Технические методы защиты информации

Практическая криптография

Аппаратные ключи против пиратства

Привязка к носителям информации

Обеспечение секретности данных

Управление цифровыми правами

Инструментарий исследователя

ДМИТРИЙ СКЛЯРОВ

ОН ПОКАЗАЛ НЕЭФФЕКТИВНОСТЬ ЗАЩИТЫ ЭЛЕКТРОННЫХ КНИГ ADOBE

ИСКУССТВО ЗАЩИТЫ И ВЗЛОМА ИНФОРМАЦИИ

bhv

ДМИТРИЙ
СКЛЯРОВ

ИСКУССТВО ЗАЩИТЫ И ВЗЛОМА ИНФОРМАЦИИ

Санкт-Петербург
«БХВ-Петербург»
2004

УДК 681.3.06
ББК 32.973.26-018.2
С43

Скляров Д. В.

С43 Искусство защиты и взлома информации. — СПб.: БХВ-Петербург, 2004. — 288 с.: ил.

ISBN 5-94157-331-6

Защита информации — очень сложная наука, но начинать ее изучение можно с простых вещей. Именно так и задумана эта книга. Читателю предстоит узнать, чем занимается информационная безопасность и какие методы она использует для решения своих задач. Особое внимание уделяется криптографии — пожалуй, самому мощному инструменту защиты. Подробно рассматриваются вопросы защиты программ от несанкционированного тиражирования, а также различные аспекты обеспечения безопасности данных, включая управление цифровыми правами и применение стеганографии. Изложение материала сопровождается примерами неудачных средств защиты и объяснением причин их появления. Рассказывается также об анализе средств защиты, целях, которые ставятся при проведении анализа, и инструментах, применяемых при исследовании.

Для широкого круга пользователей,
интересующихся вопросами защиты информации

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зав. редакцией	*Григорий Добин*
Редактор	*Нина Седых*
Компьютерная верстка	*Натальи Караваевой*
Корректор	*Виктория Пиотровская*
Дизайн обложки	*Инна Тачина*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 26.12.03.
Формат 70×100 $^{1}/_{16}$. Печать офсетная. Усл. печ. л. 23,2.
Тираж 3 000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Гигиеническое заключение на продукцию, товар № 77.99.02.953.Д.001537.03.02
от 13.03.2002 г. выдано Департаментом ГСЭН Минздрава России.

Отпечатано с готовых диапозитивов
в Академической типографии "Наука" РАН
199034, Санкт-Петербург, 9 линия, 12.

ISBN 5-94157-331-6

Содержание

Посвящается

Оксане, Егору и Полине
Саше Каталову
Лене Павловской и Сереже Осокину
Маше Ручке и Игорю Баздыреву
Марине Портновой и Леониду Агранонику
Джеку Палладино (Jack Palladino)
Эдмунду Хинцу (Edmund Hintz)
Полу Хольману (Paul Holman)

И многим другим,
чья поддержка и помощь
помогли выжить и победить.

Введение

Большинство книг по защите информации содержит в себе стройный набор правил, беспрекословное выполнение которых, по идее, должно обеспечить необходимый уровень защиты. Однако, как показывает практика, точное следование правилам далеко не всегда приводит к желаемому результату. Этому есть несколько причин.

Во-первых, все математически строгие доказательства строятся на моделях, которые трудно применимы на практике из-за чрезмерной жесткости накладываемых ограничений. Так, например, легко доказать, что одноразовый блокнот является абсолютно стойким шифром, но при его использовании размер ключа должен быть не меньше размера шифруемых данных и ключ не должен использоваться дважды. На подобные условия согласятся разве что дипломаты, военные или спецслужбы, а для массового использования такой алгоритм не пригоден.

Во-вторых, реальный мир гораздо разнообразней, чем его описывают в книгах, и всегда может возникнуть ситуация, которая не только никому не встречалась на практике, но и даже не приходила в голову. Следовательно, не может быть и полных формальных правил поведения в такой ситуации.

А в-третьих, людям свойственно ошибаться. И программист, реализующий правила безопасности, тоже не застрахован от ошибок. Для обычных программ работоспособность обычно подтверждается путем выполнения серии тестов, проверяющих все основные режимы. Но если программа имеет дело с безопасностью, все обстоит иначе. Адекватное (обеспечивающее должный уровень защиты) поведение программы на всех тестах не гарантирует отсутствия "дыры" в одном из режимов, который не был протестирован. Для получения подобных гарантий требуется выполнить тестирование во всех возможных режимах, что практически нереализуемо.

В этой книге нет универсальных рекомендаций по построению надежных средств защиты, как нет и подробного описания техник, применяемых для

взлома. Внимание читателя направляется на то, какие ошибки чаще всего допускаются в процессе разработки средств защиты, и приводятся примеры реальных систем, которые были взломаны из-за таких ошибок.

Первая, вводная часть книги призвана дать читателю общее понимание задач информационной безопасности и проблем, возникающих при решении этих задач.

Вторая часть, в основном, посвящена криптографии, т. к. криптография является очень мощным инструментом, без которого построение большинства систем защиты было бы просто невозможно.

В третьей части рассматриваются вопросы защиты программ от несанкционированного тиражирования. Приводятся описания наиболее распространенных приемов защиты, и объясняется, почему эти приемы не всегда работают.

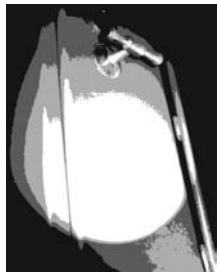
Четвертая часть рассказывает о защите данных. В числе прочих рассматриваются вопросы реализации систем управления цифровыми правами. Дается анализ основных причин, приводящих к появлению ненадежных средств защиты.

В пятой, заключительной части собрана информация о том, как и для чего проводятся исследования программных средств защиты информации. Разработчикам защит полезно знать, какие средства есть в распоряжении противника, чтобы максимально осложнить его работу.

Часть I

КОМУ НУЖНА ЗАЩИТА?

Эта часть вводная. Вряд ли она будет очень интересна профессионалам в области защиты информации, т. к. призвана донести до читателя основные понятия и терминологию предметной области, а также общее представление о том, что может и чего не может информационная безопасность. Однако, наверняка, даже хорошо знакомые с данной темой люди смогут найти для себя в этой части что-то новое.



Глава 1

Общие сведения о защите информации

Перед тем как начинать рассмотрение вопросов защиты информации, стоит более или менее формально определить, что скрывается за терминами "информационная безопасность" и "защита информации". Прежде всего, оба этих словосочетания являются переводом на русский язык английского термина "information security". Словосочетание "информационная безопасность" имеет скорее научный, теоретический окрас, а "защита информации" обычно используется при описании практических мероприятий. Однако, в целом, они являются синонимами, и в книге между ними не будет делаться каких-либо различий.

Мы будем оперировать термином "информация" в максимально широком его понимании. *Информацией* являются любые данные, находящиеся в памяти вычислительной системы, любое сообщение, пересылаемое по сети, и любой файл, хранящийся на каком-либо носителе. Информацией является любой результат работы человеческого разума: идея, технология, программа, различные данные (медицинские, статистические, финансовые), независимо от формы их представления. Все, что не является физическим предметом и может быть использовано человеком, описывается одним словом — информация.

1.1. Что и от чего защищать

До начала рассмотрения различных аспектов защиты информации необходимо выяснить, что и от кого предполагается защищать. Без этого рассуждать о преимуществах и недостатках систем информационной безопасности просто бессмысленно.

1.1.1. Характеристики информации

Прежде всего, у каждой "единицы" защищаемой информации есть несколько параметров, которые необходимо учитывать:

- статичность;
- размер и тип доступа;

- ❒ время жизни;
- ❒ стоимость создания;
- ❒ стоимость потери конфиденциальности;
- ❒ стоимость скрытого нарушения целостности;
- ❒ стоимость утраты.

Статичность определяет, может ли защищаемая информация изменяться в процессе нормального использования. Так, например, передаваемое по сети зашифрованное сообщение и документ с цифровой подписью изменяться не должны, а данные на зашифрованном диске, находящемся в использовании, изменяются постоянно. Также изменяется содержимое базы данных при добавлении новых или модификации существующих записей.

Размер единицы защищаемой информации может накладывать дополнительные ограничения на используемые средства защиты. Так блочные алгоритмы шифрования в некоторых режимах оперируют порциями данных фиксированной длины, а использование асимметричных криптографических алгоритмов приводит к увеличению размера данных при зашифровании *(см. гл. 5)*. *Тип доступа* (последовательный или произвольный) также накладывает ограничения на средства защиты — использование потокового алгоритма шифрования для больших объемов данных с произвольным доступом требует разбиения данных на блоки и генерации уникального ключа для каждого из них.

Время жизни информации — очень важный параметр, определяющий, насколько долго информация должна оставаться защищенной. Существует информация, время жизни которой составляет минуты, например отданный приказ о начале атаки или отступления во время ведения боевых действий. Содержимое приказа и без расшифровки сообщения станет ясно противнику по косвенным признакам. Время жизни большей части персональной информации (банковской, медицинской и т. п.) соответствует времени жизни владельца — после его смерти разглашение такой информации уже никому не принесет ни вреда, ни выгоды. Для каждого государственного секрета, как правило, тоже определен период, в течение которого информация не должна стать публичной. Однако с некоторых документов грифы не снимаются никогда — это случай, когда время жизни информации не ограничено. Никогда не должна разглашаться информация и о ключах шифрования, вышедших из употребления, т. к. у противника могут иметься в наличии все старые зашифрованные сообщения и, получив ключ, он сможет обеспечить себе доступ к тексту сообщений.

Стоимость создания является численным выражением совокупности ресурсов (финансовых, человеческих, временны*х*), затраченных на создание информации. Фактически, это ее себестоимость.

Стоимость потери конфиденциальности выражает потенциальные убытки, которые понесет владелец информации, если к ней получат неавторизован-

ный доступ сторонние лица. Как правило, стоимость потери конфиденциальности многократно превышает себестоимость информации. По истечении времени жизни информации стоимость потери ее конфиденциальности становится равной нулю.

Стоимость скрытого нарушения целостности выражает убытки, которые могут возникнуть вследствие внесения изменений в информацию, если факт модификации не был обнаружен. Нарушения целостности могут носить различный характер. Они могут быть как случайными, так и преднамеренными. Модификации может подвергаться не только непосредственно текст сообщения или документа, но также дата отправки или имя автора.

Стоимость утраты описывает ущерб от полного или частичного разрушения информации. При обнаружении нарушения целостности и невозможности получить ту же информацию из другого источника информация считается утраченной.

Четыре различных стоимости, перечисленные выше, могут очень по-разному соотноситься друг с другом. Рассмотрим два примера.

Представим следующую ситуацию. Человек при помощи специализированной программы заносит информацию обо всех своих счетах и финансовых операциях в базу данных. Вследствие особенностей налоговой системы подобная практика является обычной для жителей некоторых стран. Стоимость создания подобной базы данных складывается преимущественно из времени, потраченного на ее заполнение актуальными данными. Финансовая информация, по большому счету, является конфиденциальной. Для того чтобы защитить эту информацию от потенциальных похитителей, почти все программы ведения личной финансовой истории, такие как Microsoft Money или Intuit Quicken, позволяют зашифровать базу данных и защитить ее паролем. Утечка информации крайне нежелательна, но однозначно оценить величину возможного ущерба довольно тяжело. Для кого-то потеря конфиденциальности финансовой информации пройдет бесследно, для кого-то создаст значительные трудности. Если в базу будут внесены скрытые изменения, это может привести к ошибкам в налоговой отчетности, а это, в свою очередь, чревато серьезными последствиями, вплоть до уголовного преследования. Ущерб от утраты содержимого зашифрованной базы зачастую оказывается больше ущерба от нарушения конфиденциальности вследствие попадания базы в чужие руки. В таком случае при утере пароля к базе владелец может обратиться в компанию, оказывающую услуги по восстановлению забытых паролей.

В качестве второго примера возьмем смарт-карту, в памяти которой хранится секретный ключ криптосистемы с открытым ключом, используемый как для шифрования, так и для подписи сообщений. Стоимость создания такой карты сравнительно мала. В случае потери конфиденциальности (если противнику удастся извлечь секретный ключ, получить неограниченный доступ

к самой карте или создать ее точную копию) могут наступить весьма тяжелые последствия: противник получает возможность читать все зашифрованные сообщения и подписывать сообщения от имени владельца карты. Скрытое нарушение целостности в данном случае почти не имеет смысла. Даже если противнику удастся подменить в карте секретный ключ, владелец карты не сможет не заметить, что не в состоянии расшифровать старые сообщения, а создаваемая подпись не опознается как принадлежащая ему, т. к. опубликованный открытый ключ не соответствует новому секретному ключу. То же самое произойдет и при утрате карты или ключа. Как видно, в этом случае, несмотря на невозможность повторного создания карты с тем же самым секретным ключом, утрата карты предпочтительнее потери конфиденциальности. Именно поэтому современные смарт-карты не позволяют прочитать секретный ключ стандартными средствами, а при попытке физического вмешательства во "внутренности" карты, данные просто уничтожаются.

1.1.2. Угрозы безопасности

При рассмотрении вопросов безопасности информационных систем практически все авторы выделяют три вида угроз безопасности:

- угрозы конфиденциальности информации;
- угрозы целостности информации;
- угрозы отказа в обслуживании.

Рассмотрим их подробнее.

Нарушение конфиденциальности возникает тогда, когда к какой-либо информации получает доступ лицо, не имеющее на это права. Этот вид угроз, пожалуй, наиболее часто встречается в реальном мире. Именно для уменьшения подобных угроз рекомендуется хранить в сейфах документы, содержащие секретные сведения, а при работе с такими документами вводить специальные защитные процедуры (допуски, журналы регистрации и т. п.).

Нарушение целостности происходит при внесении умышленных или неумышленных изменений в информацию. В реальном мире примером нарушения целостности может являться, например, подделка документов. Чтобы избежать этого, используются специальная бумага (с водяными знаками, голограммами и т. д.), печати и подписи. Для заверки подлинности документов существуют нотариальные службы.

Отказ в обслуживании угрожает не самой информации, а автоматизированной системе, в которой эта информация обрабатывается. При возникновении отказа в обслуживании уполномоченные пользователи системы не могут получить своевременный доступ к необходимой информации, хотя имеют на это полное право.

1.1.3. Потенциальный противник

Теперь, когда мы рассмотрели свойства информации и угрозы ее безопасности, осталось определить, кто может попытаться реализовать эти угрозы.

Очевидно, что отсутствие ключа в замке зажигания и запертая дверь не дадут угнать автомобиль первому попавшемуся прохожему. Но взломщик с набором инструментов и соответствующими навыками легко откроет дверь и заведет двигатель. От такого взломщика может спасти противоугонная система, купленная за несколько сотен долларов. Но и она, с большой вероятностью, окажется бессильной против профессионала, использующего оборудование стоимостью в десятки тысяч долларов и собирающегося угнать не первую попавшуюся, а совершенно определенную машину.

То же самое происходит и при защите информации. Некоторые методы способны обеспечить защиту от рядового пользователя, но оказываются бессильны, если атаку выполняет профессионал. А те средства защиты, которые способны остановить профессионала, не обязательно являются непреодолимым препятствием для правительственного агентства крупной мировой державы.

С правительственными агентствами связан еще один нюанс. Законодательство многих стран содержит статьи, регулирующие использование средств информационной безопасности и, в частности, криптографии. Так в течение многих лет существовали и повсеместно применялись экспортные ограничения правительства США, направленные на запрет продажи за границу программного обеспечения, использующего стойкие криптографические алгоритмы. Разрешенная длина ключа составляла 40 бит, что на момент введения ограничений позволяло защищать информацию от противника-одиночки, т. к. перебор 2^{40} комбинаций на персональном компьютере требовал нескольких десятков, если не сотен лет непрерывной работы процессора. А Агентство Национальной Безопасности США (National Security Agency, NSA) могло, используя имеющийся в наличии парк вычислительных систем, взломать 40-битовый шифр в течение нескольких дней, а то и часов. Суммарная вычислительная мощность, доступная Агентству Национальной Безопасности (АНБ), возможно, самая большая в мире. По некоторым данным, финансирование АНБ превышает суммарное финансирование ЦРУ и ФБР. И при этом про само АНБ известно крайне мало, даже существует полушутливая расшифровка аббревиатуры NSA: No Such Agency (Нет Такого Агентства).

С ростом производительности вычислительных систем 40-битовый ключ стал явно недостаточным, и производителям программного обеспечения пришлось пускаться на различные ухищрения. Так, например, в Lotus Notes для шифрования отсылаемых сообщений использовался 64-битовый ключ,

что обеспечивало высокий уровень стойкости, хотя и не являлось абсолютной защитой. Но интернациональная (экспортная) версия Lotus Notes посылала вместе с каждым сообщением 24 бита из ключа, тем самым уменьшая эффективную длину ключа до 40 бит. Эти 24 бита зашифровывались с использованием открытого ключа, принадлежащего АНБ, и помещались в так называемое *поле сокращения перебора* (Work factor Reduction Field, WRF). Для расшифровки перехваченного сообщения потенциальному противнику необходимо было выполнить перебор 2^{64} возможных ключей, в то время как АНБ могло с помощью известного только ему секретного ключа расшифровать 24 бита, переданные в поле сокращения перебора. После этого АНБ оставалось перебрать только 2^{40} вариантов ключа, что в 16 миллионов раз меньше полного перебора.

При оценке возможностей потенциального противника не стоит упускать из виду и тот факт, что технический прогресс не стоит на месте и каждый день появляются более мощные компьютеры, более эффективные технологии, а иногда и принципиально новые методы атаки. Все это необходимо учитывать при выборе средств защиты для информации с относительно большим сроком жизни.

Если 5 лет назад полный перебор всех возможных комбинаций 40-битового ключа шифрования на одном компьютере считался практически непосильной задачей, то сейчас (в 2004 году) документ в формате Microsoft Word или PDF, защищенный ключом такой длины, может быть расшифрован меньше чем за неделю. В качестве наибольшего достижения, демонстрирующего возможности современных распределенных вычислительных систем, можно назвать отыскание полным перебором 64-битового ключа алгоритма RC5, занявшее 1757 дней (почти 5 лет!) и законченное 14 июля 2002 года.

Еще одной хорошей иллюстрацией прогресса технических средств являются оценки стоимости взлома алгоритма шифрования DES (Data Encryption Standard). DES представляет собой модификацию шифра Lucifer, разработанного компанией IBM и представленного на рассмотрение правительства США в 1975 году. Внесенные в Lucifer изменения, прежде всего, коснулись длины ключа: она была сокращена со 112 до 56 бит по решению АНБ. 23 ноября 1976 года DES был утвержден в качестве федерального стандарта шифрования США и разрешен к использованию во всех несекретных правительственных каналах связи. А 15 января 1977 года было опубликовано официальное описание стандарта, вступившего в силу 6 месяцев спустя.

В статье, опубликованной в 1977 году, известные специалисты в области криптографии Уитфилд Диффи (Whitfield Diffie) и Мартин Хеллман (Martin Hellman) описали проект специализированной вычислительной машины для взлома DES. По их оценкам, она обошлась бы в 20 миллионов долларов

и была бы способна найти нужный ключ максимум за 20 часов работы. В 1981 году Диффи изменил свои оценки, увеличив стоимость до 50 миллионов долларов, а время вскрытия — до двух суток. В 1993 году Майкл Винер (Michael Wiener) спроектировал машину стоимостью 1 миллион долларов, которая должна была находить ключ максимум за 7 часов. Весной 1998 года общественная организация Electronic Frontier Foundation (EFF) продемонстрировала специализированный компьютер стоимостью 250 тысяч долларов, который за 56 часов расшифровал сообщение, зашифрованное DES. В январе 1999 года DES был взломан за 22 часа путем совместного использования 100 тысяч персональных компьютеров и машины, построенной EFF. Сейчас производительность процессоров выросла в несколько раз по сравнению с 1999 годом, и стоимость взлома DES сократилась еще сильнее. Хотя о полном переборе 2^{56} возможных ключей DES на одном персональном компьютере говорить пока не приходится.

1.2. Задачи информационной безопасности

Так с чем же имеет дело информационная безопасность? Далее следует список основных целей и задач, решение которых она должна обеспечить (в скобках приведены английские эквиваленты):

- секретность (privacy, confidentiality, secrecy);
- целостность (data integrity);
- идентификация (identification);
- аутентификация (data origin, authentication);
- уполномочивание (authorization);
- контроль доступа (access control);
- право собственности (ownership);
- сертификация (certification);
- подпись (signature);
- неотказуемость (non-repudiation);
- датирование (time stamping);
- расписка в получении (receipt);
- аннулирование (annul);
- анонимность (anonymity);
- свидетельствование (witnessing);
- подтверждение (confirmation);
- ратификация (validation).

Рассмотрим каждую из перечисленных задач подробнее.

Секретность — одна из самых востребованных задач защиты. Практически у каждого человека или организации найдутся документы, которые ни в коем случае не должны стать всеобщим достоянием, будь то личные медицинские данные, информация о финансовых операциях или государственная тайна. Пока для хранения используются неэлектронные средства (бумага, фотопленка), секретность обеспечивается административными методами (хранение в сейфах, транспортировка в сопровождении охраны и т. д.). Но когда информация обрабатывается на компьютерах и передается по открытым каналам связи, административные методы оказываются бессильны и на помощь приходят методы информационной безопасности. Задача обеспечения секретности, фактически, сводится к тому, чтобы сделать возможным хранение и передачу данных в таком виде, чтобы противник, даже получив доступ к носителю или среде передачи, не смог получить сами защищенные данные.

Целостность — еще одна очень важная задача. В процессе обработки и передачи по каналам связи данные могут быть искажены, как случайно, так и преднамеренно. Также информация может быть изменена прямо на носителе, где она хранится. Проверка целостности просто необходима в ситуациях, когда интерпретация неправильных данных может привести к очень серьезным последствиям, например при возникновении ошибки в сумме банковского перевода или значении скорости самолета, заходящего на посадку. Обеспечение целостности (контроль целостности) заключается в том, чтобы позволить либо утверждать, что данные не были модифицированы при хранении и передаче, либо определить факт искажения данных. То есть никакое изменение данных не должно пройти незамеченным.

Идентификация необходима для того, чтобы отождествить пользователя с некоторым уникальным идентификатором. После этого ответственность за все действия, при выполнении которых предъявлялся данный идентификатор, возлагается на пользователя, за которым этот идентификатор закреплен.

Аутентификация является необходимым дополнением к идентификации и предназначена для подтверждения истинности (аутентичности) пользователя, предъявившего идентификатор. Неанонимный пользователь должен получить возможность работать только после успешной аутентификации.

Уполномочивание сводится к тому, что ни один пользователь не должен получить доступ к системе без успешного выполнения идентификации и последующей аутентификации и ни один пользователь не должен получить доступ к ресурсам, если он не уполномочен на такие действия специальным разрешением.

Контроль доступа — комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам.

Доступ должны иметь только уполномоченные пользователи, и попытки доступа должны протоколироваться.

Право собственности используется для того, чтобы предоставить пользователю законное право на использование некоторого ресурса и, при желании, возможность передачи этого ресурса в собственность другому пользователю. Право собственности обычно является составной частью системы контроля доступа.

Сертификация — процесс подтверждения некоторого факта стороной, которой пользователь доверяет. Чаще всего сертификация используется для удостоверения принадлежности открытого ключа конкретному пользователю или компании, т. к. эффективное использование инфраструктуры открытых ключей возможно лишь при наличии системы сертификации. Организации, занимающиеся выдачей сертификатов, называются удостоверяющими центрами.

Подпись позволяет получателю документа доказать, что данный документ был подписан именно отправителем. При этом подпись не может быть перенесена на другой документ, отправитель не может отказаться от своей подписи, любое изменение документа приведет к нарушению подписи, и любой пользователь, при желании, может самостоятельно убедиться в подлинности подписи.

Неотказуемость — свойство схемы информационного обмена, при котором существует доказательство, которое получатель сообщения способен предъявить третьей стороне, чтобы та смогла независимо проверить, кто является отправителем сообщения. То есть отправитель сообщения не имеет возможности отказаться от авторства, т. к. существуют математические доказательства того, что никто кроме него не способен создать такое сообщение.

Расписка в получении передается от получателя к отправителю и может впоследствии быть использована отправителем для доказательства того, что переданная информация была доставлена получателю не позже определенного момента, указанного в расписке.

Датирование часто применяется совместно с подписью и позволяет зафиксировать момент подписания документа. Это может быть полезно, например, для доказательства первенства, если один документ был подписан несколькими пользователями, каждый из которых утверждает, что именно он является автором документа. Кроме этого датирование широко используется в сертификатах, которые имеют ограниченный срок действия. Если действительный сертификат был использован для подписи, а затем соответствующей службой сертифицирующего центра была проставлена метка времени, то такая подпись должна признаваться правильной и после выхода сертификата из употребления. Если же отметка времени отсутствует, то после

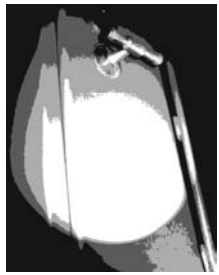
истечения срока действия сертификата подпись не может быть признана корректной.

Аннулирование используется для отмены действия сертификатов, полномочий или подписей. Если какой-либо участник информационного обмена или принадлежащие ему ключи и сертификаты оказались скомпрометированы, необходимо предотвратить доступ этого пользователя к ресурсам и отказать в доверии соответствующим сертификатам, т. к. ими могли воспользоваться злоумышленники. Также процедура аннулирования может быть использована в отношении удостоверяющего центра.

Свидетельствование — удостоверение (подтверждение) факта создания или существования информацией некоторой стороной, не являющейся создателем.

Анонимность — довольно редко вспоминаемая задача. Сильным мира сего — правительствам и корпорациям — не выгодно, чтобы пользователь мог остаться анонимным при совершении каких-либо действий в информационном пространстве. Возможно, по этой причине проекты по обеспечению анонимности носят единичный характер и, как правило, долго не живут. Да и средства коммуникации, в подавляющем большинстве, позволяют определить маршрут передачи того или иного сообщения, а значит, вычислить отправителя.

Все перечисленные задачи сформулированы, исходя из потребностей существующего информационного мира. Возможно, со временем часть задач потеряет свою актуальность, но более вероятно, что появятся новые задачи, нуждающиеся в решении.



Глава 2

Основные способы обеспечения защиты

Наверное, потребность в защите информации появилась одновременно с самой информацией. И возможные методы защиты информации почти всегда определялись формой ее представления и предполагаемыми способами использования.

2.1. Общая классификация

В первом приближении все методы защиты информации можно разделить на три класса:

- ❒ законодательные;
- ❒ административные;
- ❒ технические.

Законодательные методы определяют, кто и в какой форме должен иметь доступ к защищаемой информации, и устанавливают ответственность за нарушения установленного порядка. Например, в древнем мире у многих наций были тайные культы, называемые мистериями. К участию в мистериях допускались только посвященные путем особых обрядов лица. Содержание мистерий должно было сохраняться в тайне. А за разглашение секретов мистерий посвященного ждало преследование, вплоть до смерти. Также смертью каралось недозволенное участие в мистериях, даже произошедшее по случайности. В современном мире существуют законы о защите государственной тайны, авторских прав, положения о праве на тайну личной переписки и многие другие. Такие законы описывают, кто и при каких условиях имеет, а кто не имеет право доступа к определенной информации. Однако законодательные методы не способны гарантировать выполнение установленных правил, они лишь декларируют эти правила вместе с мерой ответственности за их нарушение.

Административные методы заключаются в определении процедур доступа к защищаемой информации и строгом их выполнении. Контроль над соблюдением установленного порядка возлагается на специально обученный