анализа с избранным открытым текстом. Используется при взломе современных симметричных алгоритмов шифрования, в которых текст последовательно проходит несколько раундов преобразований (в частности, известен алгоритм дифференциального криптоанализа шифра DES). Метод основан на прослеживании изменения схожести между двумя текстами. Выбирается пара незашифрованных текстов с определенным отличием (X), после чего анализируются отличия, получившиеся после шифрования одним раундом алгоритма, и определяются вероятности различных ключей. Если для многих пар входных значений, имеющих одно и то же отличие X, при использовании одного и того же подключа одинаковыми (Y) оказываются и отличия соответствующих выходных значений, то можно говорить, что X влечет Y с определенной вероятностью. Эта вероятность и присваивается данному подключу раунда. Затем выбирается подключ с наибольшей вероятностью. Процесс повторяется для всех раундов. Цель — определить таким образом все подключи данного ключа (сам ключ при этом может остаться неизвестным).

Линейный криптоанализ. Применяется для взлома блочных симметричных шифров. В основе лежит понятие линейного приближения — предположение о том, что если выполнить выполнить операцию XOR над некоторыми битами открытого текста, затем над некоторыми битами шифротекста, а затем над результатами, получится бит, который представляет собой XOR некоторых бит ключа. Если это предположение верно с вероятностью выше ½, то на основе большого числа известных пар открытый текст/зашифрованный текст можно с удовлетворительной вероятностью определить значения отдельных битов ключа.

4.10. Проблемы симметричных алгоритмов

Все алгоритмы симметричного щифрования имеют общую проблему, проистекающую из того обстоятельства, что и отправитель и получатель сообщения должны обладать одним и тем же ключом. При этом предполагается, что у них нет абсолютно надежного канала связи, поскольку в противном случае в шифровании бы не было нужды.

Если столетие назад эта проблема вполне решалась, например, путем личной встречи. Но в настоящее время, когда интенсивность обмена информацией возросла в сотни раз и автоматизированы практически все сферы человеческой деятельности, это невозможно. Необходимость в срочной конфиденциальной переписке может возникнуть у деловых партнеров, живущих в разных странах (и, может быть, даже не знакомых лично). Интернет-банкинг позволяет управлять своим банковским счетом, не выходя из дома, но при

этом все операции должны быть конфиденциальными, а следовательно, весь поток данных между банком и клиентом должен быть зашифрован. При этом ключи шифрования должны регулярно меняться, поскольку обмен даже несколькими сообщениями с одним ключом уменьшает надежность шифрования.

Таким образом, для симметричных алгоритмов характерна *проблема обмена ключами*. В настоящее время существует несколько способов ее решения, которые будут рассматриваться далее.

Кроме того, возникает проблема управления большим количеством ключей, поскольку отдельный ключ необходим для каждой пары «отправитель-получатель». Если группа из n человек желает обмениваться конфиденциальными сообщениями, понадобится $O(n^2)$ ключей (n-1 ключ каждому). Если же группа будет использовать один общий ключ, то его компрометация (утечка) у одного члена скомпрометирует переписку всей группы.

Эти проблемы и привели к появлению в середине XX века приницпиально нового класса алгоритмов шифрования.

Тест для самоконтроля № 2

1. Какие из этих утверждений, относящихся к шифру Плейфейра, верны?

а) шифр Плейфейера относится к моноалфавитным шифрам;

б) шифр Плейфейера относится к подстановочным шифрам;

в) единицей шифрования в шифре Плейфейера является биграмма;

г) шифр Плейфейера уязвим для взлома методом перебора ключей.

2. Зашифруйте сообщение 01010 скремблером 101 с ключом 011

3. В чем заключается главная слабость моноалфавитного шифра?

а) в небольшом количестве возможных ключей (уязвим к перебору)

б) зашифрованный текст сохраняет статистические особенности открытого текста;

в) если два текста зашифрованы одним и тем же ключом, шифр вскрывается автоматически;

г) противник может узнать ключ, получив достаточное количество образцов открытого и зашифрованного текстов.

4. Зашифруйте слово «КНИГА» шифром Гронсфельда с ключом 12.

5. Зашифруйте слово «КНИГА» шифром Цезаря.

6. Какой метод криптоанализа наиболее эффективен для взлома шифра Хилла?

а) Анализ с избранным текстом;

б) Анализ с избранным зашифрованным текстом;

в) Анализ с избранным открытым текстом;

г) Анализ с известным открытым текстом

д) Анализ только шифрованного текста.

7. Что такое симметричное шифрование?

а) способ шифрования, при котором каждый символ (или последовательность символов) исходного сообщения заменяются другим символом (или другой последовательностью символов);

б) способ шифрования, при котором один и тот же ключ используется и для шифрования и для расшифрования текста;

в) способ шифрования, при котором используются два свзяанных ключа: один для шифрования, другой для расшифрования;

г) способ шифрования, при котором символы открытого текста изменяют порядок следования в соответствии с правилом, которое определяется ключом.

8. Какой из перечисленных шифров является самым надежным?

а) шифр Плейфейера;

б) шифр Хилла;

в) одноразовый блокнот;

г) шифр Цезаря;

д) моноалфавитный шифр.

9. Как называется свойство современных симметричных алгоритмов: каждый бит открытого текста должен влиять на каждый бит зашифрованного текста?

10. В чем заключается основная проблема использования симметричных алгоритмов?

а) Сложность реализации на ЭВМ;

б) Легкость криптоанализа таких шифров с появлением ЭВМ;

в) Трудности при передаче ключей и управлении ими;

г) Работа этих алгоритмов на ЭВМ требует значительных вычислительных ресурсов.

11. Какой метод криптоанализа использует предположение о том, что если выполнить выполнить операцию XOR над некоторыми битами открытого текста, затем над некоторыми битами шифротекста, а затем над результатами, получится бит, который представляет собой XOR некоторых бит ключа?

а) дифференциальный;

б) статистический;

в) линейный.

12. Как называется режим шифрования блочных шифров, при котором текст разбивается на блоки и каждый блок шифруется с одним и тем же ключом?

а) Режим сцепления шифрованных блоков;

б) Режим шифрованной обратной связи;

в) Режим обратной связи по выходу;

г) Режим электронной шифровальной книги.

Глава 5. Шифрование с открытым ключом. ЭЦП

5.1. Алгоритмы шифрования с открытым ключом

В *алгоритмах шифрования с открытым ключом* каждый пользователь имеет пару ключей, связанных друг с другом некоторой зависимостью. Ключи обладают свойством: *текст, зашифрованный одним ключом, может быть расшифрован только с помощью парного ему ключа*. Один ключ называется *секретным (закрытым) ключом*. Пользователь хранит свой секретный ключ в надежном месте и никому его не передает. Второй ключ называется *открытым ключом*, и пользователь, напротив, сообщает его всем желающим (а также может опубликовать в любом общедоступном источнике).

Если пользователь A хочет отправить зашифрованное послание пользователю B, он шифрует его с помощью открытого ключа B. Теперь текст не сможет прочесть никто, кроме B (даже сам A), поскольку для дешифрования нужен закрытый ключ.

Схему шифрования можно записать в следующем виде:

$M' = E(M, K_{откр})$

$M = D(M', K_{закр})$,

где E — функция шифрования (encrypt), D — функция дешифрования (decrypt), а $K_{откр}$ и $K_{закр}$ — соответственно открытый и закрытый ключи *получателя* сообщения.

Принципиальный метод шифрования с открытым ключом впервые был публично предложен в 1976 году Диффи и Хеллманом. При этом они не смогли придумать конкретного алгоритма, но сформулировали принципиальные условия, которым такие алгоритмы должны удовлетворять:

1. Процесс генерации пары ключей (открытый и закрытый) не должен представлять вычислительных трудностей.

2. Процесс зашифрования текста, т.е. вычисления $E(M, K_{откр})$, а также процесс дешифрования, т.е. вычисления $D(M', K_{закр})$ также не должны представлять вычислительных трудностей.

3. Для противника должно быть невозможно (с точки зрения вычислительных возможностей) вычисление закрытого ключа $K_{закр}$ по имеющемуся открытому ключу $K_{откр}$.

4. Для противника должно быть невозможно (с точки зрения вычислительных возможностей) вычисление открытого текста M по имеющемуся зашифрованному тексту M' и открытому ключу $K_{откр}$.

Кроме этого желательно, чтобы операции шифрования и дешифрования выполнялись в любом поряке, т.е. можно было бы зашифровать текст закрытым ключом, а расшифровать открытым. Преимущества этой возможности будут рассмотрены позже.

Алгоритм RSA

RSA — один из первых алгоритмов шифрования с открытым ключом — разработан в 1977 году, название составлено из первых букв имен его авторов (Райвест, Шамир и Адлеман). На протяжении двадцати лет он был самым опулярным и практически единственным широко использующимся алгоритмом с открытым ключом.

Рассмотрим этот алгоритм подробно.

Для генерации ключей выбираются два больших случайных простых числа p и q и вычисляется их произведение $n = pq$. Затем вычисляется функция Эйлера:

$$\varphi(n) = (p-1)(q-1)$$

Далее выбирается целое число e, такое что $1 < e < \varphi(n)$ и e взаимно просто с $\varphi(n)$. Находится число d такое, что $ed \equiv 1 \pmod{\varphi(n)}$. Это может быть сделано, например, при помощи расширенного алгоритма Евклида.

Открытым ключом является пара чисел (n, e), а закрытым ключом — пара (n, d).

Как видно, для того, чтобы по открытому ключу определить закрытый, необходимо вычислить $\varphi(n)$, а для этого большое (на практике порядка 1024 битов) число n необходимо разложить на простые множители. Но эффективного алгоритма разложения числа на простые множители не существует.

RSA предназначен для шифрования двоичных текстов. Открытый текст разбивается на блоки и каждый блок рассматривается как двоичное число M. При этом должно соблюдаться ограничение M < n, исходя из этого условия выбираются длина блока и минимально возможные значения p и q.

Для того, чтобы зашифровать сообщение, вычисляется

$$M' = M^e \bmod n$$

Для дешифрования необходимо вычислить

$$M = M'^d \bmod n$$

Убедимся в корректности алгоритма.

$$M'^d \bmod n = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n$$

Т.к. $ed \equiv 1 \pmod{\varphi(n)}$, то $ed \equiv k\varphi(n) + 1$ для некоторого целого k. Отсюда:

$$M^{ed} \bmod n = M^{k\varphi(n)+1} \bmod n$$

По теореме Эйлера $M^{\varphi(n)} \equiv 1 \pmod{n}$. Т.о.:

$$M^{k\varphi(n)+1} \bmod n = M$$

Получили $M'^d \bmod n = M$, что и требовалось доказать.

Очевидно, что открытый и закрытый ключ в алгоритме RSA взаимозаменяемы: то, что зашифровано одним из них, расшифровывается другим.

Недостатком алгоритмов с открытым ключом является низкая скорость выполняемых операций. Так, в алгоритме RSA шифрование и дешифрование заключается в возведении очень большого числа в очень большую степень, а это достаточно ресурсоемкая операция.

Поэтому на практике чаще всего используется комбинация двух алгоритмов. Сообщение шифруется с помощью симметричного алгоритма шифрования (например, AES). При этом каждый раз генерируется новый случайный ключ. Этот ключ зашифровывается открытым ключом получателя (например, с помощью RSA) и отправляется вместе с сообщением. Такая гибридная схема обеспечивает как скорость операций шифрования/дешифрования, так и надежность.

5.2. Электронная цифровая подпись

Как отмечалось выше, многие алгоритмы шифрования с открытым ключом работают со взаимозаменяемой парой ключей, т.е. любым из них можно зашифровать текст и тогда расшировываться он будет вторым ключом.

Для целей конфиденциальности текст шифруется открытым ключом получателя.

Рассмотрим ситуацию, когда сообщение шифруется закрытым ключом отправителя. В этом случае расшифровать его сможет кто угодно, поскольку открытый ключ общедоступен. Однако получатель сообщения может быть уверен в том, что подлинный автор сообщения — владелец закрытого ключа, поскольку никто другой не имеет возможности его создать (при условии, что закрытый ключ не скомпрометирован, т.е. не украден). Таким образом, достигается *аутентичность* (подлинность) сообщения. С юридической точки зрения это означает, что автор сообщения не сможет от него отказаться (апеллируемость).

Эта идея нашла свое воплощение в концепции *электронной цифровой подписи*.

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Такое определение приводится в ст. 3 федерального закона «Об электронной цифровой подписи».

В качестве электронной цифровой подписи может выступать сам текст сообщения, зашифрованный закрытым ключом отправителя. Однако такой вариант не используется в силу его неэффективности. Во-первых, шифрование/дешифрование всего текста занимает очень много времени. Во-вторых, длина ЭЦП в этом случае будет равна (и даже превышать) длину исходного сообщения, что создает неудобство при пересылке. Поэтому современные алгоритмы электронной цифровой подписи основаны на использовании *хэш-функций*.

Хэш-функцией называется функция (H), которая принимает на входе сообщение M произвольной длины, а на выходе выдает значение H(M) фиксированной длины, называемое *хэшем* или *профилем* сообщения M. При этом в криптографии (в частности, в алгоритмах ЭЦП) используются функции, обладающие следующими свойствами:

1. *Односторонность*. Для любого хэша h должно быть практически невозможно вычислить или подобрать такое x, что $H(x) = h$.
2. *Стойкость к коллизиям первого рода*. Для любого сообщения x должно быть практически невозможно вычислить или подобрать другое сообщение y, такое что $H(x) = H(y)$.
3. *Стойкость к коллизиям второго рода*. Должно быть практически невозможно вычислить или подобрать любую пару различных сообщений x и y для которых $H(x) = H(y)$.

Среди наиболее известных алгоритмов хэширования можно назвать MD5, SHA-512, ГОСТ Р34.11-94 (российский стандарт вычисления хэш-функции).

Электронная цифровая подпись, основанная на применении хэш-функций, вычисляется следующим образом:

1. Для сообщения M вычисляется хэш H(M).
2. Хэш шифруется с помощью закрытого ключа отправителя, т.е. вычисляется $E(H(M), K_{закр})$, где E — функция шифрования асимметричного алгоритма.
3. Полученное значение берется в качестве электронной цифровой подписи для сообщения M. Сообщение пересылается получателю вместе с ЭЦП (при этом ЭЦП обычно пересылается отдельным файлом, хотя может и припысываться к сообщению). Если необходимо обеспечить как аутентичность, так и конфиденциальность, сообщение M предварительно зашифровывается открытым ключом получателя[9].

Чтобы убедиться в подлинности полученного сообщения, необходимо проделать шаги алгоритма в обратном порядке:

1. Полученная электронная цифровая подпись h расшифровывается открытым ключом предполагаемого отправителя сообщения, т.е. вычисляется $D(h, K_{откр})$.
2. Вычисляется хэш полученного сообщения H(M).
3. Если $D(h, K_{откр}) = H(M)$, то сообщение подлинно. В противном случае оно признается неаутентичным (возможно, оно было изменено при пересылке, либо создано другим лицом).

Свойства криптографически стойкой хэш-функции обеспечивают надежность электронной цифровой подписи. Действительно, если изменить в оригинальном сообщении хотя бы один символ, его хэш (а следовательно, и ЭЦП) изменится, а подобрать другое сообщение с таким же хэшем невозможно. При этом, очевидно, что, поскольку длина хэша фиксирована (например, 512 бит), а различных сообщений — бесконечное число, то для любого сообщения найдется бесконечно много сообщений, имеющих точно такой же хэш. Но вероятность случайно выбрать такое сообщение обратно пропорциональная числу всевозможных хэшей и при длине 512 бит равна:

$$p = \frac{1}{2^{512}},$$

то есть практически ничтожна.

Таким образом, алгоритм электронной цифровой подписи может представлять собой простое объединение некоторого алгоритма шифрования с открытым ключом и некоторого алгоритма (функции) хэширования. При этом, если новые исследования криптоанализа обнаруживают слабость в одном из этих алгоритмов, его легко заменить на более современный и надежный.

Но при всей надежности этих алгоритмов электронная цифровая подпись имеет одну серьезную организационную слабость. Дело в том, что получатель сообщения не всегда может надежно удостовериться, что открытый ключ, который он использует для проверки ЭЦП действительно принадлежит лицу, называющему себя автором сообщения. А при этом никто не мешает злоумышленнику разместить, например, на сайте свой открытый ключ от имени другого человека, а затем отправлять сообщения, подписанные электронной цифровой подписью его от же имени.

Эффективное функционирование ЭЦП в глобальном масштабе (когда необходимость в аутентичном обмене сообщениями постоянно появляется у множества лично не

[9] При этом с точки зрения безопасности надежнее вычислять ЭЦП для уже зашифрованного сообщения.

знакомых друг с другом людей) возможно лишь с участием третьей стороны — посредника, которому доверяют все участники обмена сообщениями. Эта сторона выполняет роль удостоверяющего центра.

В федеральном законе «Об электронной цифровой подписи» устанавливаются правовой статус удостоверяющих центров (УЦ) и их функции. В частности, удостоверяющий центр выдает так называемые *сертификаты ключа подписи*, содержащие следующие сведения (ст. 6):

— Уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания его срока действия;
— Фамилия, имя, отчество или псевдоним владельца сертификата ключа подписи;
— Открытый ключ электронной цифровой подписи;
— Наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;
— Сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

УЦ обязан вести реестр сертификатов ключей подписей и обеспечивать участникам информационного обмена свободный доступ к содержащимся в нем сведениям. Удостоверяющий центр должен подтверждать подлинность электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей.

Таким образом, каждому участнику обмена сообщениями достаточно быть уверенным в подлинности «своего» удостоверяющего центра.

Забота о защите своего закрытого ключа от компрометации возлагается законом на его владельца. Согласно ст. 12 ФЗ «Об электронной цифровой подписи», он обязан хранить закрытый ключ в тайне и немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа ЭЦП нарушена. В противном случае на него возлагается возмещение причиненных убытков[10].

5.3. Российский стандарт электронной цифровой подписи ГОСТ Р 34.10—2001

Отечественный стандарт ГОСТ Р 34.10—2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» определяет схему электронной цифровой подписи, процессы формирования и проверки цифровой подписи под заданным сообщением (документом), передаваемым по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения.

В алгоритме, утвержденном данным стандартом, хэш сообщения обрабатывается алгоритмом, основанном на математике эллиптических кривых.

Пусть задано простое число $p > 3$. Тогда *эллиптической кривой* E, определенной над конечным простым полем F_p, называется множество пар чисел, удовлетворяющих тождеству:

$$y^2 = x^3 + ax + b \pmod p,$$

где $a, b < p$ и $4a^3 + 27b^2$ не делится на p.

[10] На практике это чаще всего означает, что он считается автором отправленных от его имени сообщений со всеми вытекающими юридическими последствиями.

Суммой двух точек эллиптической кривой Q_1 и Q_2 с координатами (x_1, y_1) и (x_2, y_2) назовем точку Q_3, координаты которой определяются сравнениями:

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p, \quad y_3 = \lambda(x_1 - x_3) + y_1 \pmod p, \quad где \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$

в случае, если $x_1 \neq x_2$, и сравнениями:

$$x_3 = \lambda^2 - 2x_1 \pmod p, \quad y_3 = \lambda(x_1 - x_3) + y_1 \pmod p, \quad где \quad \lambda = \frac{3x_1^2 + a}{2y_1} \pmod p$$

в противном случае.

Если выполнено условие $x_1 = x_2$, $y_1 = -y_2$, то сумма точек Q_1 и Q_2 называется нулевой точкой O (без уточнения ее координат).

В алгоритме используются следующие параметры:

простое число p — модуль эллиптической кривой, удовлетворяющее неравенству $p > 2^{255}$;

E — эллиптическая кривая, задаваемая коэффициентами a и b;

m — целое число; порядок группы точек эллиптической кривой E; $m \neq p$.

q — простое число; порядок циклической подгруппы группы точек эллиптической кривой E, для которого выполнены следующие условия:

$$m = nq, \quad n \in Z, \quad n \in 1, 2^{254} \in q \in 2^{256}$$

точка $P \neq O$ эллиптической кривой E, с координатами (x_p, y_p), $qP \neq O$.

Ключ подписи — целое d; $0 < d < q$.

Ключ проверки — точка эллиптической кривой Q с координатами (x_q, y_q), удовлетворяющая равенству $dP = Q$.

Для формирования электронной цифровой подписи сообщения M применяется следующая последовательность шагов:

1. Вычисляется хэш-код сообщения M: $\bar{h} = h(M)$. Здесь h — функция хэширования, описанная в отечественном стандарте ГОСТ Р 34.11—94.
2. Вычисляется целое число a, двоичным представлением которого является вектор $\bar{h}$, и определяется число $e = a \pmod q$.
3. Генерируется случайное целое число k, удовлетворяющее неравенству: $0 < k < q$.
4. Вычисляется точка эллиптической кривой $C = kP$ и определяется $r = x_C \pmod q$, где x_C — x-координата точки C. Если $r = 0$, возвращение к шагу 3.
5. Вычисляется значение $s = (rd + ke) \pmod q$. Если $s = 0$, возвращение к шагу 3.
6. Вычисляются двоичные векторы, соответствующие r и s. Цифровая подпись будет представлять собой конкатенацию двух двоичных векторов.

Для проверки электронной цифровой подписи сообщения M применяется следующая последовательность шагов:

1. По полученной подписи вычисляются r и s. Если не соблюдаются условия $0 < r < q$, $0 < s < q$, подпись неверна.
2. Вычисляется хэш-код полученного сообщения M: $\bar{h} = h(M)$.
3. Вычисляется целое число a, двоичным представлением которого является вектор $\bar{h}$, и определяется число $e = a \pmod q$. Если $e = 0$, берется $e = 1$.
4. Вычисляется значение $v = e^{-1} \pmod q$.

5. Вычисляются значения $z_1 = sv \pmod q$, $z_2 = -rv \pmod q$.
6. Вычисляется точка эллиптической кривой $C = z_1P + z_2Q$ и определяется $R = x_C \pmod q$.
7. Если выполнено равенство R = r, подпись принимается; в противном случае подпись неверна.

Доказательство правильности алгоритма выходит за рамки настоящего учебника и может быть выведено самостоятельно после более подробного ознакомления с математикой эллиптических кривых. Следует отметить, что криптосистемы на основе эллиптических кривых занимают все большее место в схемах ЭЦП, асимметричного шифрования и выработки пар связанных ключей.

5.4. Российский стандарт хэширования ГОСТ Р 34.11—94

Отечественый стандарт хэширования ГОСТ Р 34.11—94 является обязательным для применения в системах защиты государственных и ряда коммерческих организаций РФ. Он используется в рассмотренном выше стандарте электронной цифровой подписи и, в свою очередь, сам базируется на алгоритме симметричного шифрования ГОСТ 28147—89. Коротко алгоритм хэширования можно представить следующим образом:

1. Инициализируется так называемый регистр хэш-значения.
2. Сообщение дополняется в конце нулями таким образом, чтобы его длина стала кратной 256.
3. Сообщение разбивается на 256-битные блоки. На основе очередного блока вычисляется ключ шифрования. С использованием этого ключа содержимое регистра хэш-значения шифруется по алгоритму ГОСТ 28147—89. Результат подвергается функции перемешивания и помещается в регистр.
4. Результат, полученный в регистре после обработки последнего блока сообщения, и будет искомым хэш-значением.

Глава 6. Криптографические протоколы

6.1. Понятие криптографического протокола

Протокол — это последовательность шагов, которые предпринимают две или большее количество сторон для совместного решения некоторой задачи. Все шаги предпринимаются в порядке строгой очередности и ни один из них не может быть сделан прежде, чем закончится предыдущий.

Криптографические протоколы используются для выполнения некоторых действий по обмену информацией в ситуации, когда цели участников могут быть нарушены злоумышленником (например, под угрозой оказывается конфиденциальность, целостность или подтверждаемость сообщений). Шаги криптографического протокола позволяют осуществить информационный обмен таким образом, что цели участников оказываются выполненными, а цели злоумышленника — нет.

Приведенная в предыдущем разделе последовательность шагов по созданию и проверке электронной цифровой подписи может служить примером протокола, в котором целью участников являются гарантия подлинности сообщения, а целью злоумышленника — его фальсификация.

Криптографические протоколы широко используют шифрование, хэширование, односторонние функции, генерацию случайных чисел.

6.2. Протоколы аутентификации

Аутентификация пользователей — процесс, с помощью которого одна сторона (проверяющий) убеждается в идентичности другой стороны.

Протоколы аутентификации должны обеспечивать защиту от потенциального злоумышленника, цель которого — выдать себя за другого пользователя. В частности, протокол аутентификации не должен позволить проверяющему получить такую информацию о стороне, доказывающей свою подлинность (аутентичность), которая впоследствии помогла бы ей выдать себя за нее.

Все протоколы аутентификации можно разбить на три класса:

1. На основе знания чего-либо. Наиболее распространенный вариант — пароли.
2. На основе обладания чем-либо (магнитные карты, смарт-карты и т.д.)
3. На основе неотъемлемых характеристик (голос, сетчатка глаза, отпечатки пальцев). В данной категории криптографические методы обычно не используются.

Также протоколы аутентификации классифицируются по уровню обеспечиваемой безопасности:

1. Простая аутентификация (на основе паролей). Самый простой вариант такой аутентификации — когда система хранит пароли в открытом виде в специальном файле и сравнивает с ними пароль, вводимый пользователем при входе в систему. С точки зрения безопасности такой подход очень уязвим: файл с паролями может быть похищен злоумышленником. Поэтому гораздо надежнее, когда в специальном файле хранятся только хэши паролей. Когда пользователь вводит пароль, вычисляется его хэш с сравнивается. Если злоумышленник похитит файл, содержащихся в нем хэшей будет недостаточно, чтобы восстановить пароли.

2. Строгая аутентификация (на основе криптографических методов). Чаще всего заключается в том, что пользователь идентифицируется по признаку владения некоторым закрытым ключом, но сам ключ в ходе протокола не раскрывается.
3. Протоколы доказательства с нулевым разглашением.

Рассмотрим примеры протоколов:

Строгая односторонняя аутентификация на основе случайных чисел. Обе стороны разделяют (им известен) общий ключ K и выбрали симметричный алгоритм шифрования.

1. Сторона B (проверяющий) генерирует случайное число r и отправляет его стороне A.
2. Сторона A составляет сообщение, включающее полученное число r и свое имя, шифрует его ключом K и отправляет стороне B.
3. Сторона B расшифровывает сообщение и убеждается в том, что имя A и число r совпадает.

Если злоумышленник перехватывает отправляемые по сети сообщения, он не сможет воспользоваться ими, чтобы выдать себя за A или B, поскольку ключ K в явном виде не передается, а каждый сеанс аутентификации использует новое случайное число.

Строгая двусторонняя аутентификация на основе случайных чисел. Двусторонность означает, что во время сеанса аутентификации обе стороны убеждаются в подлинности друг друга. Обмен сообщениями происходит по следующей схеме:

B $\rightarrow$ A: случайное число r_1.

A $\rightarrow$ B: сообщение, содержащее r_1, имя B и случайное число r_2, зашифрованное ключом K.

B $\rightarrow$ A: сообщение, содержащее r_1 и r_2, зашифрованное ключом K.

Аутентификация на основе асимметричного алгоритма.

1. Сторона B (проверяющий) выбирает случайное число r и отправляет стороне B набор значений: H(r), B, P_A(r, B). Здесь H — некоторая хэш-функция, а P_A — алгоритм асимметричного шифрования (шифрование осуществляется посредством открытого ключа A).
2. Сторона A расшифровывает P_A(r, B), убеждается, что хэш r совпадает с полученным значением H(r) и отправляет стороне B число r.
3. Сторона B проверяет полученное значение и, если оно совпадает с r, убеждается в подлинности A (т.е. в том, что сторона A знает закрытый ключ).

6.3. Протоколы обмена ключами

Протокол обмена ключами — это такой протокол, с помощью которого знание некоторого секретного ключа (который может впоследствии использоваться для шифрования с помощью симметричного алгоритма) разделяется между двумя или более сторонами, причем противник, имеющий возможность перехватывать пересылаемые сообщения, не способен этот ключ получить.

Различают три вида протоколов обмена ключами: протоколы передачи (уже сгенерированных) ключей, протоколы совместной выработки общего ключа и схемы предварительного распределения ключей.

Схема предварительного распределения ключей состоит из двух алгоритмов: распределения исходной ключевой информации и формирования ключа. С помощью первого алгоритма генерируется открытая часть исходной ключевой информации, которая размещается на общедоступном сервере и секретные части (для каждой стороны). Второй предназначен для вычисления действующего ключа для взаимодействия между абонентами по имеющимся у них секретной и общей открытой части исходной ключевой информации. Применяется для уменьшения объема хранимой и распределяемой секретной ключевой информации. Схема предварительного распределения ключей должна быть устойчивой, то есть учитывать возможность раскрытия части ключей при компрометации (утечке), обмане или сговоре части абонентов и гибкой — допускать возможность быстрого восстановления путем удаления скомпрометированных ключей и подключения новых абонентов[11].

Один из самых известных протоколов обмена ключами — *алгоритм Диффи-Хеллмана*. Он является весьма надежным для обмена ключами по каналу, исключающему возможность модификации (т.е. злоумышленник имеет возможность перехватывать данные, но не изменять их). Стойкость алгоритма проистекает из сложности дискретного логарифмирования: не существует эффективного алгоритма решения уравнения $a^x \bmod n = b$ (для простого n такое $x < n$ существует и единственно).

1. Участники обмена ключами выбирают два больших числа v и n (эти числа могут быть определены заранее и даже быть фиксированными, например, «зашитыми» в программное обеспечение).
2. Каждый участник генерирует случайное простое число (x и y соответственно).
3. Первый участник вычисляет значение $v^x \bmod n$ и пересылает его второму, а второй вычисляет $v^y \bmod n$ и передает первому.
4. Первый участник возводит полученное значение в степень x по модулю n, а второй участник — в степень y по модулю n. В результате оба участника получают одно и то же число $v^{xy} \bmod n$. Оно и берется в качестве секретного ключа.

Нетрудно заметить, что, располагая значениями v, n, $v^x \bmod n$ и $v^y \bmod n$, но не зная x и y, злоумышленник не может вычислить ключ $v^{xy} \bmod n$.

6.4. Специфические протоколы

Протоколы аутентификации и протоколы обмена ключами — наиболее многочисленные классы криптографиечских протоколов. Однако существует ряд протоколов, предназначенных для решения других специфических задач, в частности:

Протоколы голосования. Предназначены для обеспечения проведения выборов, в ходе которых каждый участник может анонимно подать свой голос. При этом ни один участник не может проголосовать дважды; голосовать могут только зарегистрированные участники; каждый участник может проверить, правильно ли учтен его голос.

Протокол безопасного голосования основывается на использовании двух доверенных сторон — агентства по проверке голосующего T_1 и агентства для подведения итогов голосования T_2. Перед проведением голосования T_1 должно отослать T_2 список всех разрешенных идентификаторов участников голосования. Каждый голосующий (i) посылает

[11] Б.А. Погорелов, А.В.Черемушкин, С.И.Чечета. Об определении основных криптографических понятий. http://www.ict.edu.ru/ft/002455/pogorelov.pdf

T_1 некоторую идентифицирующую его информацию, после чего, если голосующему разрешено голосовать, то T_1 отправляет ему значение $E_1(i)$ — идентификатор голосующего и фиксирует факт участия в выборах. Далее голосующий вычисляет секретный идентификатор $E_2(i)$ и результат голосования $E_3(i)$ и посылает T_2 набор $(E_1(i), E_2(i), E_3(i))$. T_2 проверяет, существует ли $E_1(i)$ в списке разрешенных идентификаторов голосующих; если существует, то добавляет $E_2(i)$ к списку голосующих за $E_3(i)$. Преобразования E_1, E_2, и E_3 основаны на асимметричных алгоритмах или необратимых функциях[12].

Протоколы одновременной подписи. Цель участников: подписать некоторый документ таким образом, чтобы каждая сторона имела гарантию, что если она поставит свою подпись, это сделает и другая сторона. При этом участники могут быть удалены друг отдруга и подписывать документ при помощи ЭЦП.

Протоколы групповой подписи. Только члены группы могут подписывать сообщение, при этом получатель подписи может убедиться, что сообщение подписано членом группы, но не может определить — каким именно. Тем не менее, при споре подпись может быть раскрыта для определения личности подписавшего.

Самый простой протокол групповой подписи — с использованием доверенного арбитра. Арбитр генерирует большое количество пар открытых и закрытых ключей и раздает их членам группы (по m ключей каждому из n членов). Список открытых ключей публикуется. Чтобы подписать сообщение, член группы выбирает любой из своих закрытых ключей. Чтобы убедиться, что сообщение подписано одним из членов группы, достаточно проверить, что открытый ключ, с помощью которого проверяется ЭЦП, входит в набор открытых ключей группы. Наконец, проверка личности подписавшего определяется посредством обращения к арбитру. Единственная слабость этого протокола — сам арбитр, который может подделывать подписи всех участников.

Неоспариваемая подпись. Отличается от обычной цифровой подписи тем, что для ее проверки необходимо разрешение подписавшего.

Слепая подпись. Обладает свойствами электронной цифровой подписи, но при этом подписывающий не может ознакомиться с содержанием документа (пример: заверение завещания у нотариуса).

Протоколы разделения секрета. Позволяют разделить сообщение на несколько частей между членами группы таким образом, что каждый член группы не сможет извлечь никакой информации из своей части и только собравшись вместе участники группы смогут прочитать сообщение.

Наиболее распространенный протокол разделения секрета требует участия арбитра, который генерирует множество бессмысленных сообщений, которые дают исходное, будучи сложенными вместе операцией XOR. Например, чтобы разделить сообщение между двумя участниками арбитр генерирует случайное число R той же длины, что и исходное сообщение M, а затем вычисляет $R \oplus M = S$. Части R и S раздаются участникам. Чтобы получить исходное сообщение, выполняется операция $R \oplus S = M$.

[12] См. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. — М.: ДМК, 2000. С. 158.

6.5. Генерация случайных чисел

Большое значение для криптографии имеет генерация истинно случайных (непредсказуемых) чисел. Случайные числа используются при генерации сеасовых ключей (а также открытых и закрытых ключей асимметричных алгоритмов), во многих криптографических протоколах. Многие приложения имеют уязвимости связанные именно с предсказуемостью генерируемых паролей, сеансовых ключей и т.д.

Проблема заключается в том, что программное приложение не может генерировать абсолютно случайные числа в силу свойства детерминированности алгоритма. Поэтому для целей криптографии используются генераторы псевдослучайных чисел.

Генератор псевдослучайных чисел (ГПСЧ) — алгоритм, генерирующий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению (обычно равномерному).

Криптографически стойкие генераторы псевдослучайных чисел должны обладать следующими свойствами:

- Существенно большой период генератора (последовательность, выдаваемая ГПСЧ, является периодической).
- Последовательно выдаваемые элементы последовательности независимы друг от друга.
- Все элементы генерируемой последовательности являются одинаково «случайными» (т.е. можно говорить о равномерном распределении).
- Непредсказуемость. Зная алгоритм генератора и все предыдущие элементы последовательности (но не зная секретного ключа, инициализирующего генератор) противник не может вычислить следующий элемент (если не пройден период ГПСЧ).

Рассмотрим примеры ГПСЧ:

1. Линейный конгруэнтный генератор. Выбираются три константы $m > 0$ (модуль), a (множитель) и c (приращение), такие что $0 \le a < m$, $0 \le c < m$. Выбирается начальное значение x_0. Значения элементов последовательности вычисляются по формуле:

$$x_{n+1} = (ax_n + c) \bmod m$$

При этом число m должно быть очень большим, для a предпочтительный диапазон $0.01 \le a < 0.99m$, а c не должно иметь общего множителя с m. Генератор следует использовать для получения не более, чем m/1000 элементов последовательности, далее их случайность уменьшается.

2. Смешанный квадратичный генератор. Применяется для генерации битовой последовательности b_1, b_2, ... по следующим соотношениям:

$$x_{n+1} = x_n^2 \bmod m,\ b_n = x_n \cdot z \bmod 2,$$

где произведение $x \cdot z$ — скалярное произведение чисел x и z, представленных в двоичной форме, т.е. $x \cdot z = x_r x_{r-1} \dots x_0 \cdot z_r z_{r-1} \dots z_0 = x_r z_r \oplus x_{r-1} z_{r-1} \oplus x_0 z_0$. Кроме того m должно представлять собой произведение двух больших простых чисел вида $4k + 3$, а x_0 взаимно просто с m.

В мощных криптосистемах военного применения используются действительно случайные генераторы чисел, основанные на физических процессах. Они представляют собой платы, либо внешние устройства, подключаемые к ЭВМ через порт ввода-вывода. Два ос-

новных источника белого Гауссовского шума – высокоточное измерение тепловых флуктуаций и запись радиоэфира на частоте, свободной от радиовещания.

Тест для самоконтроля № 3

1. Чтобы подписать сообщение электронной цифровой подписью, используются:

а) открытый ключ отправителя;

б) открытый ключ получателя;

в) закрытый ключ отправителя;

г) закрытый ключ получателя.

2. Какие утверждения о протоколе строгой двусторонней аутентификации на основе случайных чисел справедливы?

а) в основе протокола лежит симметричный алгоритм шифрования;

б) на первом шаге проверяющий B отправляет проверяемому A случайное число;

в) на втором шаге проверяемый A отправляет проверяющему B зашифрованное сообщение, содержащее полученное на первом шаге случайное число, а также новое случайное число.

г) всего протокол требует отправки двух сообщений.

3. Какова последовательность подписания сообщений с помощью ЭЦП?

а) вычисляется хэш, затем хэш зашифровывается;

б) сообщение зашифровывается, после чего результат хэшируется;

в) при подписании сообщение зашифровывается, при проверке вычисляется хэш;

г) вычисляется хэш исходного сообщения, после чего оно зашифровывается.

4. Линейный конгруэнтный генератор имеет параметры: m = 10, c =7, a = 2, x0 = 5. Каким будет второй член последовательности, выданной с помощью этого генератора?

5. В чем заключается такое свойство функции хэширования H как стойкость к коллизиям первого рода?

а) Для любого хэша h должно быть практически невозможно вычислить или подобрать такое x, что H(x) = h.

б) Должно быть практически невозможно вычислить или подобрать любую пару различных сообщений x и y для которых H(x) = H(y);

в) Длина хэша должна быть фиксированной независимо от длины входного сообщения;

г) Для любого сообщения x должно быть практически невозможно вычислить или подобрать другое сообщение y, такое что H(x) = H(y).

6. Доказательство корректности алгоритма RSA основано на:

а) теореме Эйлера;

б) теореме о сумме эллиптических кривых;

в) китайской теореме об остатках;

г) расширенном алгоритме Евклида.

7. Какими свойствами должен обладать генератор псевдослучайных чисел?

а) недетерминированность;

б) непредсказуемость;

в) независимость очередного элемента от предыдущего;

г) равномерное распределение элементов последовательности;

д) неповторяемость элементов последовательности (в пределах периода).

8. Какие из перечисленных алгоритмов являются алгоритмами электронной цифровой подписи?

а) DES;

б) ГОСТ Р 34.10—2001;

в) ГОСТ Р 34.11—94;

г) RSA.

9. Открытым ключом RSA является пара (15, 2). Зашифруйте число 4.

10. Эллиптическая кривая имеет вид:

а) $y2 = x3 + ax + b \pmod p$;

б) $y3 = x2 + ax + b \pmod p$;

в) $y = x3 + ax2 + b \pmod p$;

г) $x3 = y2 + ax + b \pmod p$.

11. Чтобы расшифровать сообщение с помощью асимметричного алгоритма шифрования используются:

а) открытый ключ отправителя;

б) открытый ключ получателя;

в) закрытый ключ отправителя;

г) закрытый ключ получателя.

12. К какой разновидности протоколов относится протокол опознания пользователя на основе пароля?

а) протокол аутентификации;

б) протокол обмена ключами;

в) протокол одновременной подписи;

г) протокол групповой подписи;

д) протокол голосования.

Глава 7. Парольная защита

7.1. Роль парольной защиты в обеспечении безопасности АИС

Криптографические методы, в частности, шифрование, хорошо обеспечивают защиту информации (конфиденциальности, целостности, аутентичности и т.д.) от внешнего нарушителя. Такой нарушитель, возможно, может перехватывать сообщения, передающиеся по каналу связи а, в некоторых случаях, модифицировать их и даже вставлять в сеанс связи собственные сообщения (зачастую стараясь выдать их за сообщения другого источника). Однако информация в канале связи предварительно подвергается криптографическим преобразованиям и передается в соответствии с криптографическими протоколами, специально разработанными для того, чтобы помешать нарушителю реализовать угрозы безопасности. Для того, чтобы нарушить безопасность информации, циркулирующей в системе, ему необходимо найти уязвимость в системе защиты, либо в использованных в ней криптографических алгоритмах. Аналогичные трудности встают перед нарушителем, получившим доступ к защищенной АИС в качестве пользователя, не обладающего привилегиями, необходимыми для доступа к интересующим его данным.

Однако ситуация меняется, если нарушитель получает доступ в систему от имени пользователя, уполномоченного выполнять операции с интересующими его данными (например, копирование конфиденциальных файлов, уничтожение критически важных данных и т.д.). В этом случае вся криптографическая защита оказывается бесполезной. Таким образом — самое уязвимое место автоматизированной информационной системы — точки доступа к ней. Эти точки доступа защищаются протоколами аутентификации (проверки подлинности пользователя). А самая удобная для пользователя и наиболее используемая форма аутентификации — *парольная защита*.

Поэтому в большинстве случаев злоумышленника, который тем или иным образом может добраться до точки входа в систему (с рабочего места пользователя или удаленным способом), от его цели отделяет только пароль — вводимый с клавиатуры набор символов. Часто пароль выбирается неопытными пользователями таким образом, что его легко подобрать, в отличие от случайных 1024-битных криптографических ключей)[13]; часто не принимаются должные организационные меры по обеспечению безопасности пароля.

Существует ряд стандартных приемов, применяемых злоумышленниками с целью обойти парольную защиту. Для каждого из этих приемов выработан механизм противодействия. На основе этих механизмов можно сформулировать правила выбора безопасного пароля и работы с ним.

7.2. Способы атаки на пароль. Обеспечение безопасности пароля

Рассмотрим приемы обхода парольной защиты и методы противодействия им.

1. Полный перебор (метод грубой силы, bruteforce).

Самая простая (с технической точки зрения) атака на пароль — перебор всех комбинаций допустимых символов (начиная от односимвольных паролей). Современные вычис-

[13] Между тем, ключи (в частности, закрытые ключи алгоритмов асимметричного шифрования) часто хранятся в файлах, доступ к которым ограничивается с помощью парольной защиты.

лительные мощности позволяют перебрать все пароли длиной до пяти-шести символов за несколько секунд.

Некоторые системы не позволяют реализовать атаки, основанные на переборе, поскольку реагируют на несколько попыток неправильно набранного пароля подряд. Например, ОС Windows после трех неудачных попыток входа в систему делает минутную паузу (что делает полный перебор практически нереализуемым), а сим-карты сотовых телефонов и кредитные карточки банкоматов полностью блокируются.

Однако существует множество систем, позволяющих бесконечный перебор. Например, к защищенному паролем файлу (архив rar или zip, документ Microsoft Office и т.д.) можно пробовать разные пароли бесконечно. Существует множество программ, которые позволяют автоматизировать эту процедуру: Advanced RAR Password Recovery, Advanced PDF Password Recovery, Advanced Office XP Password Recovery. Кроме того, многие программы хранят хэш пароля в доступном файле. Например, таким образом клиент для работы с электронной почтой (работающий на общедоступном компьютере) может хранить пароли пользователей. Существуют способы похитить файл, содержащий хэши паролей доступа к операционной системе. После этого можно заниматься подбором паролей уже в обход системы, с помощью специальных программ.

Важной характеристикой пароля, затрудняющей (и даже делающей невозможным) полный перебор, является его длина. *Современный пароль должен иметь длину не менее 12 символов.*

Два лишних символа в пароле (при условии, что в нем могут встречаться все символы, которые можно набрать с клавиатуры, т.е. порядка 200) увеличивают время перебора в 40000 раз, а четыре символа — уже в 1.600.000.000 раз. Для того, чтобы перебрать все возможные пароли длиной 15 символов, потребуется время большее, чем возраст Вселенной. Однако не стоит забывать, что вычислительные мощности компьютеров постоянно растут (еще несколько лет назад безопасным считался пароль длиной 8 символов).

2. Перебор в ограниченном диапазоне.

Известно, что многие пользователи, составляя пароль, используют символы, находящиеся в определенном диапазоне. Например, пароль, состоящий только из русских букв или только из латинских букв или только из цифр. Такой пароль значительно легче запомнить, однако задача противника, осуществляющего перебор, неимоверно упрощается.

Пусть n = 70 — количество символов, из которых можно составить пароль, причем 10 из них — цифры, 30 — буквы одного языка и 30 — буквы другого языка. Пусть мы составляем пароль длиной m = 4 символа.

Если пароль составляется абсолютно случайно, то количество возможных комбинаций (которые необходимо перебрать) составляет $70^4 = 24010000$. Однако противник может сделать предположение, что пароль состоит из символов одного диапазона (пусть даже, неизвестно, какого). Всего таких паролей $10^4 + 30^4 + 30^4 = 10000 + 810000 + 810000 = 163000$. Если он оказался прав, то количество комбинаций (а следовательно, время, которое необходимо затратить на перебор) уменьшилось в 147 раз. Это число резко возрастает, когда увеличивается длина пароля и число диапазонов символов, из которых он может быть составлен.

Программы автоматического перебора пароля (такие как Advanced Office XP Password Recovery) включают опцию, позволяющую перечислить символы, которые следует пробовать при подборе пароля.

Как следствие, *надежный пароль должен содержать в себе символы из различных диапазонов*. Рекомендуется использовать русские и английские, прописные и строчные буквы, цифры, а также прочие символы (знаки препинания, подчеркивание и т.д.).

3. Атака по словарю

Бессмысленный, абсолютно случайный пароль труден для запоминания. Между тем угроза забыть пароль и потерять важную информацию для многих пользователей выглядит гораздо реальнее и страшнее, чем взлом их системы неизвестным злоумышленником. Поэтому в качестве пароля очень часто выбирается какое-то слово.

В этом случае задача подбора пароля превращается для злоумышленника почти в тривиальную Программа автоматического перебора паролей проверяет слова, содержащиеся в заданном файле со словарем (существует огромное количество доступных словарей такого рода для разных языков). Словарь из двухсот тысяч слов проверяется такой программой за несколько секунд.

Многие пользователи считают, что если применить к задуманному слову некоторое простое преобразование, например, написать его задом наперед или русскими буквами в английской раскладке или намеренно сделать ошибку, то это обеспечит безопасность. На самом деле, по сравнению с подбором случайного пароля подбор пароля по словарю с применением различных преобразований (сделать первую букву заглавной, сделать все буквы заглавными, объединить два слова и т.д.) делает невыполнимую задачу вполне возможной.

Надежный пароль не должен строиться на основе слов естестенного языка.

4. Атака по персональному словарю

Если атака по словарю и перебор паролей небольшой длины либо составленных из символов одной группы не помогает, злоумышленник может воспользоваться тем фактом, что для облегчения запоминания, многие пользователи выбирают в качестве пароля личные данные (номер сотового телефона, дату рождения, записанную наоборот, кличку собаки и т.д.).

В том случае, если цель злоумышленника — обойти парольную защиту именно этого пользователя, он может составить для него персональный словарь личных данных, после чего использовать программу автоматического перебора паролей, которая будет генерировать пароли на основе этого словаря.

Таким образом, *надежный пароль должен быть полностью бессмысленным*.

5. Сбор паролей, хранящихся в общедоступных местах

Во многих организациях пароли создает и распределяет системный администратор, который использует приведенные выше правила. Пользователи обязаны пользоваться выданным им паролем. Однако, поскольку этот пароль сложно запомнить, он часто хранится под рукой в записанном виде. Нередки случаи, когда пароль записывается на стикер и

приклеивается к монитору, либо содержатся в записной книжке, которая часто лежит на столе раскрытой.

Проблема в том, что, как показывают исследования, пользователи зачастую несерьезно относятся к вопросам обеспечения безопасности своего служебного пароля. Обычно это происходит из за непонимания политики безопасности организации и недооценки важности тех данных или сервисов, которые защищены паролем. Кроме того, пользователи считают, что, поскольку в организации «все свои», небрежное хранения пароля вреда не наносит. Между тем, проникнуть в помещение организации под благовидным предлогом и провести визуальный осмотр — достаточно простая задача для злоумышленника.

Более того, часто получив пароль от администратора на бумажке и переписав его в записную книжку, пользователи теряют или просто выбрасывают эту бумажку. В поисках пароля злоумышленики иногда не брезгуют копаться и в мусоре.

Пароль не должен храниться в общедоступном месте. Идеальный вариант — запомнить его и не хранить нигде. Если пароль содержится в записной книжке, она не должна оставляться без присмотра, а при вводе пароля не должно присутствовать посторонних, которые могут заглянуть в книжку через плечо.

6. Социальный инжиниринг

Социальный инжиниринг — манипулирование людьми (а не машинами) с целью проникновения в защищенные системы пользователя или организации. Если подобрать или украсть пароль не удается, можно попытаться обманом заставить пользователя отдать пароль самому. Классическая тактика социального инжиниринга — телефонный звонок жертве от имени того, кто имеет право знать запрашиваемую информацию. Например, злоумышленник может представиться системным администратором и попросить сообщить пароль (или другие сведения) под убедительным предлогом. Склонение пользователя к открытию ссылки или вложения, которые открывать не следует (см. главу 4) или заманивание его на подставной сайт (см. следующий пункт) также относят к методам социального инжиниринга.

Приемы, используемые злоумышленником, могут быть самыми разными. Начиная от звонка среди ночи с абсолютно неправдоподобной историей типа «в нашу банковскую сеть попал вирус и он уничтожает все данные о счетах клиентов, а мы не можем их спасти, потому что вирус уничтожил файл с паролями — срочно скажите ваш и мы спасем ваши деньги».

В любом случае, необходимо помнить правило: сообщать пароль посторонним лицам ни в коем случае нельзя. Даже если эти лица имеют право его знать[14]. Единственным исключением может являться требование суда или правоохранительных органов выдать пароль под угрозой ответственности за отказ от дачи показаний. Но и в этом случае необходимо убедиться, что сотрудники правоохранительных органов — именно те, за кого они себя выдают.

[14] Лица, имеющие право знать ваш пароль, его уже знают. И несут ответственность за его сохранность.

7. Фишинг

Фишинг — это процедура «выуживания» паролей случайных пользователей Интернета. Обычно заключается в создании «подставных» сайтов, которые обманом вынуждают пользователя ввести свой пароль.

Например, чтобы получить пароль к банковскому счету, может быть создан сайт с дизайном, идентичным сайту некоторого банка. Адрес этого сайта, естественно, будет другим, но чаще всего злоумышленник регистрирует доменное имя, отличающееся от банковского на один символ. В результате пользователь, сделав опечатку, попадет на подставной сайт и не заметит своей ошибки. Для заманивания пользователей клиентам банка могут также рассылаться электронные письма с содержанием типа «проверьте свой счет» или «ознакомьтесь с новыми акциями», причем в письме содержится ссылка, ведущая на подставной сайт.

Когда клиенты банка попадают на сайт злоумышленника, им (как и на настоящем сайте) предлагается ввести логин и пароль для доступа к счету. Эта информация сохраняется в базе данных злоумышленника, после чего клиент перенаправляется на главную страницу настоящего сайта. Пользователь видит, что ввод пароля «не сработал» и думает, что совершил ошибку или сайт просто «глючит». Он пробует ввести пароль заново и на этот раз успешно входит в систему. Это рассеивает его подозрения. Между тем, утечка пароля уже произошла...

Другая разновидность фишинга основана на том факте, что многие пользователи используют один и тот же пароль для разных ресурсов. В результате, произведя успешную атаку на менее защищенный ресурс, можно получить доступ к более защищенному.

Например, создается сайт, потенциально интересный некоторому кругу пользователей. Если цель атаки — конкретный человек, то предварительно изучаются его интересы и увлечения. Информация об этом сайте доносится до потенциальных жертв (персонально или за счет широкой рекламы). Пользователю, зашедшему на сайт, предлагается зарегистрироваться, в частности, придумать себе пароль. Теперь остается только посмотреть, не подходит ли введенный пароль к другим ресурсам этого пользователя (например, к электронной почте, адрес которой был указан при регистрации).

Чтобы противостоять угрозе фишинга необходимо внимательно проверять адрес сайта, прежде чем вводить важный пароль. Лучше всего поместить этот адрес в закладки браузера и пользоваться исключительно этими закладками, ни в коем случае не переходя по ссылкам из электронных писем. *Наконец, следует пользоваться разными паролями для доступа к разным сервисам*.

Соблюдение всех семи перечисленных выше рекомендаций достаточно сложно. Трудно запомнить несколько надежных (длинных и бессмысленных) паролей, а вероятность забыть пароль выше вероятности подвергнуться взлому. Однако существует ряд средств, облегчающих эту задачу, в частности, программы для хранения паролей.

Рассмотрим, например, программу *KeePass Portable*. В этой программе все пароли хранятся в зашифрованном файле, для доступа к которому необходимо ввести пароль (единственный, который придется по-настоящему запомнить). При этом программа не отображает эти пароли на экране в явном виде. Чтобы ввести пароль для доступа к ресурсу (например, определенному сайту или электронной почте), необходимо выбрать ресурс из списка

и выбрать в контекстном меню команду *Copy Password To Clipboard* (см. рис. 4.1). Пароль будет помещен в буфер обмена. То есть, даже внимательно отслеживая действия пользователя, противник не увидит пароля, который не набирается на клавиатуре и не появляется в явном виде на экране. Далее необходимо просто перейти в окно программы, требующей пароль, и поместить его из буфера обмена в поле для ввода (нажатием Ctrl + V или командой *Вставить* контекстного меню). Пароль сразу будет отображаться в виде звездочек. Кроме того, спустя несколько секунд он будет автоматически удален из буфера. Программа позволяет также генерировать случайные пароли заданной длины, причем пользователь может даже не знать, какой пароль создала ему программа — важно, чтобы она предоставляла этот пароль каждый раз, когда необходимо авторизоваться. Наконец, KeePass Portable не требует установки в системе: программа может переноситься на флешке и запускаться непосредственно с нее.

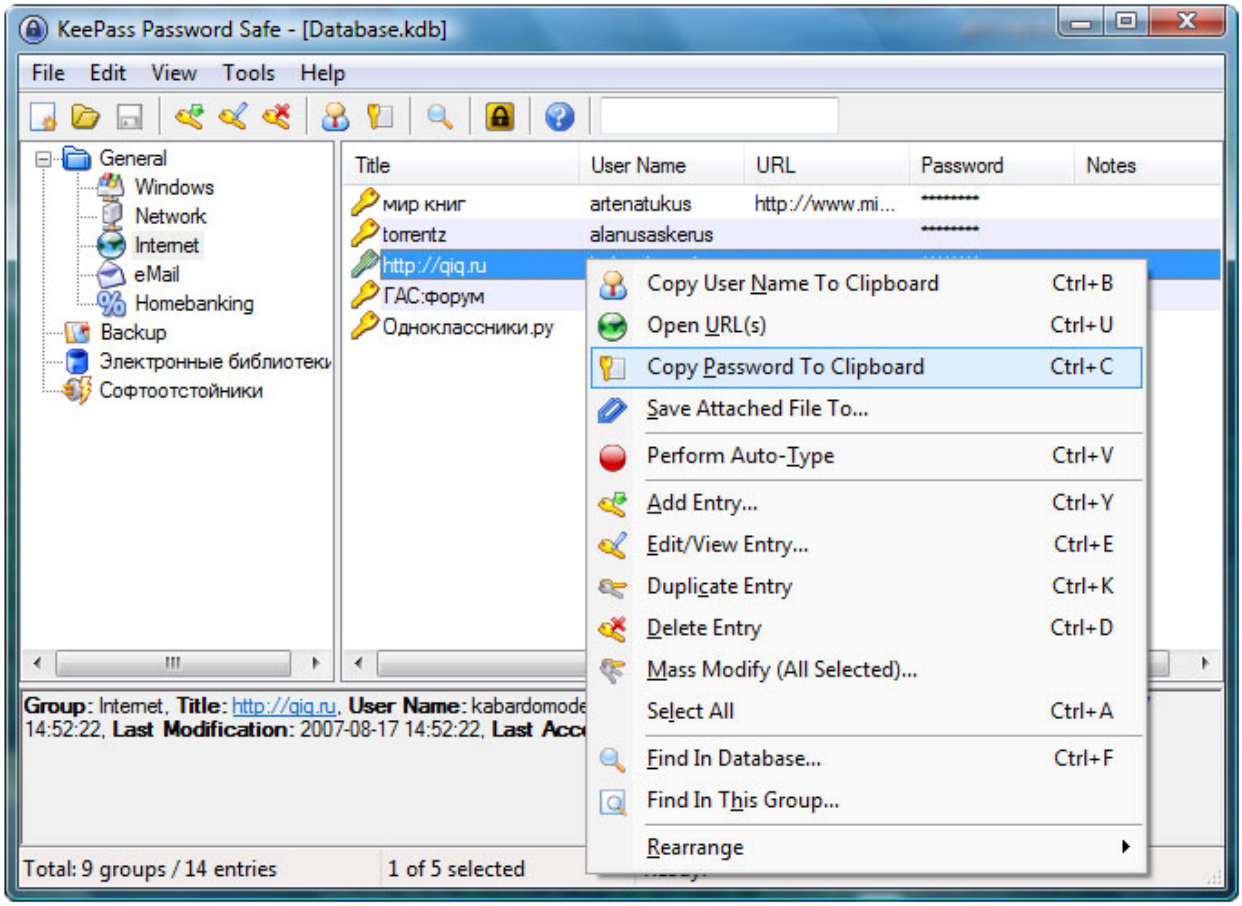

Рис. 4.1. Окно программы KeePass Portable

Глава 8. Компьютерные вирусы и борьба с ними

8.1. Общие сведения о компьютерных вирусах

Компьютерным вирусом называется программа, способная к *саморазмножению*. Это означает, что программа, будучи запущенной, способна создавать свои копии (возможно, модифицированные) и распространять их некоторым образом с компьютера на компьютер. При этом, как правило, внедрение вируса на компьютер и его запуск происходит без ведома (и вопреки желанию) владельца компьютера.

Вирус, как программа, состоит из двух частей: *механизм размножения* и *начинка*. Механизм размножения определяет способ, которым копии вируса создаются, распространяются и запускаются. Начинка представляет собой дополнительное поведение вируса (помимо размножения) на зараженном компьютере.

Начинка некоторых вирусов является вполне безобидной (например, вывод собщения на экране), а некоторых — весьма опасной: уничтожение данных, похищение информации или использование компьютера в качестве плацдарма для DOS-атаки. В любом случае вирус оказывает негативное воздействие, расходуя ресурсы процессора, оперативную память и дисковое пространство. Кроме того, масштабная эпидемия вируса, размножающегося по сети, когда оказываются зараженными тысячи компьютеров, может привести к тому, что сеть выйдет из строя из-за перегрузки. По этой причине вирусы называют вредоносными программами.

Вообще под *вредоносной программой* (malware) эксперты понимают любую программу, которая устанавливает себя на компьютер без ведома его владельца и осуществляет нежелательные для него функции[15].

Другое определение вредоносного программного обеспечения (которое, в частности, взято на вооружение российскими правоохранительными органами) — это любое ПО, написанное с целью нанесения ущерба или использования ресурсов атакуемого компьютера.

8.2. Классификация вирусов

По начинке вирусы делятся на деструктивные и недеструктивные. Деструктивные вирусы классифицируют по выполняемым ими функциям:

1. Вирусы, уничтожающие данные. Наиболее характерный пример — вирус «Чернобыль» (Win95.CIH), массовое распространение которого случилось в 1999 году. При запуске проверял системную дату компьютера и 26 апреля активировал механизм уничтожения данных на жестком диске[16]. Другой вирус, Klez.E, произвел эпидемию в 2002 году. Он срабатывал на шестой день каждого нечетного месяца и заполнял файлы определенных форматов (.doc, .txt и др.) случайным содержимым, после чего их восстановление становилось неозможным.

---

[15] По этой причине вредоносной программой был признан руткит фирмы Sony: эта программа автоматически устанавливалась при проигрывании DVD-диска с фильмом, а затем без предупреждения запускалась и собирала информацию о лицензионности других DVD с фильмами.

[16] При этом производится попытка записать «мусор» во FLASH BIOS компьютера. Некоторые старые модели это позволяли, после чего восстановить материнскую плату можно было только заменой микросхемы.

2. Вирусы-шпионы. Начинка заключается в похищении информации, например, отслеживании всех нажатий пользователя на клавиатуру, записи этих данных в специальный файл и регулярной отправки создателю вируса. Другой вариант — пересылка файлов с паролями и учетных данных платежных систем.
3. Использование зараженных компьютеров в качестве плацдарма для рассылки спама или распределенной DoS-атаки (группа зараженных таким вирусом компьютеров называется «зомби-сетью»). Пример такого вируса — MsBlast — был предназначен для атаки на сайт windowsupdate.com: 16 августа 2003 года со всех зараженных компьютеров осуществлялись запросы к этому сайту, в результате чего сервер должен был подвергнуться критической перегрузке и выйти из строя.
4. Крипто-вирусы. Шифруют информацию на жестком диске алгоритмом с открытым ключом и предлагают пользователю (например, оставив текстовый файл с сообщением) купить закрытый ключ, переведя деньги на определенный счет.

Общепринятая классификация вирусов — по механизму их размножения. Выделяются файловые вирусы, макровирусы, загрузочные вирусы и сетевые черви. Рассмотрим все эти разновидности более подробно.

8.3. Файловые вирусы

Файловые вирусы внедряются в исполняемые файлы на компьютере (заражают их), дописывая самих себя в начало, в середину или в конец файла. Таким образом, при запуске пользователем зараженного файла автоматически будут выполнены и команды вируса (поиск незараженных файлов, их заражение, а также начинка).

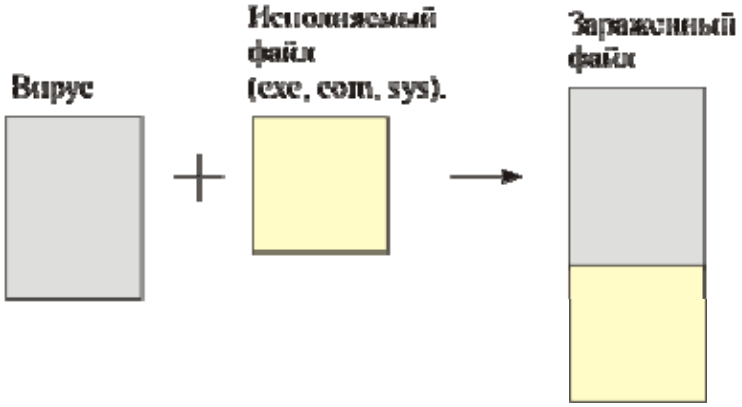

Рис. 1. Механизм работы файлового вируса

Распространение таких вирусов происходит через зараженные файлы. Достаточно принести один такой файл на незараженный компьютер и запустить его, чтобы вирус начал действовать. Спустя короткое время все исполняемые файлы на компьютере оказываются зараженными и при запуске любой программы вместе с ней срабатывает и вирус.

Файловые вирусы были весьма распространены в 90-х годах, когда программы были небольшими и распространялись «из рук в руки» на дискетах. В настоящее время эти вирусы непопулярны, не в последнюю очередь потому, что их достаточно легко обнаружить: во-первых, увеличивается размер всех исполняемых файлов, а во-вторых, многие программы при запуске проверяют свою целостность (например, по размеру или контрольной

сумме) и сигнализируют о ее нарушении. Тем не менее, опасность скачать из Интернета или по пиринговой сети зараженный файл по-прежнему остается.

8.4. Макровирусы

Макровирусы не отличаются по механизму размножения от файловых вирусов; их особенность в том, что заражают они не исполняемые файлы, а файлы некоторых популярных форматов документов (в частности, .doc и .xls). Макровирусы оказались опасны тем, что пользователи привыкли к мысли о том, что зараженной может быть только программа и не опасались получить вирус вместе с документом.

Макровирусы используют возможности некоторых программ (текстовых, графических, табличных редакторов, СУБД и пр.) внедрять в документы, создаваемые этими программами, так называемые *макросы* — процедуры, написанные на встроенном в них языке программирования и выполняемые в ответ на определенные события (нажатие пользователем кнопки или открытие документа). Например, Microsoft Office поддерживает встроенный язык программирования Visual Basic for Applications (VBA).

Макровирус представляет собой программу на макроязыке, внедренную в документ соответствующего формата и запускающуюся автоматически обычно при открытии документа. После запуска вирус ищет другие доступные документы этого формата и внедряется в них, а также исполняет свою начинку (возможностей современных макроязыков вполне хватает, чтобы эта начинка могла содержать серьезные деструктивные функции).

В настоящее время макровирусы также непопулярны, поскольку современные версии программ, поддерживающих макроязыки, предупреждают пользователя о наличии макросов в документе. Более того, чтобы позволить макросу запуститься, от пользователя нередко требуется изменить настройки программы.

8.5. Сетевые черви

Современные вирусы не заинтересованы в том, чтобы заразить как можно больше файлов на компьютере (и тем самым повысить вероятность своего запуска и размножения). С повсеместным проникновением Интернета наиболее привлекательная цель для вирусов — проникнуть на как можно большее число компьютеров в сети. При этом достаточно, чтобы на каждом компьютере содержался лишь один экземпляр вируса, но при этом соблюдалось два условия:

1. Вирус должен автоматически запускаться (желательно одновременно с запуском операционной системы).
2. Содержащий вирус файл долден быть надежно скрыт от пользователя.

Вирусы, которые автоматически запускаются в момент старта операционной системы и, таким образом, постоянно функционируют в оперативной памяти, называются *резидентными*. Вирусы, распространяющие свои копии по локальной сети или через Интернет называются *сетевыми червями*. Большинство сетевых червей являются резидентными.

Вирусы, распространяющиеся через Интернет, являются наиболее популярными и представляют наибольшую угрозу. Они имеют два основных механизма проникновения на компьютер жертвы:

1. Через стандартные коммуникационные сервисы.

2. Через «дыры» в популярных сетевых приложениях, в том числе самой ОС.

В роли стандартного коммуникационного сервиса чаще всего выступает обыкновенная электронная почта. Вирус распространяется в виде прикрепленного к электронному письму файлового вложения, которое доверчивые и халатные пользователи, имеющие низкую культуру в области информационной безопасности, из любопытства запускают, отдавая тем самым свой компьютер под контроль вируса.

Этому способствует тот факт, что письмо с вирусным вложением может прийти со знакомого почтового адреса. Действительно, заразив компьютер, почтовый вирус, как правило, обрабатывает файл, в котором содержится адресная книга почтовой программы, и извлекает из нее адреса постоянных корреспондентов пользователя, после чего им направляются автоматически сгенерированные письма с копией вируса.

Один из самых нашумевших сетевый червей — вирус «I love you», эпидемия которого началась 4 мая 2000 года. После открытия файла, приложенного к электронному письму, вирус уничтожал или изменял некоторые файлы на зараженной машине, а кроме того сразу же, в момент запуска, рассылал себя по всем адресам адресной книги пользователя. По оценкам различных компаний, поражению подверглось огромное количество компьютерных сетей (в отдельных странах — от 30 до 80 процентов). Количество получателей «любовных писем» оценивается в 45 миллионов человек, общие убытки — до 10 миллиардов долларов США[17]. Адресат получал письмо следующего содержания:

Subject «ILOVEYOU»

Сообщение: «kindly check the attached LOVELETTER coming from me.»

Присоединенный файл: «LOVE-LETTER-FOR-YOU.TXT.vbs»

Несмотря на то, что механизм проникновения вирусов через почтовые вложения имеет достаточно почтенный возраст и широко известен, пользователи по-прежнему заражаются почтовыми вирусами, неосторожно запуская вложения.

Второй механизм заражения — ошибки в сетевых программах, позволяющие вредоносной программе проникать на компьютер пользователя и получать на нем управление без каких-либо действий со стороны самого пользователя. Такие вирусы появляются значительно реже (поскольку обнаружение подобной ошибки и написание программы, которая ей пользуется, непросто). Однако, появившись, они вызывают серьезную вирусную эпидемию (как вирус MsBlast в 2003 году), которая прекращается только тогда, когда выпускается патч (программа, исправляющая уязвимость) и его устанавливают большинство пользователей.

Единственный способ хоть как-то противостоять подобным вирусам — своевременная установка обновлений.

Рассмотрим теперь резидентные вирусы. Их характерной особенностью является автоматический запуск после загрузки операционной системы. Большинство резидентных вирусов под Windows обеспечивает выполнение этого условия, прописывая себя в разделы автозагрузки в реестре:

HKEY_LOCAL_MACINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\

[17] http://www.securitylab.ru/informer/240711.php

При этом многие вирусы, резидентно находясь в памяти, следят за реестром и если пользователь удаляет соответствующую запись (ключ), восстанавливают ее. Поэтому чтобы удалить вирус вручную, необходимо загрузиться в безопасном режиме.

Маскируются сетевые черви в большинстве своем в системных папках Windows (например, System32) среди сотен файлов, назначение которых пользователю неизвестно.

8.6. Загрузочные вирусы

Загрузочные вирусы заражают носители данных. Изначально заражению подвергались дискеты и жесткие диски. Загрузочный вирус прописывает себя в первый (нулевой) сектор раздела, где обычно находится программа-загрузчик. Сама эта программа перемещается в другое место, а при загрузке с зараженного носителя сначала запускается вирус. Вирус предпринимает меры к тому, чтобы закрепиться в оперативной памяти и получить контроль над системой, после чего позволяет загружаться стандартному загрузчику.

Классические загрузочные вирусы в настоящее время устарели, поскольку загрузка с дискеты (а именно на дискетах такие вирусы и распространялися) уже практически не используется. Однако в последние годы появилась вариация вирусов (которые также можно назвать загрузочными), распространяющиеся через флэш-накопители.

Такой вирус представляет собой обычный исполняемый файл с атрибутом «скрытый», который записывается в корневой каталог флешки либо в скрытую папку, эмулирующую корзину Windows либо другую системную папку. Кроме этого в корневом раталоге размещается файл autorun.inf со ссылкой на вирус. Вирус активируется, если у флешки срабытывает автозапуск, а это обычно происходит автоматически, если открывать флешку двойным щелчком по ее ярлыку при условии, что настройки Windows установлены по умолчанию. Вирус оставляет свои копии (вместе с autorun.inf) на всех разделах жесткого диска и, таким образом, получает управление во время каждого сеанса работы пользователя, когда тот случайно активирует автозапуск на одном из этих разделов. Далее вирус постоянно находится в оперативной памяти, исполняет свою начинку, а также отслеживает подключение к компьютеру новых переносных носителей и заражает их.

Для профилактики таких вирусов (помимо антивирусной защиты) необходимо открывать переносные устройства таким образом, чтобы не позволить сработать автозапуску. Например, открывать их через оболочку типа Total Commander, либо через адресную строку проводника Windows (но не двойным щелчком по ярлыку).

8.7. Троянские кони

Троянским конем (разг.: троян, троянец) называется вредоносная программа, которая не имеет (в отличие от вирусов) способности к саморазмножению, а вместо этого маскируется под программу, выполняющую полезные функции. Таким образом, распространение троянских коней часто происходит посредством самих пользователей, которые скачивают их из Интернета или друг у друга, не догадываясь о последствиях.

Особая опасность в том, что пользователи принимают их за легальные программы. Поэтому запуская троянского коня пользователь может вручную (в ответ на предупреждение операционной системы или файервола) дать ей все необходимые права, открыть доступ в Интернет и к системным ресурсам.

Одна из распространенных начинок троянских коней — *бэкдор* (backdoor) — программа, позволяющая злоумышленнику получать удаленный доступ к системе (а в некоторых случаях полностью ее контролировать).

8.8. Технологии маскировки вирусов

Помимо начинки и механизма размножения интерес представляют приемы, с помощью которых вирусы скрывают свое присутствие в системе, с тем, чтобы продержаться в ней как можно дольше.

Стелс-вирус — вирус, полностью или частично скрывающий свое присутствие путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т.д.) Например, файловый вирус может перехватывать функции чтения/записи в файл, чтения каталога и т. д., чтобы скрыть увеличение размера зараженных программ; перехватывает функции чтения/записи файла в память, чтобы скрыть факт изменения файла.

Полиморфные вирусы — вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совладать ни в одном бите. Это затрудняет анализ и обнаружение его антивирусом. Для модификации кода используется шифрование. Т.е. вирус содержит шифратор, причем при размножении каждая копия вируса шифруется новым случаным ключом, а расшифровывает вирус сам себя уже во время выполнения. Естественно, дешифратор при этом не зашифровывается, но полиморфные вирусы обычно содержат код генерации дешифратора, чтобы, выполняя одни и те же функции, эта часть в каждой копии вируса имела различный вид.

Рис 2. Структура полиморфного вируса.

8.9. Тенденции современных компьютерных вирусов

Рассмотрим характерные черты, которые за последние годы наиболее четко проявились в современных вирусах:

- наибольшее распространение получили сетевые черви;
- вирусы активно используют уязвимости в различных операционных системах и программном обеспечении;
- для быстрого распространения вирусов используются спам-технологии;
- один вирус сочетает в себе мноество технологий: полиморфных, стелс, бэкдор;
- вместо пересылки своего тела по электронной почте часто отправляется ссылка на вебсайт или на зараженный ранее компьютер;
- увеличивается число вирусов для новых платформ: КПК, сотовых телефонов, смартфонов и коммуникаторов, при этом активно используются беспроводные среды передачи данных (Bluetooth, Wi-Fi).

8.10. Борьба с вирусами

Для борьбы с вирусами используется специальное программное обеспечение — *антивирусы*. По выполняемым ими функциям выделяют следующие виды антивирусов:

- *Программы-детекторы* осуществляют поиск характерного для вируса кода (сигнатуры) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение.
- Программы-доктора или *фаги* также осуществляют поиск зараженных файлов и «лечат» их, т.е. возвращают в исходное состояние. Среди фагов выделяют *полифаги*, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.
- *Ревизоры* запоминают исходное состояние объектов незараженной системы и периодически сравнивают текущее состояние с исходным.
- Программы-*фильтры* — резидентные (то есть постоянно работающие) программы, предназначенные для обнаружения при работе компьютера подозрительных действий, характерных для вирусов.
- *Вакцины* — резидентные программы, предотвращающие заражение файлов.

Современные антивирусы представляют собой многофункциональные программные комплексы, которые способны обнаруживать, лечить (удалять) вирусы, а также препятствовать их проникновению на компьютер.

Современные антивирусы могут работать в двух режимах. В режиме *монитора* антивирус постоянно работает, отслеживая все обращения системы к файлам, вклиниваясь в этот процесс и проверяя эти файлы на предмет заражения. Таким образом, при первой попытке вируса активироваться антивирус блокирует эту попытку и выдает предупреждение. При использовании режима монитора работа компьютера замедляется (так как часть вычислительных ресурсов тратится на работу антивируса, а любое ображение к файлам и некоторым другим объектам сопровождается процедурой сканирования). Кроме того, если на компьютере присутствуют зараженные файлы, которые не проявляют активности и обращения к ним не происходит, они останутся незамеченными.

В режиме *сканера* антивирус проверяет все файлы в заданной области (определенный каталог, раздел жесткого диска или все устройства хранения информации) и удаляет/лечит зараженные (либо просто оповещает о них — в зависимости от настроек сканера). Проверка всех данных на компьютере может занять значительное время (несколько часов). Кроме того, вирус может попасть в систему сразу после сканирования.

Для надежной защиты рекомендуется применение обоих режимов: постоянная работа антивируса в режиме монитора и регулярная (раз в неделю) проверка всех данных с помощью сканера (обычно сканирование запускается на ночь).

Рассмотрим методы обнаружения антивирусом своих жертв.

Обнаружение, основанное на сигнатурах — метод работы антивирусов и систем обнаружения вторжений, при котором антивирус, просматривая файл (или передаваемый по сети пакет), обращается к словарю, в котором содержатся сигнатуры известных атак или вирусов. Под *сигнатурой* понимается фрагмент кода, однозначно идентифицирующий вирус. Например, вирус Email-Worm.Win32.Happy содержит строку «Happy New Year 1999 !!», которая с низкой вероятностью может встретиться в другой программе.

Основной принцип, по которому выделяются сигнатуры — *она должна содержать только уникальные строки из этого файла, настолько характерные, чтобы гарантировать минимальную возможность ложного срабатывания*. Разработка сигнатур осуществляется вручную путем кропотливого исследования нескольких файлов, зараженных (или принадлежащих) одним вирусом. Автоматическая генерация сигнатур (особенно в условиях полиморфных вирусов) пока не дает удовлетворительных результатов.

Каждый современный антивирус имеет обширную (несколько сот тысяч) базу сигнатур, которая регулярно обновляется. Проблема обнаружения, основанного на сигнатурах заключается в том, что новый вирус (сигнатуры которого еще нет в базе) может беспрепятственно обойти антивирусную защиту. При этом создание сигнатуры и доставка ее пользователям занимает от 11 до 97 часов в зависимости от производителя, в то время как теоретически, вирус может захватить весь интернет меньше, чем за 30 секунд[18].

Метод обнаружения подозрительного поведения программы. Антивирус прослеживает поведение всех работающих программ и пытается выявить действия, характерные для вируса (например, запись данных в exe-файл). Однако этот метод часто вызывает ложные срабатывания (в результате пользователи перестают обращать внимание на предупреждения). Разновидность этого метода — *эмуляция программы*: перед запуском приложения антивирус пытается имитировать его поведение с целью отслеживая подозрительных действий. Данный метод наиболее требователен к ресурсам.

Метод «белого списка». Предотвращается выполнение всех компьютерных кодов кроме тех, которые были ранее обозначены системным администратором как безопасные.

Эвристическое сканирование — метод, основанный на сигнатурах и эвристике, призван улучшить способность сканеров применять сигнатуры и распознавать модифицированные версии вирусов в тех случаях, когда сигнатура совпадает с телом неизвестной программы не на 100 %, но в подозрительной программе налицо более общие признаки вируса. Данная технология, однако, применяется в современных программах очень осторожно, так как может повысить количество ложных срабатываний[19].

Наиболее известные современные антивирусы: антивирус Касперского, Doctor WEB, NOD32, Norton Antivirus, Panda Antivirus, Avast! Antivirus (последний является бесплатным для домашнего использования).

---

[18] http://www.icir.org/vern/papers/cdc-usenix-sec02\, http://ru.wikipedia.org

[19] http://ru.wikipedia.org/wiki/Эвристическое_сканирование

Глава 9. Средства защиты сети

Если локальная сеть организации или персональный компьютер пользователя имеют выход в сеть Интернет, количество угроз безопасности увеличивается в десятки раз по сравнению с изолированной сетью или компьютером. Сетевые вирусы, попытки проникновения в систему извне (используя подобранный или украденный пароль, уязвимости программного обеспечения и т.д.), перехват и подмена данных, передаваемых в сеть или получаемых из сети — вот перечень наиболее типичных угроз.

Существует ряд средств, методов и технологий защиты информации, учитывающих специфику сетевых атак. К ним, в частности, относятся межсетевые экраны (брандмауэры), виртуальные частные сети (VPN) и системы обнаружения вторжений.

9.1. Межсетевые экраны

Межсетевой экран (брандмауэр, файрвол) — комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Межсетевой экран, как правило, обладает несколькими интерфейсами, по одному на каждую из сетей, к которым он подключен. Набор правил политики определяет, каким образом трафик передается из одной сети в другую. Если в правиле отсутствует явное разрешение на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты.

Межсетевой экран может выступать в роли proxy-сервера. *Proxy-сервер* — это программа или узел сети, играющий роль посредника между внутренней сетью организации и внешней сетью (например, Интернет). В этом случае он может также скрывать внутренние адреса компьютеров организации. Эта функция называется *трансляцией сетевых адресов* (NAT — Network Address Translation). Когда какой-то узел внутренней сети хочет передавать информацию вовне, он отправляет ее proxy-серверу (одновременно являющемуся межсетевым экраном). Проверив передаваемые пакеты на соответствие политике фильтрации, межсетевой экран инициирует новое соединение, и передает пакеты уже от своего имени. В результате скрывается схема внутренней адресации сети и тем самым существенно затрудняется ее анализ злоумышленником (с целью обнаружения уязвимостей).

Существует ряд классификаций межсетевых экранов по различным критериям:

1. В зависимости от охвата контролируемых потоков данных.

— *Традиционный* межсетевой экран — программа, установленная на шлюзе (сервере передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями. Основная задача такого брандмауэра — предотвращение несанкционированного доступа во внутреннюю сеть организации.

— *Персональный* межсетевой экран — программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

2. В зависимости от уровня модели OSI, на котором происходит контроль доступа.

— *Работающие на сетевом уровне* — фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором;
— *Работающие на сеансовом уровне* — отслеживаются сеансы между приложениями и не пропускаются пакеты, нарушающие спецификации TCP/IP (такие пакеты часто используются в злонамеренных операциях: сканировании ресурсов, взломах через неправильные реализации TCP/IP, обрыв/замедление соединений и т.д.).
— *Работающие на уровне приложений* — фильтрация на основании анализа данных приложения, передаваемых внутри пакета; передача потенциально опасной и нежелательной информации блокируется на основании политик и настроек.

3. В зависимости от отслеживания активных соединений.

— *Stateless (простая фильтрация)* — не отслеживают текущие соединения (например, TCP), а фильтруют поток данных исключительно на основе статических правил;
— *Stateful (фильтрация с учётом контекста)* — отслеживают текущие соединения и пропускают только такие пакеты, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений.

Рассмотрим некоторые популярные брандмауэры, реализованные в виде прикладных программ.

1. Outpost Firewall Pro. Персональный брандмауэр, обладает следующими функциональными возможностями:

— предотвращение несанкционированного доступа к данным;
— сокрытие присутствия зщищаемой системы в сети (таким образом она делается «невидимой» для взломщиков);
— анализ входящих почтовых сообщений и блокировка потенциально опасных;
— мониторинг и анализ сетевой активности системы;
— блокировка доступа к «запрещенным» сайтам (для детей или сотрудников).

2. ZoneAlarm Pro. Мощный брандмауэр с гибко настраиваемыми функциональными возможностями, включающими:

— фильтр приложений, позволяющий устанавливать права для каждой программы, используемой в сети;
— поддержку цифровой подписи;
— подробный лог-файл событий и средства для его анализа, с последующей выдачей текстовых и графических отчетов;
— настраиваемый контроль cookies;
— механизм мгновенной автоматической или ручной блокировки доступа приложений к Интернет;
— автоматическую проверку вложений электронной почты.

9.2. Виртуальные частные сети (VPN)

Виртуальная частная сеть (VPN) — логическая сеть, создаваемая поверх другой сети, чаще всего Интернет. Все данные, передающиеся между узлами этой сети шифруются, поэтому, хотя физически данные передаются по публичным сетям с использованием не-

безопасных протоколов, по сути, VPN представляет собой закрытые от посторонних каналы обмена информацией.

Канал между двумя узлами, защищенный за счет шифрования проходящего по нему трафика, называется *туннелем*.

Выделяют два основных класса VPN:

1. Защищенные. Наиболее распространённый вариант. С его помощью на основе ненадёжной сети (как правило, Интернета) создается надежная и защищенная подсеть. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP (протокол тунеллирования от точки к точке).

2. Доверительные. Используются для создания виртуальной подсети в рамках другой, надежной и защищенной сети, т.е. задача обеспечения безопасности по сути не ставится. К доверительным VPN относятся протоколы MPLS и L2TP.

По архитектуре технического решения выделяют следующие классы VPN [5]:

1. Внутрикорпоративные. Предназначены для обеспечения защищенного взаимодействия между подразделениями внутри предприятия или между группой предприятий, объединенных корпоративными связями, включая выделенные линии.
2. VPN с удаленным доступом. Предназначены для обеспечения защищенного удаленного доступа мобильных или удаленных сотрудников компаний к корпоративным информационным ресурсам.
3. Межкорпоративные (extranet VPN). Обеспечивают прямой защищенный доступ из сети одной компании к сети другой компании (партнера, клиента и т.д.).

По способу технической реализации различают *VPN на основе маршрутизаторов* (задача шифрования трафика ложится на маршрутизаторы, через которые проходит вся исходящая из локальных сетей информация), *на основе межсетевых экранов*, *на основе программного обеспечения* и *на основе специализированных аппаратных средств*.

Рассмотрим набор протоколов *IPSec*, предназначенный для обеспечения защиты данных, передаваемых по протоколу IP. Он позволяет осуществлять подтверждение подлинности и шифрование IP-пакетов, а также включает протоколы для защищенного обмена ключами через Интернет.

Протоколы IPsec работают на сетевом уровне модели OSI. Они подразделяются на два класса: протоколы отвечающие за защиту потока передаваемых пакетов (ESP, AH) и протоколы обмена ключами (IKE). Протоколы защиты передаваемого потока могут работать в двух режимах — в транспортном режиме и в режиме туннелирования. В *транспортном режиме* шифруется (или подписывается) только информативная часть IP-пакета, а заголовок не затрагивается (поэтому процедура маршрутизации не изменяется). В *туннельном режиме* IP-пакет шифруется целиком. Для того, чтобы его можно было передать по сети, он помещается в другой IP-пакет. Именно этот режим используется для организации виртуальной частной сети.

Режим IPSec-тунеллирования работает следующим образом [6]:

1. Обычный IP-пакет посылается на отправляющее IPSec-устройство (межсетевой экран или маршрутизатор), где он должен быть зашифрован и направлен в конечную систему по локальной сети.

2. Отправляющее IPSec-устройство проводит аутентификацию принимающего устройства.

3. Два IPSec-устройства «договариваются» о шифре и алгоритме аутентификации, которыми будут пользоваться.

4. Отправляющее IPSec-устройство шифрует IP-пакет с информацией и помещает его в другой пакет с AH (аутентифицирующим заголовком).

5. Пакет пересылается по сети (по протоколам TCP/IP).

6. Принимающее IPSec-устройство читает IP-пакет, проверяет его подлинность и извлекает зашифрованное вложение для расшифровки.

7. Принимающее устройство отправляет исходный пакет в пункт его назначения.

9.3. Системы обнаружения вторжений (IDS)

Система обнаружения вторжений (Intrusion Detection System — IDS) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими (в основном через Интернет).

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которые могут нарушить безопасность системы или сети. К ним относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (вирусов, троянских коней).

Структурно СОВ состоит из следующих компонентов:

1. Сенсорная подсистема отслеживает события, которые могут затрагивать безопасность защищаемой системы.

2. Подсистема анализа выявляет среди этих событий те, которые представляют угрозу или нарушения безопасности (атаки, подозрительные действия). В *пассивных СОВ* при обнаружении такого события информация о нем помещается в хранилище, после чего сигнал опаности по определенному каналу направляется администратору системы. *Активные СОВ* (системы предотвращения вторжений) могут также предпринять ответные действия (например, прервать соединение или автоматически настроить межсетевой экран для блокирования трафика от злоумышленника).

3. Хранилище обеспечивает накопление и хранение данных сенсорной подсистемы и результатов их анализа;

4. Консоль управления используется для настройки СОВ, наблюдения за состоянием защищаемой системы, просмотра выявленных подсистемой анализа инцидентов.

Рассмотрим основные разновидности современных СОВ [8].

1. СОВ, защищающие сегмент сети. Развертываются на специализированном сервере, на котором не работают никакие другие приложения (поэтому он может быть особенно надежно защищен от нападения; кроме того, этот сервер может быть сделан «невидимым» для нападающего). Для защиты сети устанавливаются несколько таких серверов, которые анализируют сетевой трафик в различных сегментах сети. Таким образом, несколько удачно расположенных систем могут контролировать большую сеть.

К недостаткам таких систем относят проблемы распознавания нападений в момент высокой загрузки сети, и неспособность анализировать степень проникновения (система просто сообщает об инициированном нападении).

2. СОВ, защищающие отдельный сервер. Собирают и анализируют информацию о процессах, происходящих на конкретном сервере. Благодаря узкой направленности, могут проводить высоко детализированный анализ и точно определять, кто из пользователей выполняет злонамеренные действия. Некоторые СОВ этого класса могут управлять группой серверов, подготавливая централизованные обобщающие отчеты о возможных нападениях. В отличие от предыдущих систем могут работать даже в сети, использующей шифрование данных (когда информация находится в открытом виде на сервере до ее отправки потребителю). Однако систем этого класса не способны контролировать ситуацию во всей сети, так как видят только пакеты, получаемые «своим» сервером. Кроме того, снижается эффективность работы сервера вследствие использования его вычислительных ресурсов.

3. СОВ на основе защиты приложений. Контролируют события, проявляющиеся в пределах отдельного приложения. Знания о приложении, а также возможность анализировать его системный журнал и взаимодействовать с ним посредством API, позволяет таким системам контролировать деятельность пользователей (работающих с данным приложением) с очень высокой степенью детализации.

Аналогично антивирусным программам, системы обнаружения вторжений используют два основных подхода к методам обнаружения подозрительной активности. *Подход на основе сигнатуры* выявляет деятельность, которая соответствует предопределенному набору событий, уникально описывающему известное нападение. Эта методика чрезвычайно эффективна и является основным методом, используемым в коммерческих программах. Однако, такая СОВ не может бороться с новыми видами нападений, а также с видоизмененными вариантами традиционных нападений, сигнатура которых незначительно отличается от имеющейся в базе. *СОВ на основе аномалий* обнаруживают нападения, идентифицируя необычное поведение на сервере или в сети. Они способны обнаруживать нападения, заранее не запрограмированные в них, но производят большое количество ложных срабатываний.

Тест для самоконтроля № 4

1. Каким образом проникают в систему макровирусы?

а) по электронной почте;

б) любым способом вместе с зараженными ими файлами;

в) злоумышленник должен вручную внести вирус в систему;

г) через Интернет, используя ошибки в сетевых программах;

д) через съемные носители данных при срабатывании автозагрузки с них.

2. Какому требованию должен удовлетворять пароль для противодействия атаке по персональному словарю?

а) при придумывании пароля не должны использоваться личные данные;

б) длина пароля должна составлять 12 и более символов;

в) пароль нельзя открывать никому;

г) разные сервисы должны защищаться разными паролями;

д) пароль должен включать символы разных алфавитов и регистров, цифры, знаки препинания и т.д.

3. Какие недостатки имеют системы обнаружения вторжений, работающие на основе обнаружения аномалий?

а) высокий процент ложных срабатываний;

б) не способны контролировать ситуацию во всей сети;

в) неспособны анализировать степень проникновения;

г) работа затруднена при высокой загрузке сети;

д) снижается эффективность работы сервера, на котором они установлены.

4. ... — канал между двумя узлами, защищенный за счет шифрования проходящего по нему трафика.

5. Как называются вирусы, которые автоматически запускаются в момент старта операционной системы и, таким образом, постоянно функционируют в оперативной памяти?

а) резидентные вирусы;

б) стелс-вирусы;

в) макровирусы;

г) полиморфные вирусы;

д) троянские кони.

6. К какому классу относятся межсетевые экраны, которые отслеживают текущие соединения и пропускают только такие пакеты, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений?

а) Работающие на сетевом уровне;

б) Работающие на сеансовом уровне;

в) Работающие на уровне приложений;

г) Stateless;

д) Stateful.

7. Как называются антивирусы, которые работают резидентно, предотвращая заражение файлов?

а) детекторы;

б) фаги;

в) ревизоры;

г) вакцины;

д) фильтры.

8. Какие вирусы заражают носители данных?

а) файловые вирусы;

б) загрузочные вирусы;

в) макровирусы;

г) сетевые черви;

д) троянские кони.

9. Как называются VPN, с помощью которых на основе ненадёжной сети создается надежная и защищенная подсеть?

а) Внутрикорпоративный;

б) Защищенные;

в) С удаленным доступом;

г) Доверительные;

д) Межкорпоративные.

10. Какому требованию должен удовлетворять пароль для противодействия фишингу?

а) пароль не должен быть производным от слов любого естественного языка;

б) длина пароля должна составлять 12 и более символов;

в) пароль нельзя открывать никому;

г) разные сервисы должны защищаться разными паролями;

д) пароль должен включать символы разных алфавитов и регистров, цифры, знаки препинания и т.д.

11. Что такое VPN?

а) система обнаружения вторжений;

б) протокол обмена ключами;

в) трансляция сетевых адресов;

г) виртуальная частная сеть;

д) протокол защиты передаваемого потока.

12. Каков основной недостаток обнаружения вирусов путем эвристического сканирования?

а) значительная вероятность ложного срабатывания;
б) крайне медленная работа антивируса;
в) невозможность обнаружения новых вирусов;
г) необходимость трудоемкой ручной настройки антивируса.

Практические задания

1. Ролевая игра

Разбейтесь на группы из 5 человек. Каждая группа выбирает сферу деятельности из представленного ниже списка:

— производство высокотехнологичных товаров
— рекламное агентство
— разработка программного обеспечения
— банк
— университет

Придумайте название для вашей организации, ее миссию, положение на рынке, основные задачи. Опишите особенности вашей организации в двух-трех абзацах.

Распределите между собой роли, соответстующие организационной структуре вашей организации (директор предприятия, начальник ИТ-отдела, директор охраны, администратор сети и т.д.).

Составьте политику безопасности вашей организации. Каждый участник группы отвечает за раздел политики безопасности, соответствующей своей роли.

Оценка задания будет включать как индивидуальную оценку каждого участника, так и групповую (полнота и согласованность).

2. Программирование

Используя любой язык программирования, напишите программу, реализующую соответствующий алгоритм шифрования/дешифрования (варианты распределеяются преподавателем):

1. Модифицированный шифр Цезаря (ключом является любое число).
2. Моноалфавитный шифр (шифр простой замены)
3. Шифр Гронсфельда
4. Шифр Плейфейера
5. Шифр Хилла
6. Простой перестановочный шифр
7. Решетка Флейберга
8. Скремблер

Следующие варианты заданий являются усложненными и могут предлагаться группам по 2 человека.

9. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте Шифр Хилла в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования.
10. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте Шифр Гронсфельда в качестве

симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования.

11. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте решетку Флейберга в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования.
12. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте Шифр Плейфейера в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования.
13. Запрограммируйте линейный конгруэнтный генератор псевдослучайных чисел.
14. Запрограммируйте смешанный квадратичный генератор псевдослучайных чисел

Следующие варианты представляют задания повышенной сложности и могут выполняться группами по 3 человека.

15. Разработайте программу, реализующую модель безопасности Белла-ЛаПадула. Основные функции программы: регистрация пользователей (при регистрации пользователь получает уровень допуска), авторизация, создание текстовых заметок (при создании заметка получает уровень секретности), просмотр и редактирование заметок.
16. Разработайте программу, реализующую диспетчер безопасности на основе ACL. Функции программы: регистрация объектов, регистрация субъектов, просмотр и редактирование привилегий, вход от лица субъекта и попытка доступа к объекту.
17. Разработайте программу, реализующую диспетчер безопасности на основе списков полномочий субъектов. Функции программы: регистрация объектов, регистрация субъектов, просмотр и редактирование привилегий, вход от лица субъекта и попытка доступа к объекту.

3. Использование прикладных программ

1. Установите и настройте любой антивирус. Проверьте ваши жесткие диски в режиме сканнера таким образом, чтобы антивирус сформировал лог в виде файла. Отправьте этот файл преподавателю как результат выполнения задания.
2. Установите программу PGP. Сгенерируйте пару ключей: открытый и закрытый. Отправьте ваш открытый ключ преподавателю. В ответ вы получите открытый ключ преподавателя и зашифрованное для вас сообщение, подписанное электронной цифровой подписью. Расшифруйте сообщение. Проверьте ЭЦП (она может оказаться неверной). Отправьте преподавателю ответное зашифрованное сообщение, подписанное вашей электронной цифровой подписью. В сообщении напишите результат проверки ЭЦП преподавателя и текст, содержащийся в расшифрованном вами сообщении.

Список литературы

1. Брюс Шнайер. Секреты и ложь. Безопасность данных в цифровом мире. СПб.: Питер, 2003.
2. Вильям Столлингс. Криптография и защита сетей: принципы и практика, 2-е изд. : Пер. с англ. — М., Издательский дом «Вильямс», 2001.
3. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. — М.: МИФИ, 1995.
4. Домарев В.В. "Безопасность информационных технологий. Методология создания систем защиты" – К.: ООО "ТИД "ДС", 2002.
5. Шаныгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2008.
6. Элсенпитер Р., Тоби Дж. Велт. Администрирование сетей Microsoft Windows XP Professional. Эком, 2006.
7. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография — М.: Норма, 2004
8. Гриняев Сергей. Системы обнаружения вторжений. Журнал «Connect! Мир Связи», 08.2003. — http://www.connect.ru/article.asp?id=3884
9. Б.А. Погорелов, А.В.Черемушкин, С.И.Чечета. Об определении основных криптографических понятий. http://www.ict.edu.ru/ft/002455/pogorelov.pdf
10. ФЗ «Об электронной цифровой подписи».
11. Доктрина информационной безопасности Росийской Федерации — справочно-правовая система "КонсультантПлюс".
12. ГОСТ Р 34.10—2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
13. ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования.» — М.: Госстандарт России, 1994.
14. ГОСТ 28147—89 «Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» — М.: Госстандарт СССР, 1989.
15. Руководящий документ Государственной технической комиссии при Президенте РФ «Защита от несанкционированного доступа к информации» — справочно-правовая система "КонсультантПлюс".
16. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. — М.: ДМК, 2000.
17. Новиков В.Е., Ридель В.В. Введение в криптологию: Учебное пособие для студентов, специализирующихся в области защиты информации. — Саратов: изд-во СГУ, 2000.
18. Черкасов В.Н. Бизнес и безопасность. Комплексный подход. — М.: Армада-пресс, 2001.
19. Девянин П.Н. Модели безопасности компьютерных систем: Уч. пособие для студентов ВУЗов. — М.: Академия, 2005.

20. Панасенко С.П., Батура В.П. Основы криптографии для экономистов: Уч. пособие / Под ред. Л.Г. Гагариной. — М.: Финансы и статистика, 2005.
21. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей. — СПб.: БХВ-Петербург, 2000.

Глоссарий

Алгоритмы шифрования с открытым ключом — алгоритмы шифрования, в которых используются два ключа: один (закрытый) предназначен для шифрования сообщения, а второй (закрытый) — для расшифровывания.

Апеллируемость — возможность доказать, что автором является именно данный человек и никто другой.

Атака — попытка реализации угрозы.

Аутентификация пользователей — процесс, с помощью которого одна сторона (проверяющий) убеждается в идентичности другой стороны.

Аутентичность — возможность достоверно установить автора сообщения.

Бэкдор (backdoor) — программа, позволяющая злоумышленнику получать удаленный доступ к системе и возможность удаленного управления ею.

Блочные шифры — алгоритмы шифрования, в которых единицей шифрования является блок (последовательность бит фиксированной длины), преобразовываемые в блок зашифрованного текста такой же длины.

Виртуальная частная сеть (VPN) — логическая сеть, создаваемая поверх другой сети, чаще всего Интернет. За счет криптографической защиты передаваемых данных обеспечивает закрытые от посторонних каналы обмена информацией.

Вирус (компьютерный) — программа, способная к саморазмножению, т.е. способная, создавать свои копии (возможно, модифицированные) и распространять их некоторым образом с компьютера на компьютер.

Генератор псевдослучайных чисел (ГПСЧ) — алгоритм, генерирующий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению (обычно равномерному).

Диспетчер доступа — абстрактная машина, которая выступает посредником при всех обращениях субъектов к объектам и на основании правил разграничения доступа разрешает, либо не разрешает субъекту доступ к объекту.

Диффузия — свойство алгоритма шифрования: каждый бит открытого текста должен влиять на каждый бит зашифрованного текста.

Доступ к информации — ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации

Доступность — свойство информации; наличие своевременного беспрепятственного доступа к информации для субъектов, обладающих соответствующими полномочиями.

Естественные угрозы — угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Загрузочные вирусы — вирусы, распространяющиеся через сменные носители данных и активирующиеся при загрузке с этих носителей.

Зашифрованный текст — текст сообщения после применения к нему процедуры шифрования. Информация, содержащаяся в сообщении, не может быть воспринята без проведения обратного преобразования — расшифровывания.

Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Злоумышленник — нарушитель, намеренно идущий на нарушение из корыстных побуждений.

Информационная безопасность — состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, (в том числе владельцам и пользователям информации).

Информационная безопасность Российской Федерации (согласно доктрине информационной безопасности РФ) — состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Искусственные угрозы — угрозы, вызванные деятельностью человека.

Конфиденциальность — свойство информации; означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем.

Конфузия — свойство алгоритма шифрования: отсутствие статистической взаимосвязи между ключом и зашифрованным текстом.

Криптографическая система — система обеспечения информационной безопасности сети или АИС, использующая криптографические средства.

Криптографические алгоритмы — алгоритмы, предназначенные для противодействия определенным угрозам информационной безопасности со стороны возможного нарушителя или нежелательных воздействий естественного характера. К ним относятся

алгоритмы шифрования/дешифрования, хэширования, формирования и проверки электронной цифровой подписи, распределения ключей и др.

Криптографические средства — методы и средства обеспечения информационной безопасности, использующие криптографические преобразования информации. В узком смысле под криптографическими средствами могут пониматься отдельные устройства, документы и программы, использующиеся для выполнения функций криптосистемы.

Криптографический протокол — протокол, использующийся при выполнения действий по обмену информацией для предотвращения определенных угроз информационной безопасности (в ситуации, когда цели участников могут быть нарушены злоумышленником).

Криптографическое преобразование информации — преобразование информации с использованием одного из криптографических алгоритмов.

Криптография — область науки, техники и практической деятельности, связанная с разработкой, применением и анализом криптографических систем защиты информации.

Макровирусы — разновидность файловых вирусов, заражают файлы документов, позволяющие хранить внутри себя команды на макроязыке.

Матрица доступа — таблица, в которой строки соответствуют субъектам, столбцы — объектам доступа, а на пересечении строки и столбца содержатся правила (разрешения) доступа субъекта к объекту.

Межсетевой экран (брандмауэр, файрвол) — комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Модель безопасности — описание требований безопасности к автоматизированной информационной системе. Обычно заключается в определении потоков информации, разрешенных в системе, и правил управления доступом к информации.

Нарушение — реализация угрозы.

Нарушитель — лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Неформальная модель нарушителя — описание верояного нарушителя, включающее его потенциальные возможности и знания, время и место действия, необходимые усилия и средства для осуществления атаки и т.п.

Объект доступа — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа

Односторонность хэш-функции. Свойство хэш-функции: для любого хэша h должно быть практически невозможно вычислить или подобрать сообщение с таким хэшем.

Открытый текст — исходный текст сообщения до применения к нему процедуры шифрования. Доступен для восприятия и обработки.

Перестановочные алгоритмы шифрования — класс симметричных алгоритмов шифрования, в которых шифрование осуществляется путем изменения порядка следования символов или бит открытого текста.

Подстановочные алгоритмы шифрования — класс симметричных алгоритмов шифрования, в которых шифрование осуществляется путем замены каждого символа (бита) или последовательности символов (битов) открытого текста другим символом (битом) или последовательностью символов (битов).

Полиморфные вирусы — вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совладать ни в одном бите.

Политика безопасности — совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которыми руководствуется организация в своей деятельности.

Потоковые шифры — алгоритмы шифрования, в которых символы (байты или биты) открытого текста шифруются последовательно.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Протокол — последовательность шагов, которые предпринимают две или большее количество сторон для совместного решения некоторой задачи.

Протокол обмена ключами — это такой протокол, с помощью которого знание некоторого секретного ключа разделяется между двумя или более сторонами, причем противник, имеющий возможность перехватывать пересылаемые сообщения, не способен этот ключ получить.

Резидентные вирусы — вирусы, постоянно функционирующие в оперативной памяти ЭВМ (обычно автоматически запускаются в момент старта системы).

Сетевые черви — вирусы, распространяющие свои копии по сети.

Симметричные алгоритмы шифрования — алгоритмы шифрования, в которых один и тот же ключ K используется для того, чтобы зашифровать сообщение и для его последующей расшифровки.

Система обнаружения вторжений (Intrusion Detection System — IDS) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими (в основном через Интернет).

Система разграничения доступа (СРД) — это совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

Скремблеры — программные или аппаратные реализации алгоритма, позволяющего шифровать побитно непрерывные потоки информации.

Стелс-вирус — вирус, полностью или частично скрывающий свое присутствие путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т.д.)

Стойкость к коллизиям первого рода. Свойство хэш-функции: для любого сообщения должно быть практически невозможно вычислить или подобрать другое сообщение с точно таким же хэшем.

Стойкость к коллизиям второго рода. Свойство хэш-функции: должно быть практически невозможно вычислить или подобрать любую пару различных сообщений с одинаковым хэшем.

Субъект доступа — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Троянский конь — вредоносная программа, маскирующаяся под программу, выполняющую полезные функции.

Туннель — канал между двумя узлами, защищенный за счет шифрования проходящего по нему трафика.

Угроза – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Угроза информационной безопасности — потенциально возможное событие, действие, процесс или явление, которое посредством воздействия на информацию или компоненты АИС может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений.

Файловые вирусы — вирусы, внедряющиеся ("заражающие") исполняемые файлы путем записывания в них своего тела (команд).

Фишинг — процедура «выуживания» паролей случайных пользователей Интернета. Обычно заключается в создании «подставных» сайтов, которые обманом вынуждают пользователя ввести свой пароль.

Хэш — результат применения к сообщению хэш-функции.

Хэш-функция — функция, преобразующая сообщение произвольной длины в значение H(M) фиксированной длины, называемое хэшем сообщения. Обладает свойствами односторонности, стойкости к коллизиям первого и второго рода.

Целостность — свойство информации; заключается в сохранности информации в неискаженном виде (отсутствие неправомочных и непредусмотренных владельцем информации искажений).

Шифрование — процесс преобразования исходного сообщения открытого текста в зашифрованный текст таким образом, что простое обратное преобразование возможно только при наличии некоторой дополнительной информацией — ключа.

Экранирование — средство разграничения доступа клиентов из одного множества информационных систем к серверам из другого множества информационных систем.

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Актуальные проблемы уголовно-правовой борьбы с посягательствами на компьютерную информацию (по УК РФ)

Материал для дополнительного чтения и семинарских занятий специальности «Прикладная информатика (в юриспруденции)»

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, —

наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предвари- тельному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, —

наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами —

наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, —

наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, —

наказывается лишением права занимать определенные должности или заниматься определенной деятельностью На срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, —

наказывается лишением свободы на срок до четырех лет.

Глава 1. Криминологическая характеристика компьютерных преступлений

1.1. Криминологический анализ преступлений в сфере компьютерной информации

В специальной литературе (в том числе зарубежной) наряду с термином «преступления в сфере компьютерной информации», использованным в законодательстве РФ, применяются термины «компьютерные преступления», «киберпреступления», «преступления в сфере высоких технологий» и т.д. При этом ряд авторов полагает, что все названные преступления являются просто особой формой существующих «традиционных» преступлений, специфика которых состоит в использовании для достижения противоправных целей компьютера или компьютерных коммуникаций. Выделять эти преступления в отдельную категорию вообще не имеет смысла, как не имеет смысла выделять преступления, совершенные с использованием телефона как «телефонные преступления». Наиболее последовательно данная позиция просматривается в работах А.Б. Нехорошева [1], где предлагается полное реформирование уголовного законодательства: изъятие из него 28-й главы и добавление соответствующих квалифицирующих признаков в другие статьи.

Далее наряду с термином, предложенным законодателем, мы будем пользоваться термином «компьютерные преступления», достаточно устоявшимся и вошедшим в некоторые учебники по уголовному праву.

На основе анализа уголовных дел по преступлениям, совершенным с использованием средств компьютерной техники, авторы выделяют свыше 20 основных способов совершения преступлений в сфере компьютерной информации и около 40 их разновидностей. Число их постоянно увеличивается по причине использования преступниками новых комбинаций и логической модификации алгоритмов. Такое поведение обусловлено как сложностью самих средств компьютерной техники, так и разнообразием и постоянным усложнением выполняемых информационных операций, многие из которых обеспечивают движение материальных ценностей, финансовых и денежных средств, научно-технических разработок и т.д.

Криминологическая особенность компьютерных преступлений заключается в их необычайно высокой латентности. По оценкам специалистов, от 85 до 97% компьютерных преступлений остаются не обнаруженными или о них не сообщается в правоохранительные органы по различным причинам [2]. Часто виновные лица просто увольняются или переводятся в другие структурные подразделения. Иногда с виновного взыскивается ущерб в гражданском порядке. Это можно объяснить наличием ряда факторов.

1). Компьютерный преступник, как правило, не рассматривается как типичный уголовный преступник. 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. Осужденный же преступник приобретает широкую известность в деловых и криминальных кругах, что в дальнейшем позволяет ему с выгодой использовать приобретенный опыт.

2). Расследование компьютерных преступлений может нарушить нормальное функционирование организации, привести к приостановке ее деятельности. Жертва компьютерного преступления убеждена, что затраты на его раскрытие (включая потери, поне-

сенные в результате утраты своей репутации) существенно превосходят уже причиненный ущерб.

3). Правильная квалификация преступлений зачастую затруднена в связи с непроработанностью законодательства. Правоохранительные органы не склонны относить многие компьютерные правонарушения к категории преступлений и, соответственно, отказывают в возбуждении уголовного дела.

4). Жертва боится серьезного, компетентного расследования, так как оно может вскрыть неблаговидный, если не незаконный, механизм ведения дел в организации. Расследование компьютерных преступлений может выявить несостоятельность мер безопасности, принимаемых ответственным за них персоналом организации, привести к нежелательным осложнениям, постановке вопросов о профессиональной пригодности и т.д. Кроме того, раскрытие компьютерных преступлений, сопряжено, как правило, с открытием финансовых, коммерческих и других служебных тайн, которые могут стать достоянием гласности во время судебного рассмотрения дел.

В этом отношении показательны данные, полученные Агентством систем защиты информации DISA. Специалисты агентства предприняли эксперимент, призванный показать, как реагируют владельцы на попытки проникновения в их компьютерные системы. Из 38 тыс. смоделированных нападений только 35% было блокировано системами безопасности. Из 24 700 «успешных» нападений почти 96% не было обнаружено. Но даже о проникновениях, выявленных персоналом систем, в 73% случаев не было сообщено в правоохранительные органы. Таким образом, сообщения о нарушениях поступили лишь в 0,7% случаев от общего числа нападений и в 27% из обнаруженных случаев. Достаточно хорошо коррелируют с этими результатами данные, полученные специалистами ФБР, имитировавшими нападение на 8932 системы. Из 7860 «успешных» атак только 390 были обнаружены (5%), и только в 19 случаях сообщения о нападениях поступили в правоохранительные органы (0,2% от общего числа нападений) [2].

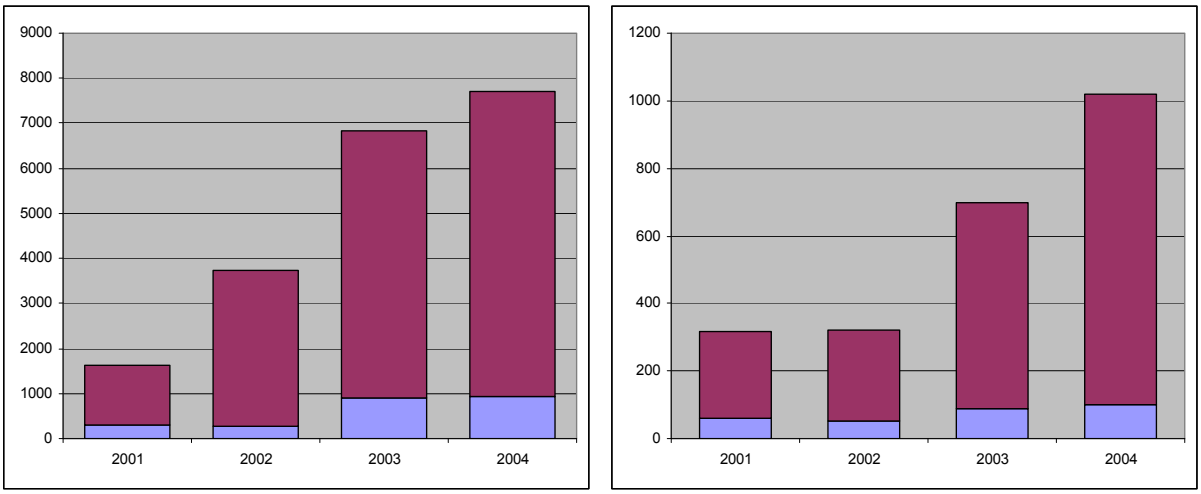

Рис. 1.1. Соотношение зарегистрированных и раскрытых (снизу) преступлений по ст. 272 УК РФ (слева) и ст. 273 УК РФ (справа).

Если же факт совершения преступления обнаруживается, то преступника удается выявить лишь в 10% случаев, о чем свидетельствуют данные российской криминологии. Диаграммы, приведенные на рис. 1.1, наглядно отображают соотношение зарегистриро-

ванных и раскрытых преступлений в 2001—2004 гг. Как видно, при тенденции к увеличению общего числа преступлений, соотношение остается прежним. Таким образом, обнаруженным и раскрытым оказывается только одно преступление из ста совершенных.

Зарегистрированные преступления в информационной сфере обнаруживаются следующим образом: 1) выявляются в результате регулярных проверок доступа к данным службами коммерческой безопасности — 31%; 2) устанавливаются с помощью агентурной работы, а также при проведении оперативных мероприятий по проверкам заявлений граждан (жалобам клиентов) — 28%; 3) случайно — 19%; 4) в ходе проведения бухгалтерских ревизий — 13%; 5) в ходе расследования других видов преступлений — 10% [3].

Отмечается постоянный рост числа компьютерных преступлений и увеличение их доли в общем числе преступлений. Так, в 2004 г. было зарегистрировано в 4,2 раза больше преступлений, чем в 2001 г. В 2001 г. компьютерные преступления составляли 0,07% от общего числа, а в 2004 г. уже 0,3%. Динамика роста компьютерных преступлений отражена на рис. 1.2.

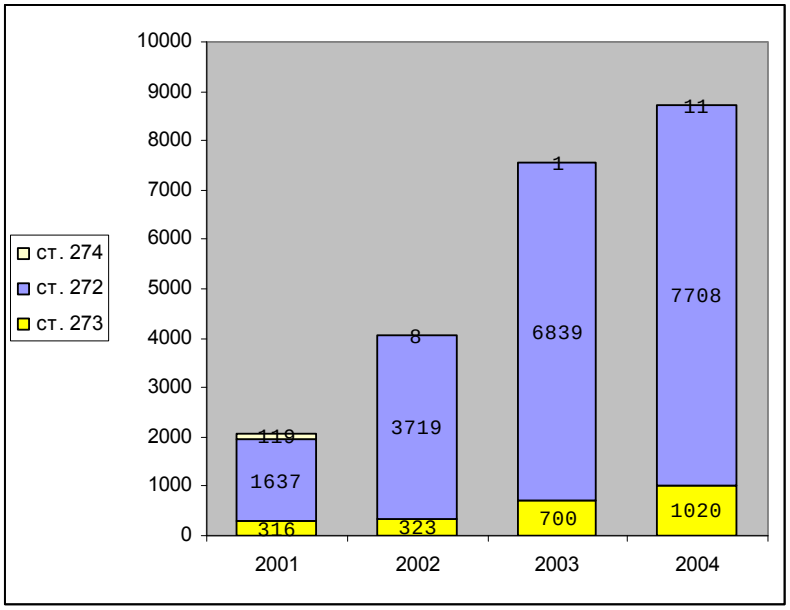

Рис. 1.2. Количество преступлений в сфере компьютерной информации, зарегистрированных в 2001 — 2004 гг.

Как видно из рисунка, больше всего преступлений зарегистрировано по ст. 272 УК РФ (88% от общего числа компьютерных преступлений в 2004 г.). Наименее распространенным является преступление, предусмотренное ст. 274 УК РФ. По данным ГИЦ МВД России, в 1997 г. в Российской Федерации не было зарегистрировано ни одного факта нарушения правил эксплуатации ЭВМ, их системы или сети, в 1998 г. — одно преступление, в 1999 г. — ни одного, а в 2000 г. их количество составило 44. По итогам 2001 г. число фактов нарушения правил эксплуатации ЭВМ достигло отметки 119, но в 2003 г. вновь зарегистрировано всего одно преступление. По мнению ученых, приведенные данные свидетельствуют, прежде всего, о недостаточной работе правоохранительных органов по выявлению фактов данных преступлений [4].

Типичные 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.);

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).

Отечественные эксперты так оценивают размеры финансовых потерь от всех видов компьютерных преступлений: менее 1000 долл. — 28%; 1000—10000 долл. — 21%; 10000—100000 долл. — 35%; свыше 100000 долл. — 16% [3]. По данным ФБР, среднестатистический ущерб от такого преступления составляет 650000 долл., в то время как от обычного ограбления — 9000 долл. Дело в том, что компьютерные преступники способны наносить максимальный ущерб при минимуме затрат. Размер кражи для злоумышленника не принципиален, так как в отличие от обычного ограбления у него нет необходимости бегать по улицам с «миллионом долларов мелкими купюрами».

Как видно из приведенных данных, компьютерные преступления несут высокую общественную опасность, обусловленную главным образом высокой латентностью и, как следствие, безнаказанностью большинства преступников. Статистика показывает постоянное увеличение числа компьютерных преступлений и их доли в общем числе преступлений, поэтому данная сфера, пока еще недостаточно изученная и проработанная, требует усиленного внимания как законодательных, так и правоохранительных органов.

1.2. Особенности личности преступника, совершающего компьютерные преступления

В настоящее время совокупность лиц, совершающих преступления в глобальных сетях, нельзя считать гомогенной группой. Данная совокупность достаточно разнородна по своему составу. Как следствие, обречено на неудачу стремление построить единый обобщенный портрет всех личностей, совершающих противоправные действия в глобальных сетях. Тем не менее, возможно выделение категорий лиц, совершающих компьютерные преступления на основе различных критериев (мотивация, уровень технической подготовленности и т.д.).

По мнению В. Б. Вехова, компьютерных преступников следует разделить на три устойчивые категории, положив в основу классификации мотивы и цели совершения преступлений.

Первая категория — это лица, сочетающие определенные черты профессионализма с элементами изобретательности и развлечения. Такие люди, работающие с компьютерной техникой, весьма любознательны, обладают острым умом, а также склонностью к хулиганству. Они воспринимают меры по обеспечению безопасности компьютерных систем как вызов своему профессионализму и стараются найти технические пути, которые доказали бы их собственное превосходство.

Вторая категория — лица, страдающие особого рода заболеваниями, развившимися на почве взаимодействия со средствами компьютерной техники. 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. В основном этим занимаются из чувства мести уволенные сотрудники, а также люди, страдающие компьютерными неврозами.

Третья категория — это специалисты или профессиональные компьютерные преступники. Эти лица обладают устойчивыми навыками, действуют расчетливо, маскируют свои действия, всячески стараются не оставлять следов. Цели их преимущественно корыстные [5].

Ю.В. Гаврилин предлагает лиц, совершающих компьютерные преступления, разбить на две категории. Первая категория — это лица, состоящие в трудовых отношениях с предприятием (организацией, учреждением, фирмой или компанией), где совершено преступление (по данным автора, они составляют более 55%), а именно: непосредственно занимающиеся обслуживанием ЭВМ (операторы, программисты, инженеры), пользователи ЭВМ, имеющие определенную подготовку и свободный доступ к компьютерной системе, административно-управленческий персонал (руководители, бухгалтеры, экономисты и т.п.). Вторая категория — граждане, не состоящие в правоотношениях с предприятием, где совершено преступление (около 45%). Ими могут быть лица, занимающиеся проверкой финансово-хозяйственной деятельности этого предприятия, пользователи и обслуживающий персонал ЭВМ других организаций, связанных компьютерными сетями с предприятием, а также лица, имеющие в своем распоряжении компьютерную технику и доступ к телекоммуникационным компьютерным сетям.

Подобная классификация используется и правоохранительными органами западных стран. До недавних пор сотрудников пострадавшей организации было принято считать основным субъектом противоправных действий. Так, по данным компании «Информзащита», несанкционированные вторжения собственных сотрудников составляли до 70% в общем объеме нарушений информационной безопасности сетевых объектов. Кроме того, по обобщенным оценкам, более чем в 80% случаев экономических преступлений, совершенных с использованием компьютерных сетей, преступником или его сообщником (пособником, наводчиком) являлся штатный сотрудник учреждения, подвергшегося нападению. Однако в последние годы ситуация постепенно меняется. В отчете ФБР и Института компьютерной безопасности США в качестве основного источника опасности для объектов вычислительной техники называются внешние подключения к сети Интернет (в 2001 г. — 74% инцидентов; в 2000 г. — 70%; в 1999 г. — 59%). Аналогичные оценки приводятся и в обзоре, подготовленном Конфедерацией британской промышленности (Confederation of British Industry). Утверждается, что основная угроза исходит не от работников компании, но в большей степени от хакеров, а также от уволенных сотрудников и представителей организованной преступности [2].

Криминологический феномен хакерского сообщества неоднократно рассматривался в трудах ученых. Термин «хакер» используется в двух значениях. Первое имеет негативную окраску, определяет личность с противоправными установками, компьютерного «взломщика»; второе позитивно и подразумевает специалиста в области информационных технологий, профессионала, увлеченного своим делом. В отечественной литературе получает распространение толкование, согласно которому хакеры — это компьютерные хулиганы, одержимые «компьютерной болезнью» и ощущающие патологическое удовольствие от проникновения в чужие информационные сети.

В последнее время получила распространение точка зрения, что хакеры образуют свою субкультуру, наподобие объединения панков, рокеров и т.д. Носители этой субкультуры со временем преодолевают серьезную психологическую трансформацию, связанную со сменой ценностных ориентаций. Объективной реальностью для хакера является компьютерная сеть — основная среда их обитания. Настоящая объективная реальность скучна и неинтересна, однако биологически необходима. Хакеры создают свои объединения (группы), издают электронные журналы, имеют собственный жаргон и постоянно обмениваются опытом с зарубежными «коллегами». Между хакерами и преступниками не всегда уместно ставить знак равенства, но именно хакерская среда оказывает определяющее влияние на компьютерную преступность. Как явление сообщество хакеров не имеет аналогов в правоохранительной практике (лишь по отдельным характеристикам приближаясь к другим криминальным сообществам). Оно имеет сложную организацию, находится в постоянном развитии и достаточно слабо изучено.

Главной проблемой, связанной с хакерами, является мода на них. Принадлежать к хакерской среде считается модным как среди профессионалов в сфере информационных технологий, так и среди подростков и лиц, не имеющих специального образования в области информатики. Эта мода влечет новых лиц к хакерским журналам, атрибутике, сленгу, к использованию хакерских программ (зачастую легко доступным и простым в применении), а, в конечном счете, — к целенаправленному развитию в качестве компьютерного правонарушителя.

В криминологии большую роль играет обобщенный портрет преступника в той или иной сфере. Анализ уголовных дел позволяет констатировать, что компьютерные преступления в подавляющем большинстве (96%) совершаются лицами мужского пола, среди которых явно преобладают молодые люди в возрасте от 14 до 25 лет. При этом кривая, характеризующая возрастное распределение этих лиц (см. рис. 1.3), имеет ярко выраженный максимум в районе 19 лет. Объяснение такой закономерности, по мнению автора, связано с вопросом мотивации субъектов, совершающих сетевые преступления. Именно в этом возрасте у таких лиц особенно высоки потребность в самоутверждении и стремление получить максимальное количество жизненных благ при отсутствии реальной возможности достичь этого.

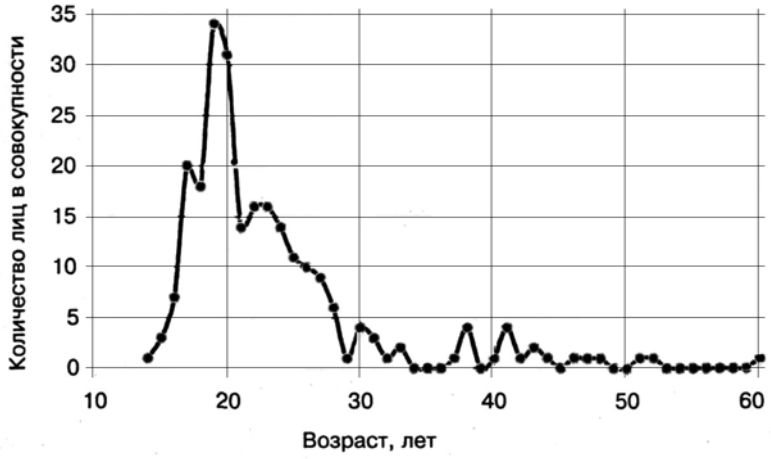

Рис. 1.3. Кривая, характеризующая возрастное распределение компьютерных преступников (из монографии А. Л. Осипенко [2])

По данным Национального центра по борьбе с компьютерной преступностью США, преступления, совершенные с корыстной направленностью, составляют 60—70% от общего числа изученных компьютерных преступлений; по политическим мотивам (терроризм, шпионаж и др.) — 15—20%; из любопытства — 5—7%; из хулиганских побуждений — 8—10%.

В. Б. Вехов называет пять распространенных мотивов совершения компьютерных преступлений: «корыстные соображения — 66%; 2) политические цели — 17%; 3) исследовательский интерес — 7%; 4) хулиганские побуждения и озорство — 5%; 5) месть — 5%» [5]. А. Л. Осипенко предлагает дополнить указанный список недостаточно изученным «игровым мотивом».

Криминологию интересует также психологические особенности личности компьютерного преступника. Среди наиболее распространенных качеств личности, определяющих структуру преступного поведения, по мнению криминологов, преобладают правовой нигилизм и завышенная самооценка.

Правовой нигилизм заключается в том, что, ощущая безнаказанность своих противоправных действий, эти лица часто пренебрегают требованиями норм права, считают допустимым определять моральность тех или иных правовых норм на основе собственных критериев, проявляя инфантилизм, безответственность, непонимание возможных опасных последствий. Криминологи отмечают, что в подобных случаях оценка ситуации осуществляется не с позиций социальных требований, а исходя из личных переживаний, обид, проблем и желаний. Сознательно нарушая определенные запреты, хакеры не принимают наказания, искренне считая себя невиновными. Для них типично оправдывать, например, нанесение ущерба зарубежным фирмам целями высокого порядка («эти фирмы обкрадывают российских пользователей»); считается даже престижным осуществить противоправные действия в отношении организаций, попавших в хакерские списки «носителей зла».

Гипертрофированная самооценка приводит к тому, что зачастую эти лица совершают противоправные деяния спонтанно, без серьезной предварительной подготовки. Под воздействием «комплекса безнаказанности» они оставляют послания руководителям служб безопасности, гордо публикуют сообщения о своих противоправных действиях в сетевых конференциях и чатах. По результатам опросов, проведенных ФБР, до 98% хакеров считают, что их никогда не смогут уличить в хакерстве. Хвастовство и восхищение собственными «подвигами» продолжаются и при даче показаний представителям правоохранительных органов. Компьютерные преступники убеждены, что их сотрудники не способны эффективно выявлять и расследовать подобные преступления.

Рассматривая качества компьютерных преступников, исследователи отмечают и присутствие у них определенных специфических положительных свойств [2]. Эти люди, как правило, являются яркими, мыслящими личностями. Для многих из них характерны достаточный уровень квалификации, глубокие познания в области информационных технологий, высокая работоспособность, упорство. Среди них относительно невысок процент тех, кто ранее подвергался уголовному преследованию. В большинстве своем они не имеют связей в уголовно-преступной среде (за исключением случаев сотрудничества с представителями организованной преступности) и отличаются стремлением иметь в своем окружении положительную репутацию. У компьютерных преступников, как правило, отсут-

ствуют стойкие антиобщественные установки, агрессивность, ими не допускается даже возможность совершения иных видов преступлений, особенно связанных с применением насилия.

Предвидение высокой вероятности наступления правовых последствий для многих из изученных лиц было способно привести к отказу от совершения преступления. Это позволяет предположить, что для таких лиц боязнь ответственности тесно связана со степенью активности правоохранительных органов.

Для российского общества проблема участия представителей «технической элиты» в противоправной деятельности связана и с определенными социальными предпосылками. Вероятность совершения сетевых преступлений повышается в тех регионах, где имеется множество подготовленных профессионалов, не получающих соответствующего своим способностям вознаграждения за свою работу.

Таким образом, опасность встать на путь компьютерных преступлений грозит, в первую очередь, подросткам и молодежи, которых привлекает своеобразная интеллектуальная романтика, «мода» хакерской субкультуры, а также уверенность в относительной безнаказанности и «незначительности» своих общественно опасных деяний. Поэтому решительные действия правоохранительных органов в борьбе с компьютерными преступлениями особенно важны с точки зрения профилактики. Второй потенциально опасной группой являются обиженные специалисты, увольняемые с предприятий. В связи с этим во многих организациях уделяется большое внимание разработке специальных процедур «безопасного» увольнения.

Глава 2. Объект и предмет преступлений в сфере компьютерной информации.

2.1. Особенности объекта преступлений в сфере компьютерной информации

Преступления в сфере компьютерной информации выделены в отдельную, 28 главу УК РФ. Эта глава помещена в девятом разделе Особенной части УК «Преступления против общественной безопасности и общественного порядка». Таким образом, по мнению законодателя, родовым объектом для всех видов компьютерных преступлений является совокупность общественных отношений, составляющих содержание общественной безопасности и общественного порядка.

Одним из классификационных критериев объединения компьютерных преступлений в единую главу является видовой объект посягательства, который составляет совокупность общественных отношений в части правомерного и безопасного использования компьютерной информации и информационных ресурсов.

По поводу непосредственного объекта анализируемых преступлений исследователи придерживаются различных точек зрения.

Учебник Ю. И. Бытко и С. Ю. Бытко лаконично называет непосредственным объектом ст. 272 УК РФ «интересы собственников, владельцев компьютерной информации и порядок доступа к ней»; ст. 273 — безопасность компьютерной информации; ст. 274 — безопасные условия эксплуатации ЭВМ, системы ЭВМ и их сети [6].

Более развернутое толкование дает учебник под редакцией Л.Д. Гаухмана и С.В. Максимова. По мнению его авторов, непосредственным объектом преступления, предусмотренного ст. 272 являются общественные отношения, обеспечивающие правомерные доступ, создание, обработку, преобразование, использование компьютерной информации самим создателем, потребление ее иными пользователями, а также правильное функционирование ЭВМ, системы ЭВМ или их сети. Данное преступление, совершенное лицом с использованием своего служебного положения, посягает и на второй непосредственный объект — общественные отношения, обеспечивающие интересы службы. Статья 273 имеет непосредственным объектом общественные отношения, обеспечивающие безопасность 1) правомерных доступа, создания, обработки, преобразования и использования компьютерной информации; 2) правильного функционирования ЭВМ, системы ЭВМ или их сети; 3) интересов предпринимательства, связанных с оборотом безопасных компьютерных продуктов. Непосредственный объект данного преступления, повлекшего по неосторожности тяжкие последствия, предусмотренные ч.2 ст. 273 УК, — общественные отношения, обеспечивающие в зависимости от характера последних иные социально значимые ценности (жизнь человека, здоровье людей и т.п.). О непосредственном объекте ст. 274 авторы пишут: «Общественные отношения, обеспечивающие: установленный нормативными правовыми актами, собственником или иным владельцем порядок эксплуатации ЭВМ, системы ЭВМ или их сети; интересы создания, обработки, преобразования и использования компьютерной информации, относящейся в соответствии с законом к информации ограниченного доступа самим создателем и потребления другими пользователями; интересы правильного функционирования ЭВМ, системы ЭВМ или их сети. Непосредственный

объект преступления, предусмотренного ч. 2 ст. 274 УК, совпадает по содержанию с соответствующим объектом преступления, предусмотренного в ч. 2 ст. 273 УК» [7].

Третья точка зрения (которой будем придерживаться и мы) заключается в том, что непосредственный объект является общим для всех составов преступлений, собранных в главе 28. Таковым являются общественные отношения по обеспечению безопасности охраняемой законом компьютерной информации и нормальной работы ЭВМ, системы ЭВМ или их сети.

В дальнейшем, проводя анализ составов анализируемых преступлений, мы покажем, что безопасность охраняемой законом компьютерной информации, подразумевающая обеспечение трех ее свойств — конфиденциальность, целостность и доступность — исчерпывающе определяет объект компьютерных преступлений, не допуская вместе с тем его излишне расширительного толкования. Другим непосредственным объектом могут выступать правильные условия эксплуатации ЭВМ, системы ЭВМ или их сети, но лишь в той мере, в которой их нарушение влечет угрозу безопасности охраняемой законом компьютерной информации.

Дополнительный объект факультативен. Его наличие зависит от того вреда, который был причинен правам и законным интересам личности, общества и государства. Дополнительным объектом может, например, выступать собственность, авторское право, право на неприкосновенность частной жизни, личную и семейную тайну, экологическая безопасность, основы конституционного строя Российской Федерации и др. Наличие дополнительного объекта, безусловно, повышает степень общественной опасности преступления, что подлежит обязательному учету при назначении виновному справедливого наказания.

2.2. «Компьютерная информация» как предмет преступлений главы 28 УК РФ

Некоторое время существовала точка зрения, что предметом компьютерных преступлений является компьютер как информационная система, носитель информации. В настоящий момент эта позиция отвергнута и исследователи единодушны во мнении, что предметом преступлений, выделенных в 28-ю главу УК РФ, является компьютерная информация или информационные ресурсы, содержащиеся на машинном носителе, в ЭВМ, системе ЭВМ или их сети. Они выступают в качестве нематериальных ценностей, на которые непосредственно воздействует виновный, осуществляя преступное посягательство на общественные отношения по обеспечению безопасности такой информации, а также нормальной работы ЭВМ, системы ЭВМ или их сети.

На практике могут возникнуть ситуации, когда преступное воздействие на будет осуществляться непосредственно на электронно-вычислительную технику (например, похищение ЭВМ и осуществление неправомерного доступ к содержащейся в ней информации в удобных для злоумышленника условиях). Действия такого лица следует квалифицировать по совокупности преступлений (ст. 272 и соответствующей статье, расположенной в главе 21 Особенной части УК РФ). Электронно-вычислительная машина рассматривается в качестве предмета преступления против собственности, а компьютерная информация, воздействие на которую осуществляется чуть позже — предметом преступления, предусмотренного ст. 272 УК РФ.

2.2.1. Понятие компьютерной информации

Современный уровень развития научного знания еще не позволяет, а возможно и никогда не позволит, дать точное и законченное определение понятия «информация». С развитием нашего представления о мире, с развитием науки содержание этого понятия расширяется и углубляется.

Норберт Винер в своей работе «Кибернетика или управление и связь в животном и машине» определяет информацию как «обозначение содержания, черпаемого нами из внешнего мира в процессе приспособления к нему и приведения в соответствие с ним нашего мышления». Т.е. информация определяется через категорию «содержание внешнего мира» и напрямую увязана с человеком, его мышлением и процессом приспособления человека к явлениям и событиям внешнего мира. Иными словами, Винер утверждает, что информация вне человеческого сознания не существует.

Отождествление информации со сведениями или фактами, которые теоретически могут быть получены и усвоены, то есть, преобразованы в человеческие знания, составляет суть антропоцентрического подхода к определению понятия «информация».

До последнего времени антропоцентрический подход удовлетворительно работал в области правовых и общественных наук. Однако в связи с широким внедрением вычислительной техники его недостатки все чаще дают о себе знать. Во-первых, подход к информации только как к сведениям не позволяет адекватно интерпретировать информационные процессы в таких объектах, как компьютерные программы, компьютерные сети, системы искусственного интеллекта, системы, ориентирующиеся в состоянии неопределенности. Здесь процессы получения, преобразования, передачи информации могут проходить без этапа осмысления их человеком. Во-вторых, в рамках антропоцентрического подхода невозможно найти адекватного объяснения генетической информации живой природы. В связи с этим возникла потребность в изменении трактовки понятия информации. Оно было расширено и включило обмен сведениями не только между человеком и человеком, но также «между человеком и автоматом, автоматом и автоматом, обмен сигналами в животном и растительном мире, передачу признаков от клетки к клетке».

Наиболее плодотворное проникновение в сущность понятия «информация» осуществил К. Шеннон в работах, опубликованных в конце 40-х годов XX в. В них под информацией понимаются лишь те сообщения, которые уменьшают неопределенность у получателя этого сообщения. Таким образом, по Шеннону информация — величина, обратная энтропии, то есть неопределенности.

В российском законодательстве в настоящее время применяется антропоцентрический подход. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» определяет информацию как «сведения независимо от формы их представления». Таким образом, современное российское право регулирует лишь те информационные отношения, в которых информация может быть каким-либо образом воспринята и проинтерпретирована человеком.

Федеральный закон «Об информации, информационных технологиях и защите информации» является основным источником данных законодателем определений в области регулируемых правом информационных отношений. Среди прочих источников важно отметить Конституцию Российской Федерации, Закон РФ от 4 июля 1996 г. № 85-ФЗ «Об

участии в международном информационном обмене», Гражданский Кодекс РФ (4 часть). Ряд требований к применяемой терминологии содержится в «Концепции формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсах» (одобрена решением Президента Российской Федерации от 23.04.95 г. № Пр-1694) и «Концепции правовой информатизации России» (утверждена Указом Президента Российской Федерации от 23.04.93 г. № 477). Существуют и совершенно конкретные требования к понятиям и определениям, зафиксированные в государственных стандартах и документах и регламентирующие их. К сожалению, эти требования (в том числе и закрепленные в международных договорах о стандартизации) не всегда учитываются законодателем.

Глава 28 УК РФ имеет название «Преступления в сфере компьютерной информации». Статья 272 уточняет, что речь идет об «информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети».

Представляется, что законодателю не стоило изобретать собственный термин. В информатике давно используется соответствующее понятие, а именно *данные* это форма представления информации, удобная для восприятия и обработки ее на ЭВМ (как правило, информация преобразовывается в данные с помощью двоичного кодирования).

Вместо того чтобы положить в основу определения форму представления информации, (которая, однако подразумевается неявно), законодатель приводит исчерпывающее перечисление возможных носителей информации, причем, не приводя определения ни одного из этих носителей, что вызывает массу проблем в правоприменительной практике.

Прежде всего, непростым оказывается вопрос об отнесении конкретного электронного устройства к категории электронно-вычислительной машины. В частности, можно ли считать ЭВМ так называемые интегрированные системы (компьютеры в нетрадиционном понимании — пейджеры, сотовые телефоны, электронные контрольно-кассовые машины, электронные банкоматы) и, соответственно, как квалифицировать неправомерные действия с рассматриваемыми объектами?

Толковый словарь по вычислительной технике и программированию утверждает, что ЭВМ есть цифровая вычислительная машина, основные узлы которой реализованы средствами электроники. В комментарии к уголовному кодексу под редакцией Ю.И. Скуратова и В.М. Лебедева ЭВМ определяется как «совокупность технических средств, создающая возможность проведения обработки информации и получения результата в необходимой форме». В комментарии к УК РФ под ред. С.И. Никулина содержится следующее определение: «ЭВМ представляет собой совокупность аппаратно-технических средств и средств программирования, позволяющих производить операции над символьной и образной информацией». Ю.В. Гаврилин приходит к следующему определению: «ЭВМ — электронное устройство, производящее заданные управляющей программой операции по хранению и обработке информации и управлению периферийными устройствами» [4] и в его рамках утвердительно отвечает на вопрос об отнесении к ЭВМ так называемых интегрированных систем.

9 ноября 1998 года УРОПД ГУВД Московской области было возбуждено уголовное дело по факту совершения неправомерного доступа к охраняемой законом компьютерной информации в кассовых аппаратах одного из частных предпринимателей города Павловский Посад. По статье 272 УК РФ в ходе следствия было квалифицировано изме-

нение информации в контрольно-кассовых аппаратах, при которых записанная в них сумма выручки за смену искусственно занижалась. Контрольно-кассовые аппараты были признаны следствием электронно-вычислительными машинами.

Понятие «система ЭВМ», введенное законодателем, также неоднозначно трактуется в юридической литературе. Ю.В. Гаврилин предлагает исходить из того, что понятие «система» предполагает определенную совокупность объектов, элементы которой находятся в упорядоченной взаимосвязи и взаимозависимости и под системой ЭВМ следует понимать упорядоченную совокупность взаимосвязанных и взаимодействующих как единое целое ЭВМ, обеспечивающих выполнение единой функции [4]. Другие авторы полагают, что систему образует ЭВМ вместе со своими перефирийными устройствами (принтер, сканнер и т.п.).

Оба подхода заслуживают определенного внимания. Второй хорош тем, что включает в охваченную законодателем сферу информацию, хранящуюся, например, в собственной памяти принтера.

Сеть ЭВМ можно определить как способ организации связи между несколькими самостоятельными ЭВМ с целью получения доступа к совместными информационным ресурсам или оборудованию. Однако среди исследователей нет единодушия в том, считать ли таковой глобальную сеть общего пользования — Интернет.

Расплывчатые формулировки законодателя вынуждают исследователей приводить дополнительные толкования термина «компьютерная информация». Одно из наиболее цитируемых принадлежит В.В. Крылову. Он пишет: «Компьютерная информация есть сведения, знания или набор команд (программ), предназначенных для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях, — идентифицируемый элемент информационной системы, имеющей собственника, установившего правила ее использования» [8].

Многие исследователи принципиально против рассмотрения «компьютерной информации» как особого объекта правоотношений. Так, например, А.Б. Нехорошев пишет: «Опираясь на тип носителя, с таким же успехом можно говорить о бумажной, текстильной, пластмассовой, кожаной, каменной информации и т.д. и т.п. В корне неверно классифицировать объект по второстепенным признакам, а ведь информация не меняется при изменении носителя» [1].

Это мнение весьма спорно. Компьютерная информация (данные) принципиально отличаются от информации вообще. Так, например, данные обладают свойством «уничтожаемости», говорить же о возможности уничтожения информации можно лишь в рамках антропоцентрического подхода, подразумевая уничтожение всех существующих носителей данной информации, включая людей. При этом информация, веками считавшаяся утерянной (уничтоженной) может быть в любой момент восстановлена с помощью новых научно-технических методов. Применительно к «чистой» информации можно говорить лишь о ее постепенном рассеянии, бесконечном приближении к исчезновению. Поэтому бессмысленно рассматривать и такой вид противоправных деяний как уничтожение информации.

Компьютерная информация (данные) отличается от «бумажной» или «каменной» принципиально иным способом обработки. Данные могут очень легко создаваться, модифицироваться, копироваться и уничтожаться, что придает им особые качества. Например,

если такие данные позволяют определить сумму переводимых на счет злоумышленника денежных средств при проникновении его в систему банка, положение запятой в указанной сумме может изменить объем похищенного на несколько порядков.

Для уничтожения компьютерной информации, равной 500 страницам текста, необходимо два нажатия клавиши клавиатуры, и через три секунды она будет бесследно стерта, в то время как для сжигания 500 страниц машинописного или рукописного текста необходимы специальные условия и значительный промежуток времени.

Эта особая «уязвимость» компьютерной информации по сравнению с информацией «бумажной» — а отсюда и уязвимость общественных отношений в сфере создания, распространения и использования такой информации — и побудила законодателя, на наш взгляд, совершенно обоснованно, выделить преступления в сфере компьютерной информации в качестве отдельной главы уголовного права.

Заметим, что хотя глава 28 УК РФ посвящена именно компьютерной информации, в явном виде этот термин приведен только в ст. 272. В ст. 273 речь идет уже об «информации», а ст. 274 оперирует непонятным термином «информация ЭВМ». Это выглядит явным недочетом, поскольку очевидно, что в статьях 273 и 274 речь идет именно о компьютерной информации — только данные подвержены угрозам со стороны вредоносных программ или нарушения правил эксплуатации ЭВМ.

Безусловно, используемые в УК термины должны быть законодательно закреплены, причем в различных нормативных актах должна соблюдаться единая терминология. При этом следует пользоваться достижениями других наук, в которых соответствующие термины достаточно устоялись, а не изобретать собственные. Игнорирование этого вопроса является главной проблемой современного уголовного законодательства в области компьютерных преступлений.

2.2.2. Свойства компьютерной информации

Хотя формального определения информации не существуют, среди исследователей не возникает споров относительно её свойств. В многочисленных трудах по кибернетике, информационным технологиям, а также в юридических учебниках содержание понятия «информация» зачастую раскрывается через её свойства. Число этих свойств у разных исследователей неодинаково, но связано это лишь с тем, что в рамках отдельной научной дисциплины не все свойства информации имеют значение.

Так, например, изучая информацию как особый объект судебной экспертизы и сравнивая свойства материальных и информационных объектов, С.А. Смирнова подробно описывает 21 различие [9]. В учебнике «Правовая информатика» Чубуковой С.Г. И Элькина В.Д. таких значимых с точки зрения авторов свойств девять, в том числе неисчерпаемость, массовость, универсальность и т.д. Причем, говоря о свойстве «качество», авторы разлагают его на восемь других свойств, таких как полнота, избыточность, адекватность, актуальность и т.д.

Уголовное законодательство восприняло (хотя и не назвало их явно) центральные свойства, изучаемые в рамках информационной безопасности: конфиденциальность, целостность и доступность. Их принципиальное отличие от всех остальных свойств заключается в том, что они не присущи информации как таковой, а появляются лишь в результате принятия мер иного, организационного характера. Более того, после того как определен-

ная информация (или компьютерная информация) обрела эти свойства, она может их и лишиться — в результате внешних воздействий. Эти воздействия могут явиться как результатом события (например, в результате стихийного бедствия был уничтожен банк данных — потеря целостности и доступности), так и действия. В свою очередь, действия могут быть правомерные и неправомерные. Учитывая, что информация, обладающая указанными свойствами (всеми тремя или двумя последними) имеет гораздо большую ценность, чем информация, такими свойствами не обладающая, неправомерные деяния, их нарушающие, наносят значительный ущерб собственнику информации, а значит — и общественным отношениям в данной области.

Таким образом, логичной является позиция законодателя, обеспечившего уголовно-правовые средства защиты этих важных свойств. Заметим, что остальные многочисленные свойства информации не нуждаются в защите такого рода. Часть из них неотъемлема по самой природе информации (идеальность, неисчерпаемость), другими же, такими как достоверность или объективность, информация может либо обладать, либо не обладать, но их изменение невозможно — это будет уже другая информация.

В 28-й главе УК РФ используется общий для УК подход, при котором в основу классификации преступлений положена их объективная сторона. Угрозы компьютерной информации рассматриваются не с точки зрения её свойств, которые нарушаются в результате неправомерных действий (бездействия), а с точки зрения самих этих действий. Как будет показано нами далее, при анализе объективных признаков компьютерных преступлений, подобный подход заранее обречен на неполноту, поскольку невозможно исчерпывающе указать перечень действий (бездействий), нарушающих свойства компьютерной информации, тем более в условиях непрерывного развития информационных технологий, средств и способов обработки данных и доступа к ним.

На наш взгляд, разумнее было бы использовать подход, устанавливающий уголовную ответственность за нарушение конфиденциальности, целостности и доступности информации (с учетом равной значимости всех трех свойств ответственность могла бы быть единой), независимо от способа совершения преступления. Отдельные способы, такие как создание или распространение вредоносных программ, в силу их особой общественной опасности могли бы выступить в качестве квалифицирующего признака. Такой подход гарантированно закрыл бы «дыры» в законодательстве, поскольку угрозы компьютерной информации «покрываются» угрозами тремя названным свойствам.

2.3. Охраняемая законом информация

В статьях 272 и 274 УК РФ речь идет об охраняемой законом информации. Такого рода информация может быть разбита на две большие категории: конфиденциальная информация, т.е. информация, составляющая какую-либо тайну, доступ к которой ограничен законодательством, и интеллектуальная собственность. Эта классификация воспринята, в частности, ГК РФ в разделе, посвященном объектам гражданских правоотношений (ст. 138, 139).

Далее мы не будем подробно рассматривать такую категорию, как интеллектуальную собственность. Отметим лишь, что неправомерный доступ к объектам интеллектуальной собственности, представленным в цифровом виде (это могут быть исходные коды программ, тексты литературных произведений и т.д.), повлекший незаконное распростра-

нение (копирование) указанных объектов и собственно незаконное распространение представляют собой разные составы преступлений. Последнее есть нарушение авторских и смежных прав либо нарушение изобретательских и патентных прав. Уголовная ответственность за эти преступления предусмотрена статьями 146 и 147 УК РФ.

В области информации с ограниченным режимом доступа (тайн) наблюдается отсутствие единого подхода к понятийному аппарату. Анализ законодательства РФ на 2000 г. позволял выделить более 30 видов упоминаемых тайн, анализ же подзаконных актов позволял увеличить этот перечень до 40. Ситуация не изменилась и к настоящему времени.

Все виды тайн, охраняемые законом, можно разделить на 4 группы.

1. Тайна частной жизни — это личная тайна и семейная; тайна переписки; тайна телефонных переговоров, телеграфных и иных сообщений; тайна почтовых отправлений; тайна исповеди; тайна голосования; персональные данные.

2. Профессиональная тайна — это банковская тайна; врачебная тайна; адвокатская тайна; нотариальная тайна; журналистская тайна; редакционная тайна; тайна совещательной комнаты; тайна страхования; секреты мастерства; налоговая тайна; сведения о мерах безопасности судей, должностных лиц, правоохранительных и контролирующих органов; служебная информация о рынке ценных бумаг; геологическая информация о недрах.

3. Коммерческая тайна — это конфиденциальные данные и сведения, имеющие коммерческую ценность; «ноу-хау».

4. Государственные секреты — служебная и государственная тайна.

Проблема защиты прав личности, защиты личности от несанкционированного сбора персональных данных, злоупотреблений, возможных при сборе, обработке и распространении информации персонального характера, приобрела особую актуальность в условиях информационного общества, характеризующегося развитием средств вычислительной техники и связи, что позволяет накапливать и обрабатывать значительные массивы информации. Основные принципы правового режима информации о частной жизни определены в части 1 статьи 24 Конституции РФ. Обязательным условием ее сбора, хранения, использования и распространения является согласие лица.

Персональные данные, согласно Федеральному закону РФ «О персональных данных» от 27.07.2006 г. № 152-ФЗ, – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Названный федеральный закон устанавливает следующие принципы обработки персональных данных:

1) законность целей и способов обработки персональных данных;

2) соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

3) соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4) достоверность персональных данных, их достаточность для целей обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5) недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по достижении целей обработки или утраты необходимости в их достижении.

Юридические и физические лица, владеющие информацией о гражданах, получающие и использующие ее, несут ответственность за нарушение режима защиты, обработки и порядка использования этой информации.

Часть 1 статьи 24 Конституции РФ устанавливает общее правило, которое действует в границах пользования правами и свободами, установленными в части 3 статьи 55. Так, не требуется согласия лица на сбор, хранение, использование и распространение сведений о нем при проведении следствия, дознания, оперативно-розыскных мероприятий.

Собирание конфиденциальной информации государственными органами предусмотрено УПК РФ, Законом РФ от 18 апреля 1991 г. № 1026-I «О милиции», Федеральным Законом от 3 апреля 1995 года N 40-ФЗ «Об органах федеральной службы безопасности в Российской Федерации», Федеральным Законом от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности». Статья 41 Закона от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» ограничивает возможность редакции разглашать в распространяемых сообщениях и материалах сведения персонального характера. Согласно части 1 статьи 30 (пункт 6) и части 2 статьи 61 Основ законодательства Российской Федерации об охране здоровья граждан от 22 июля 1993 года № 5487-1, пациент имеет право на сохранение в тайне информации о факте обращения за медицинской помощью, о состоянии здоровья, диагнозе и иных сведениях, полученных при обследовании и лечении, а органы и лица, которым эти сведения стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, обязаны не допускать их разглашения.

В соответствии с ГК РФ информация составляет *служебную или коммерческую тайны* в случаях, если эта информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам; если к этой информации нет свободного доступа на законном основании; если обладатель информации принимает надлежащие меры к охране ее конфиденциальности. Согласно Указу Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», разница между служебной и коммерческой тайной состоит в том, что коммерческая тайна — сведения, связанные с коммерческой деятельностью, а служебная тайна — служебные сведения, доступ к которым ограничен органами государственной власти.

Исходя из анализа законодательства, в литературе предлагается следующее определение: служебная тайна — несекретные сведения, ограничение в распространении которых диктуется служебной необходимостью в органах государственной власти, в подведомственных им предприятиях, учреждениях и организациях. По общему смыслу понятия «служебная тайна» можно предположить то, что носителями этой тайны должны быть субъекты, которые относятся к категории служащих. В настоящее время согласно Федеральному закону от 27 мая 2003 г. N 58-ФЗ «О системе государственной службы Российской Федерации», к государственным служащим относятся только лица, занимающие го-

сударственные должности Российской федерации и ее субъектов (законодательной, исполнительной и судебной власти).

Известно большое количество научных работ, посвященных коммерческой тайне, где предпринимаются попытки дать четкое и однозначное определение этому предмету информационных правоотношений. Авторы согласны в том, что коммерческая тайна может только тогда считаться таковой, когда собственник устанавливает для нее особый режим допуска (зафиксированный в локальных нормативных актах предприятия) и принимает организационные меры для соблюдения этого режима допуска. Если собственник таких мер не предпринимает, информация должна считаться общедоступной. Однако спорным остается вопрос о разграничении коммерческой тайны и интеллектуальной собственности (последняя должна охраняться законом независимо от режима обращения с ней).

Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами (например, постановлением Правительства Российской Федерации № 35 «О перечне сведений, которые не могут составлять коммерческую тайну» от 5 декабря 1991 г.)

Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» относит к таковой «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации». Названный закон устанавливает перечень сведений, составляющих государственную тайну, порядок отнесения сведений к государственной тайне. Отметим, что безопасность, согласно закону РФ от 5 марта 1992 г. № 2446-I «О безопасности», это «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».

Анализ различных видов тайн позволяет прийти к неожиданным выводам. В частности, оказывается, что одни и те же сведения могут по-разному классифицироваться в зависимости от субъектов, носителей этих сведений. Например, информация, которая имеет режим коммерческой тайны, может стать на законных основаниях известной работникам Министерства РФ по налогам и сборам и перейти в статус служебной тайны. Информация, составляющая тайну частной жизни гражданина, может стать известной его врачу или адвокату и перейти в разряд профессиональной тайны.

Это свидетельствует о целесообразности подготовки единого кодификационного акта, в котором необходимо провести классификацию всех существующих на сегодняшний день видов тайн и установить их правовой режим. Это позволит исключить возможную путаницу при решении вопросов, связанных с институтом тайны.

Глава 3. Уголовно-правовая характеристика преступлений в сфере компьютерной информации

3.1. Объективные признаки преступлений главы 28 УК РФ

Объективная сторона преступления, предусмотренного ст.272 УК РФ, выражается в неправомерном доступе к охраняемой законом компьютерной информации.

Законодатель не уточняет понятие неправомерности доступа, но оно вытекает из смысла понятия «охраняемая законом компьютерная информация», проанализированного нами выше. Неправомерность доступа означает, что лицо не имело право вызывать информацию, знакомиться с ней и распоряжаться ею. Способы неправомерного доступа к охраняемой законом компьютерной информации могут быть самыми разнообразными и, как правило, не влияют на юридическую оценку поведения виновного.

Неправомерный доступ к компьютерной информации общего пользования, то есть неохраняемой законом информации, адресованной неограниченно широкому кругу лиц, не образует признаков рассматриваемого преступления. Из-за этого возникают частные ошибки при квалификации незаконного подключения к сети Интернет. Так, З. осуществил незаконное проникновение в компьютерную сеть Интернет с использованием сервера фирмы «Эликом» под именем и паролем фирмы «Микст» и произвел копирование файлов, на основании чего следователем было обоснованно возбуждено уголовное дело по ч.1 ст. 272. В процессе расследования в действиях З. не было установлено признаков состава преступления, поскольку информация, содержащаяся в незащищенных файлах компьютерной сети Интернет, доступ к которой осуществил З., не охраняется законом. В связи с этим производство по данному делу было прекращено. Следователем не была до конца отработана версия о неправомерном доступе к охраняемой законом компьютерной информации, находящейся на сервере фирмы «Эликом» (списки зарегистрированных пользователей, получающих доступ через этот сервер, и их пароли) [4].

Отметим, что из всех статей 28-й главы, статья 272 вызывает наименьшие затруднения при толковании. Именно поэтому, на наш взгляд, число зарегистрированных по этой статье преступлений на порядок превосходит число преступлений, зарегистрированных по ст. 273 и на два порядка — по ст. 274 (см. выше). По этой же причине неправомерный доступ к компьютерной информации наиболее полно проанализирован в литературе, в частности, криминалистической.

Преступление, предусмотренное ст. 273 УК РФ, предусматривает совершение хотя бы одного из следующих действий: создание вредоносных программ для ЭВМ; внесение изменений в существующие программы для ЭВМ; использование или распространение вредоносных программ для ЭВМ. Совершить названное преступление путем бездействия невозможно. Рассмотрим названные действия более подробно.

1. Создание вредоносных программ для ЭВМ. Для наступления уголовной ответственности данная программа должна являться вредоносной. Законодательной дефиниции вредоносной программы не существует, что, несомненно, приводит к субъективизму в правоприменительной практике. Единственная попытка дать такое определение встречается нами в Соглашении о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации

(Минск, 1 июня 2001 г.), однако данный документ в настоящее время прекратил действие и юридической силы не имеет. В этом документе вредоносная программа определялась как «созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети». Как видно, определение неудачно, поскольку оно буквально повторяет текст ст. 273, не раскрывая его сути, а, кроме того, толкует понятие вредоносной программы расширительно. Под него попадает любая программа, ошибка в которой (или неправильное пользование ею) может привести к названным последствиям. Между тем, по эмпирическим данным, любая программа содержит не менее 5 ошибок на 1000 строк кода и если устанавливать ответственность за эти ошибки, индустрия программного обеспечения моментально рухнет.

Нам кажется более уместным одно из определений, предлагаемых в научной литературе. «Вредоносной программой является специально написанная (созданная) программа, которая, получив управление, способна совершать несанкционированные пользователем действия и вследствие этого причинять вред собственнику или владельцу информации, а также иным лицам в виде уничтожения, блокирования модификации или копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети» [10].

В других источниках приводится важное уточнение. Вредоносность или полезность соответствующих программ для ЭВМ определяется не в зависимости от их назначения, способности уничтожать, модифицировать, копировать информацию (это вполне типичные функции вполне легальных программ), а в связи с тем, предполагает ли их действие, во-первых, предварительное уведомление собственника компьютерной информации или другого законного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает программу вредоносной.

Многие юристы ошибочно отождествляют понятия вредоносной программы и компьютерного вируса. Однако многообразие вредоносных программ ими не ограничивается. Помимо вирусов к категории вредоносных программ относятся, например «троянские кони» и «логические бомбы». Логическая бомба — это умышленное изменение кода программы, частично или полностью выводящее из строя программу либо систему ЭВМ при определенных заранее условиях, например наступления определенного времени.

Хрестоматийным является случай, произошедший в 1983 г. На Волжском автомобильном заводе был изобличен программист, из мести к руководству предприятия умышленно внесший изменения в программу ЭВМ, управлявшую подачей деталей на конвейер. В результате произошедшего сбоя заводу был причинен существенный материальный ущерб: не сошло с конвейера свыше сотни автомобилей. Программист был привлечен к уголовной ответственности, обвинялся по ч. 2 ст. 98 УК РСФСР «Умышленное уничтожение или повреждение государственного или общественного имущества ... причинившее крупный ущерб». При этом обвиняемый утверждал, что ничего натурально повреждено не было — нарушенным оказался лишь порядок работы, т.е. действия, не подпадающие ни под одну статью действующего в то время законодательства. С научной точки зрения интересен приговор суда: «три года лишения свободы условно; взыскание суммы, выплаченной рабочим за время вынужденного простоя главного конвейера; перевод на долж-

ность сборщика главного конвейера» [4]. В настоящее время квалификация действий программиста должна была бы производиться по ч.1 ст.273 УК РФ.

Таким образом, смешение таких понятий как «вредоносная» и «вирусная» программа ведет к неоправданному сужению признаков объективной стороны рассматриваемого преступления, что создает возможность для безнаказанности за создание, использование и распространение вредоносных программ для ЭВМ, не являющихся по своим качественным характеристикам вирусными.

В литературе нет однозначного мнения по поводу того, следует ли считать вредоносными программами так называемые «крэки», назначение которых — снятие защиты с программных продуктов. Написание и использование такой программы, несомненно, наносит вред владельцу авторских прав на защищенный программный продукт, однако критериям, названным выше, она не удовлетворяет. Кроме того, формально применение «крэка» не влечет последствий, предусмотренных статьей 273. Поэтому «крэки» (а равно, например, программы автоматического подбора паролей и т.п.) предлагается считать лишь средством совершения преступлений, предусмотренных статьями 272 или 146 УК РФ, а их написание — подготовкой к совершению названных преступлений.

Однако в судебной практике немало противоположных случаев. Так, 6 отделом УРОПД при ГУВД Санкт-Петербурга и области 2 сентября 1998 г. было возбуждено уголовное дело по признакам преступления, предусмотренного ст. 273 УК РФ по факту распространения компакт-дисков с программами, предназначенными для снятия защиты с программных продуктов, а также «взломанных» версий программ. «Крэки» были признаны следствием вредоносными программами. Аналогичная позиция отстаивалась и по делу, возбужденному 10 марта 1998 года следственным управлением ГУВД Свердловской области по факту создания электронной доски объявлений, в одном из разделов которой находилась подборка крэков.

2. Внесение изменений в существующие программы — это несанкционированная законным пользователем или собственником программы ее модификация (переработка программы путем изменения, добавления или удаления ее отдельных фрагментов) до такого состояния, когда эта программа способна выполнить новые, изначально незапланированные функции и приводить к последствиям, предусмотренным ч. 1 ст. 273 УК РФ.

3. Под *использованием* программы (согласно ст. 1270 ГК РФ) понимается ее распространение, воспроизведение (под которым также понимается запись на электронный носитель или в память ЭВМ, т.е. собственно запуск программы), передача по сети, а также доведение до всеобщего сведения (например, путем открытия доступа к каталогу собственного компьютера, содержащего эту программу).

4. Распространение программы для ЭВМ — это предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей. Распространение вредоносных программ может осуществляться непосредственно путем их копирования на компьютер потерпевшего, например, с дискеты, а также опосредовано, путем передачи по электронной почте, по линии связи законного пользователя через компьютерную сеть.

Отметим, что уголовная ответственность по этой статье возникает в результате создания программы независимо от того, использовалась программа или нет. По смыслу ст.

273 УК наличие исходных текстов вирусных программ уже является основанием для привлечения к ответственности. Однако следует учитывать, что в ряде случаев использование подобных программ не должно являться уголовно наказуемым. Это относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих соответствующую лицензию. Также очевидно, что собственник информационного ресурса вправе в необходимых случаях (например, исследовательские работы по созданию антивирусных средств) использовать вредоносные программы. К сожалению, эти очевидные исключения прямо не оговорены в законодательстве.

Статья 274 УК РФ устанавливает уголовную ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети. Эта статья имеет целью предупреждение невыполнения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой информации.

Выше мы отмечали, что число преступлений, зарегистрированных по ст. 274 УК РФ непропорционально мало по сравнению с другими преступлениями 28-й главы, что, по мнению некоторых авторов, свидетельствует о недостаточной работе правоохранительных органов. Недостаточно разработана и уголовно-правовая характеристика рассматриваемого преступления. Закон не дает определения нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, диспозиция ст. 274 носит бланкетный (отсылочный) характер.

Под такими правилами понимаются, во-первых, гигиенические требования к технике и организации работы, во-вторых, техническая документация на приобретаемые компьютеры, в-третьих, конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие поведению до сведения соответствующих работников правила внутреннего распорядка, в-четвертых, требования по сертификации компьютерных сетей и оборудования, в-пятых, должностные инструкции конкретных сотрудников, в-шестых, правила пользования компьютерными сетями. В частности, порядок сертификации средств защиты информации в РФ устанавливается Положением о сертификации средств защиты информации, утвержденным постановлением Правительства РФ от 26 июня 1995 г. № 608.

Нарушения правил эксплуатации ЭВМ подразделяются на *физические* (неправильное подключение периферийного оборудования, отсутствие устройств бесперебойного питания, нарушение теплового режима в помещении, неправильное подключение ЭВМ к источникам питания, нерегулярное техническое обслуживание, использование несертифицированных средств защиты и самодельных узлов и приборов и пр.) и *интеллектуальные* (невыполнение процедуры резервного копирования, несанкционированная замена программного обеспечения, параметров настройки системы ЭВМ или компьютерной сети и пр.). К интеллектуальным нарушениям можно отнести и пренебрежение организационными мерами защиты компьютерной информации (предоставление посторонним лицам доступа в служебное помещение, несанкционированное разглашение сетевого имени и пароля законного пользователя и пр.).

Заметим, что из текста ст. 274 УК РФ за нарушение правил обращения с машинными носителями информации привлечь лицо к уголовной ответственности нельзя, что, конечно, является серьезным недостатком закона.

Ведется полемика о том, будет ли наступать уголовная ответственность за нарушение правил пользования глобальными сетями, например сетью Интернет. Сеть Интернет представляет собой глобальное объединение компьютерных сетей и информационных ресурсов, принадлежащих множеству различных людей и организаций. Это объединение является децентрализованным, и единого общеобязательного свода правил (законов) пользования сетью Интернет не установлено.

В учебном пособии под редакцией Гаврилова отстаивается та точка зрения, что существуют общепринятые нормы работы в сети Интернет, направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей и за нарушение таких норм должна наступать уголовная ответственность по ст. 274 УК РФ. Фундаментальное положение этих норм таково: правила использования любых ресурсов сети Интернет (от почтового ящика до канала связи) определяют владельцы этих ресурсов, и только они. Однако примеры, которые приводятся в пособии и которые, по мнению авторов, могут составлять объективную сторону анализируемого преступления (массовая рассылка рекламы (спам), оффтопик, фальсификация своего IP-адреса при выходе в сеть и т.п.) являются, на наш взгляд, неудачными, поскольку не могут повлечь предусмотренные ст. 274 УК РФ последствия. Наша точка зрения косвенно подтверждается тем, что в судебной практике отсутствуют случаи привлечения лица к уголовной ответственности за нарушение неписаных общепринятых норм работы в Интернет.

Состав всех трех преступлений 28-й главы УК РФ конструктивно сформулирован как материальный. Обязательными признаками их объективной стороны являются не только общественно опасные действия, но и наступление общественно опасных последствий, а также причинная связь между этими двумя признаками.

Общественно опасные последствия всех трех преступлений выражаются в виде уничтожения, блокирования, модификации либо копирования информации, а также нарушения работы ЭВМ, системы ЭВМ или их сети.

В законе содержание указанных понятий не раскрывается, поэтому авторы, анализирующие состав данного преступления, вынуждены давать собственные определения. В одном из последних комментариев к УК РФ предлагаются следующие. *Уничтожение информации* заключается в удалении ее с носителя. *Блокирование* — это создание препятствий правомерному доступу к ней. *Модификация* информации предполагает любое ее изменение. *Копирование* — воспроизведение указанной информации на другом носителе. При этом не имеет значения, воспроизводится ли она с помощью технических средств либо вручную. *Нарушение работы ЭВМ, их систем или сети* означает, что они в результате этого не могут выполнять свои функции, выполнять их на должном уровне, когда значительно уменьшается их производительность.

Таким образом, статьи 28-й главы обеспечивают защиту всех трех свойств компьютерной информации, которые рассматривались во второй главе дипломного проекта: конфиденциальности (копирование), целостности (уничтожение, модификация) и доступности (блокирование). Нарушение работы ЭВМ, системы ЭВМ или их сети может привести к потере любого из этих свойств в зависимости от характера такого нарушения.

Но, на наш взгляд, законодатель допустил ошибку, не воспользовавшись достижениями науки информационной безопасности и явно не назвав указанные свойства, нарушение которых является первичным последствием компьютерных преступлений. Вместо

этого законодатель использовал перечисление последствий, вторичных по своей природе, причем сделал это перечисление исчерпывающим. Это неотвратимо ведет к сужению области действия законодательства.

Наиболее яркое подтверждение тому — дискуссия, которая ведется вокруг ст. 272 УК РФ. Дело в том, что из буквального текста законодательства следует, что сам по себе факт вызова или просмотра компьютерной информации, хранящейся на машинном носителе, состава анализируемого преступления не образует. К этому выводу приходят многие авторы, утверждая, что «необходимо по крайней мере установить факт переноса указанной информации на другой машинный носитель» [4]. Нет, например, оснований привлекать к уголовной ответственности по ст. 272 УК лицо, которое с помощью подбора пароля обошло систему защиты межбанковской компьютерной сети и, получив доступ к информации о счетах клиентов, из любопытства (или из преступных намерений) ознакомилось с ними.

Конечно, во многих случаях ознакомления (чтения) информации в результате неправомерного доступа, можно «притянуть за уши» копирование, опираясь на то, что данные, прежде чем быть выведенными на экран, должны попасть с машинного носителя в оперативную память компьютера (т.е. создается временная копия указанных данных). Однако такой подход очевидно слаб (тем более, что данные могли по каким-то причинам уже находиться в памяти в результате действий управомоченного пользователя).

Отметим, что необходимым признаком объективной стороны компьютерных преступлений является причинная связь между противозаконными действиями виновного и наступившими вредными последствиями.

Действующее уголовное законодательство не выделяет квалифицированные составы преступлений по признаку использования электронной техники. Поэтому в тех случаях, когда неправомерный доступ к компьютерной информации выступает способом совершения другого умышленного преступления, а электронно-вычислительная техника используется в качестве орудия для достижения преступной цели, содеянное виновным квалифицируется по совокупности преступлений.

Примером подобного преступления может являться следующее. К., являясь оператором ЭВМ в одной из организаций, на своем личном компьютере изготовил электронное почтовое сообщение с рекламой товаров народного потребления, приложив к нему в качестве подробного каталога с ценами и условиями поставки составленную им лично вредоносную программу для ЭВМ в виде файла katalog.exe, и распространил ее согласно имеющемуся у него списку электронных почтовых адресов пользователей сети Интернет 350 адресатам. В результате массового распространения этой вредоносной программы после ее запуска пользователями сети Интернет, К. несанкционированно получил по своему электронному адресу 87 учетных имен и паролей для доступа в сеть Интернет, которые скопировал на жесткий диск своего компьютера и в дальнейшем использовал для доступа в сеть Интернет [4].

В приведенном примере налицо несколько составов преступлений. Во-первых, создание, использование и распространение вредоносных программ для ЭВМ (ч. 1 ст. 273 УК РФ). Во-вторых, мошенничество, то есть хищение чужого имущества, совершенное путем обмана, (п. «б» ч. 2 с. 159 УК РФ). В-третьих, К. совершил неправомерный доступ к охраняемой законом компьютерной информации (учетные данные пользователей), повлекший

ее блокирование (поскольку, в период работы К. законные пользователи не могли получить доступ к системе), то есть преступление, ответственность за которое предусмотрена ч. 1 ст. 272 УК РФ.

Наиболее часто компьютерные преступления выступают в качестве способа совершения следующих умышленных преступлений: воспрепятствование осуществлению избирательных прав граждан или работе избирательных комиссий (ст. 141 УК РФ); фальсификация избирательных документов, документов референдума или неправильный подсчет голосов (ст. 142 УК РФ); мошенничество (ст. 159 УК РФ); причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ); незаконное получение сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ); диверсия (ст. 281 УК РФ) и др.

Интересно то, что квалифицированные составы преступлений 28-й главы несколько различаются. Ч.2 ст. 272 устанавливает повышенную уголовную ответственность за неправомерный доступ к компьютерной информации, совершенный группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети. Ч.2 ст. 273 и ч.2 ст. 274 в качестве квалифицирующего признака называют повлекшие по неосторожности тяжкие последствия. (Эта формулировка вызывает законный вопрос у многих авторов — а как же быть, если тяжкие последствия охватываются умыслом преступника?)

Под тяжкими последствиями понимаются выход из строя важных технических средств (в том числе оборонного значения, авианавигационной техники), повлекшие аварии, катастрофы, гибель людей, а также безвозвратная утрата особо ценной информации. В последнем случае понятие тяжких последствий является оценочным и определение объема причиненного вреда должно осуществляться с учетом совокупности всех полученных данных.

Подводя итоги, следует подчеркнуть, что совершенствование уголовного законодательства в сфере компьютерной информации, устранение многих белых пятен в нем, может быть достигнуто путем законодательного определения свойств конфиденциальности, целостности и доступности информации и установления их нарушения в качестве последствий рассматриваемых общественно опасных деяний.

3.2. Субъективные признаки преступлений в сфере компьютерной информации

Субъективная сторона компьютерных преступлений в настоящее время остается предметом полемики различных авторов. Это связано с тем, что прямых указаний на этот счет в Уголовном кодексе не содержится.

Согласно одной точке зрения можно говорить об умышленной форме вины в виде прямого или косвенного умысла. Другая точка зрения состоит в том, что преступления, предусмотренные ст. 272 и 273 УК РФ могут быть совершены только с прямым умыслом. Одним из аргументов является использование слова «заведомо» в формулировке ст. 273: «…создание программ для ЭВМ…, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации…».

Мы склоняемся к первой точке зрения. На практике преступник не всегда желает наступления вредных последствий, что особенно это характерно при совершении данного

преступления из озорства, или так называемого «спортивного интереса». В учебном пособии под редакцией Гаврилова в качестве примера приводятся действия лица, осуществляющего распространение CD-дисков с вредоносными программами, достоверно знающего о вредоносных последствиях такой программы (хотя бы по этикетке компакт-диска), но вместе с тем безразлично к ним относящегося. Очевидно, что целью такого лица является не наступление общественно опасных последствий, а получение прибыли за счет продажи дисков.

Таким образом, интеллектуальный момент вины, характерный для состава анализируемых преступлений, заключается в осознании виновным факта осуществления неправомерного доступа к охраняемой законом компьютерной информации, создания, распространения или использования вредоносных программ для ЭВМ либо нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети. При этом виновный понимает не только фактическую сущность своего поведения, но и его социально-опасный характер. Кроме того, виновный предвидит возможность или неизбежность реального наступления общественно опасных последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Следовательно, субъект представляет характер вредных последствий, осознает их социальную значимость и причинно-следственную зависимость. Волевой момент вины отражает либо желание (стремление) или сознательное допущение наступления указанных вредных последствий, либо, как минимум, безразличное к ним отношение.

В любом случае для квалификации действий как использования вредоносных программ необходимо доказать, что лицо заведомо знало о свойствах используемой программы и последствиях ее применения. Заметим, что в процессе создания программы могут проявиться случайные результаты, возникшие, например, в из-за ошибок разработчика, которые могут привести к указанным в ст. 273 последствиям. При этом подобный результат будет неожиданностью для самого разработчика (как в случае со знаменитым «червем» Морриса). По российскому законодательству, в подобных ситуациях лицо не будет нести уголовную ответственность, поскольку указанные последствия не охватываются его умыслом.

Открытым остается вопрос о том, должно ли лицо, осуществляющее неправомерный доступ к охраняемой законом компьютерной информации, осознавать факт неправомерности этого доступа.

Что касается ст. 274 УК РФ, то, поскольку субъектом соответствующего преступления является должностное лицо, априорно предполагается, что это лицо ознакомлено со всеми необходимыми должностными инструкциями и, нарушая правила эксплуатации ЭВМ, системы ЭВМ или их сети, не может впоследствии ссылаться на незнание этих правил.

В некоторых работах встречается суждение о том, что компьютерные преступления могут совершаться и по неосторожности. Мы считаем эту точку зрения ошибочной. Любое из преступлений, предусмотренных статьями 28-й главы, совершенное по неосторожности, исключает правовое основание для привлечения лица к уголовной ответственности, т.к., согласно ч.2 ст.24 УК, «деяние, совершенное по неосторожности, признается преступлением только в том случае, когда это специально предусмотрено соответствующей

статьей Особенной части настоящего Кодекса». О неосторожности в диспозиции ст. 272—274 УК РФ не сказано, следовательно, деяние может быть совершено лишь умышленно.

Преступления, предусмотренные ч. 2 ст. 273 и ч.2 ст. 274, совершаются с двойной формой вины: умышленной (в виде прямого или косвенного умысла) по отношению к созданию, использованию и распространению вредоносных программ либо нарушению правил эксплуатации ЭВМ, их системы или сети, и неосторожной по отношению к наступившим тяжким последствиям. То есть, причинение тяжких последствий не охватывается умыслом виновного, однако он предвидит возможность их наступления, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение, либо не предвидит, хотя должен был и мог предвидеть возможность наступления тяжких последствий.

Мотивы и цели компьютерных преступлений имеют факультативное значение для квалификации преступлений и были подробно нами проанализированы в первой главе настоящей работы.

Согласно ст. 20 УК РФ, субъектом преступлений, предусмотренных ч.1 ст. 272 и ст. 273 УК РФ может быть любое физическое лицо, достигшее к моменту преступной деятельности шестнадцатилетнего возраста. Обязательным условием привлечения лица к уголовной ответственности является вменяемость (ст. 21 УК РФ).

В двух последних квалифицированных составах преступления, перечисленных в ч. 2 ст. 272 РФ, а также в составе преступления, предусмотренного ст. 274 УК РФ имеется специальный субъект — лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети. К таким лицам следует относить законных пользователей информации (операторов ЭВМ, программистов, абонентов системы ЭВМ), а также лиц, по характеру своей деятельности имеющих доступ к ЭВМ, системе ЭВМ или их сети (наладчиков оборудования, иной технический персонал, обслуживающий ЭВМ).

При этом необходимо подчеркнуть, что признание лица специальным субъектом преступления обусловлено не его особым положением (это бы противоречило принципу равенства граждан перед законом — ст. 4 УК РФ), а тем обстоятельством, что лицо именно вследствие занимаемого положения способно совершить такое преступление.

Абсолютное большинство лиц, совершающих неправомерный доступ к охраняемой законом компьютерной информации (до 70%) как раз и будет приходиться на долю указанной законодателем категории лиц. Использование своего служебного положения предполагает доступ к охраняемой законом компьютерной информации благодаря занимаемому виновным положению по службе. При этом действия лица хотя и находятся в пределах его служебной компетенции, но совершаются с явным нарушением порядка осуществления своих функциональных обязанностей, установленных законом или иным нормативным актом.

На субъект преступления, предусмотренного ст. 274 УК РФ, законом или иным нормативным актом возложена обязанность соблюдения правил эксплуатации ЭВМ в силу характера выполняемой трудовой, профессиональной или иной деятельности.

В литературе до сих пор ведется полемика, следует ли считать квалифицированным субъектом лицо, имеющее законный доступ к сети Интернет. Понятие «сети ЭВМ», как отмечалось выше, законодательно не сформулировано и формально Интернет может попадать под эту категорию. Авторы, придерживающиеся другой точки зрения (например, А.Б. Нехорошев), замечают, что возможность законного доступа в Интернет в настоящее

время есть практически у каждого пользователя, и рассмотрение его в качестве сети ЭВМ, названной в п.2 ст.272 УК приводит к неосновательному расширению квалифицирующего состава преступления.

Литература

1. Нехорошев А.Б. Компьютерные преступления: квалификация, расследование, экспертиза. Часть 1 / Под ред. В.Н.Черкасова — Саратов: СЮИ МВД России, 2003.
2. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография — М.: Норма, 2004.
3. Петрова С.С. Криминология: Учеб. Пособие. — М.: Издательство РИОР, 2005.
4. Преступления в сфере компьютерной информации: квалификация и доказывание: Учеб. пособие / Под ред. Ю.В. Гаврилина. — М.: ЮИ МВД РФ, 2003.
5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия. / Под ред. Б.П. Смагоринского. М.: 1996.
6. Бытко Ю.И., Бытко С.Ю. Уголовное право России. Части Общая и Особенная. Учебник. — Саратов: Изд-во «Научная книга», 2005.
7. Уголовное право. Особенная часть: Учебник / Под ред. проф Л.Д. Гаухмана и проф. С.В. Максимова. — М.: Изд-во Эксмо, 2004.
8. Крылов В.В. Информационные компьютерные преступления: Учебное и практическое пособие. — М.: ИНФРА-М-НОРМА, 1997
9. Смирнова С.А. Судебная экспертиза на рубеже XXI века. Состояние, развитие, проблемы. 2-е издание, переработанное и дополненное. — СПб.: Питер, 2004
10. Ляпунов Ю.И., Пушкин А.В. Преступления в сфере компьютерной информации // Уголовное право. Особенная часть / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. М., 1998.