Обеспечение информационной безопасности в современной ОС

Лекция 6

1. Введение

Две группы проблем безопасности в современных ОС:

- **Безопасность компьютера:** все проблемы защиты данных, хранящихся и обрабатывающихся компьютером, который рассматривается как автономная система.

Эти проблемы решаются средствами ОС и приложений, таких как БД, а также встроенными аппаратными средствами компьютера.

- **Сетевая безопасность:** все вопросы, связанные с взаимодействием устройств в сети
  - защита данных в момент их передачи по линиям связи
  - защита от несанкционированного удаленного доступа в сеть.

1. Введение

Специфика сетевой безопасности:

- Логический вход чужого пользователя в ваш компьютер является штатной ситуацией, если вы работаете в сети. **Обеспечение безопасности в такой ситуации сводится к тому, чтобы сделать это проникновение контролируемым – каждому пользователю сети должны быть четко определены его права по доступу к информации**, внешним устройствам и выполнению системных действий на каждом из компьютеров сети.
- Сети по своей природе подвержены еще **одному виду опасности — перехвату и анализу сообщений, передаваемых по сети, а также созданию «ложного» трафика**. Большая часть средств обеспечения сетевой безопасности направлена на предотвращение именно этого типа нарушений.

2. Основные понятия безопасности

- Безопасная информационная система — это система, которая
  1. защищает данные от несанкционированного доступа,
  2. всегда готова предоставить их своим пользователям, а
  3. надежно хранит информацию и гарантирует неизменность данных.
- Безопасная система по определению обладает свойствами конфиденциальности, доступности и целостности.

2.1. Конфиденциальность, целостность и доступность данных

- **Конфиденциальность** (confidentiality) — гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).
- **Доступность** (availability) — гарантия того, что авторизованные пользователи всегда получат доступ к данным.
- **Целостность** (integrity) — гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

2.1. Конфиденциальность, целостность и доступность данных

- Любое действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети, называется ***угрозой***.
- Реализованная угроза называется ***атакой***.
- ***Риск*** — это вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки.
- Значение риска тем выше, чем более уязвимой является существующая система безопасности и чем выше вероятность реализации атаки.

2.2. Классификация угроз

- **Неумышленные угрозы** вызываются ошибочными действиями лояльных сотрудников, становятся следствием их низкой квалификации или безответственности. К такому роду угроз относятся последствия ненадежной работы программных и аппаратных средств системы.

Вопросы безопасности тесно переплетаются с вопросами надежности, отказоустойчивости технических средств. предотвращаются путем их совершенствования, использования резервирования на уровне аппаратуры или на уровне массивов данных.

- **Умышленные угрозы** могут ограничиваться либо пассивным чтением данных или мониторингом системы, либо включать в себя активные действия, например нарушение целостности и доступности информации, приведение в нерабочее состояние приложений и устройств.

Так, умышленные угрозы возникают в результате деятельности хакеров и явно направлены на нанесение ущерба предприятию.

2.2. Классификация угроз

В вычислительных сетях можно выделить следующие типы умышленных угроз:

- незаконное проникновение в один из компьютеров сети под видом легального пользователя;
- разрушение системы с помощью программ-вирусов;
- нелегальные действия легального пользователя;
- «подслушивание» внутрисетевого трафика.

2.2. Классификация угроз

Незаконное проникновение может быть реализовано через

- уязвимые места в системе безопасности с использованием недокументированных возможностей операционной системы.
- использование «чужих» паролей, полученных путем подглядывания, расшифровки файла паролей, подбора паролей или получения пароля путем анализа сетевого трафика.
- внедрение в чужой компьютер «троянского коня». Программа - «троянский конь» всегда маскируется под какую-нибудь полезную утилиту или игру.

2.2. Классификация угроз

- Нелегальные действия легального пользователя —легальные пользователей сети, используя свои полномочия, пытаются выполнять действия, выходящие за рамки их должностных обязанностей.
- «Подслушивание» внутрисетевого трафика — это незаконный мониторинг сети, захват и анализ сетевых сообщений.

3. Системный подход к обеспечению безопасности

Средства и приемы:

- морально-этические (нормы, которые сложились по мере распространения вычислительных средств в стране)
- законодательные (законы, постановления правительства и указы президента, нормативные акты и стандарты, которыми регламентируются правила использования и обработки информации ограниченного доступа, а также вводятся меры ответственности за нарушения этих правил),
- административные (действия, предпринимаемые руководством предприятия или организации для обеспечения информационной безопасности)
- психологические,
- физические (экранирование помещений для защиты от излучения, проверка поставляемой аппаратуры на соответствие ее спецификациям и отсутствие аппаратных «жучков», средства наружного наблюдения, устройства, блокирующие физический доступ к отдельным блокам компьютера и т. д.),
- защитные возможности программных и аппаратных средств сети (службы сетевой безопасности, решающие задачи по защите системы, например контроль доступа, включающий процедуры аутентификации и авторизации, аудит, шифрование информации, антивирусную защиту, контроль сетевого трафика и много других задач)

4. Политика безопасности

Важность и сложность проблемы обеспечения безопасности требует выработки политики информационной безопасности, которая подразумевает ответы на следующие вопросы:

- Какую информацию защищать?
- Какой ущерб понесет предприятие при потере или при раскрытии тех или иных данных?
- Кто или что является возможным источником угрозы, какого рода атаки на безопасность системы могут быть предприняты?
- Какие средства использовать для защиты каждого вида информации?

4. Политика безопасности

Базовые принципы политики безопасности:

- предоставление каждому сотруднику минимально уровня привилегий на доступ к данным, необходимый для выполнения должностных обязанностей;
- использование комплексного подхода к обеспечению безопасности;
- используя многоуровневую систему защиты, важно обеспечивать баланс надежности защиты всех уровней;
- использование средств, которые при отказе переходят в состояние максимальной защиты;
- принцип единого контрольно-пропускного пункта — весь входящий и выходящий во трафик должен проходить через единственный узел сети, например через межсетевой экран (firewall);
- Принцип баланса возможного ущерба от реализации угрозы и затрат на ее предотвращение. Ни одна система безопасности не гарантирует защиту данных на уровне 100 %, поскольку является результатом компромисса между возможными рисками и возможными затратами.

4. Политика безопасности

При определении политики безопасности для сети, имеющей выход в Интернет, специалисты рекомендуют разделить задачу на две части:

- Выработать политику доступа к сетевым службам Интернета.
- Выработать политику доступа к ресурсам внутренней сети компании.

4. Политика безопасности

Политика доступа к сетевым службам Интернета включает следующие пункты:

- Определение списка служб Интернета, к которым пользователи внутренней сети должны иметь ограниченный доступ.
- Определение ограничений на методы доступа, например на использование протоколов SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol).
- Принятие решения о том, разрешен ли доступ внешних пользователей из Интернета во внутреннюю сеть. Если да, то кому. Часто доступ разрешают только для некоторых, абсолютно необходимых для работы предприятия служб, например электронной почты.

4. Политика безопасности

Политика доступа к ресурсам внутренней сети компании может быть выражена в одном из двух принципов:

- запрещать все, что не разрешено в явной форме или;
- разрешать все, что не запрещено в явной форме.

В соответствии с выбранным принципом определяются правила обработки внешнего трафика межсетевыми экранами или маршрутизаторами.

Реализация защиты на основе первого принципа дает более высокую степень безопасности, однако при этом могут возникать большие неудобства у пользователей, а кроме того, такой способ защиты обойдется значительно дороже.

При реализации второго принципа сеть окажется менее защищенной, однако пользоваться ею будет удобнее и потребуется меньше затрат.

5. Базовые технологии безопасности. Шифрование

- **Шифрование** — это краеугольный камень всех служб информационной безопасности, будь то система аутентификации или авторизации, средства создания защищенного канала или способ безопасного хранения данных.
- Любая процедура шифрования, превращающая информацию из обычного «понятного» вида в «нечитабельный» зашифрованный вид, естественно, должна быть дополнена процедурой дешифрирования, которая, будучи примененной к зашифрованному тексту, снова приводит его в понятный вид. **Пара процедур — шифрование и дешифрирование — называется криптосистемой.**
- Информацию, над которой выполняются функции шифрования и дешифрирования, будем условно называть «текст», учитывая, что это может быть также числовой массив или графические данные.
- **В современных алгоритмах шифрования предусматривается наличие параметра** — секретного ключа.

5. Базовые технологии безопасности. Шифрование

- Алгоритм шифрования считается раскрытым, если найдена процедура, позволяющая подобрать ключ за реальное время.
- Сложность алгоритма раскрытия является одной из важных характеристик криптосистемы и называется ***криптостойкостью***.
- **Существуют два класса криптосистем — симметричные и асимметричные**.
- В симметричных схемах шифрования (классическая криптография) секретный ключ зашифровки совпадает с секретным ключом расшифровки.
- В асимметричных схемах шифрования (криптография с открытым ключом) открытый ключ зашифровки не совпадает с секретным ключом расшифровки.

5. Базовые технологии безопасности. Шифрование

- **Модель симметричного алгоритма шифрования**

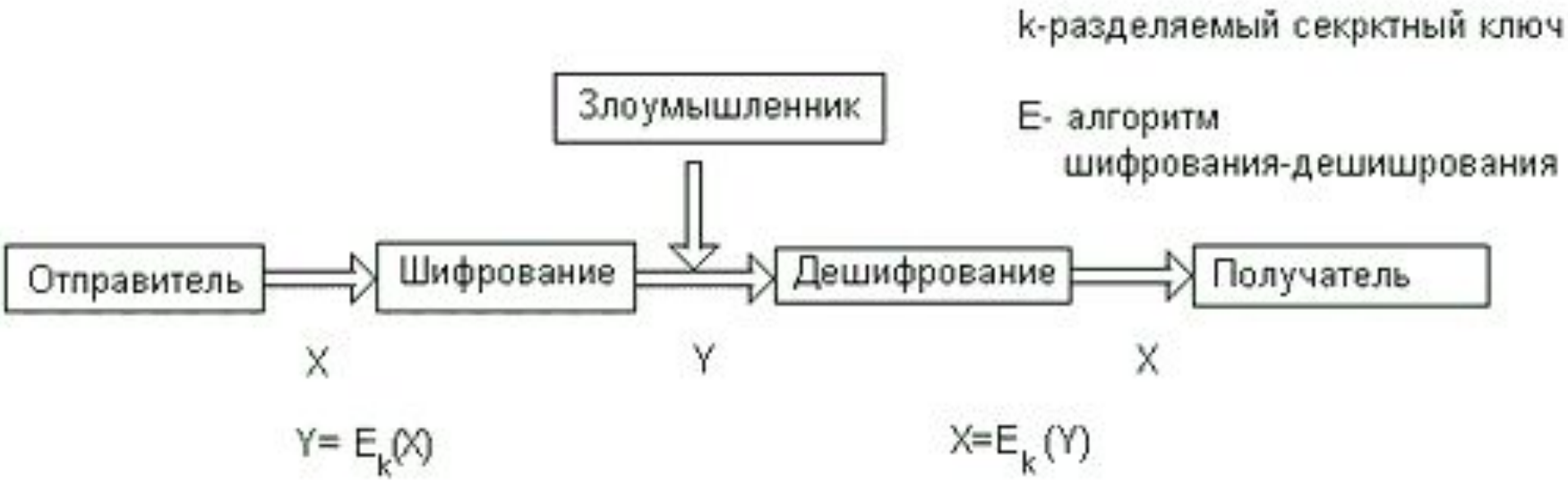

Рис. 6.1. Модель симметричного шифрования

5. Базовые технологии безопасности. Шифрование

- На рис. 6.1 приведена классическая модель симметричной криптосистемы, теоретические основы которой впервые были изложены в 1949 году в работе Клода Шеннона.
- В данной модели три участника: отправитель, получатель, злоумышленник.
- Задача отправителя заключается в том, чтобы по открытому каналу передать некоторое сообщение в защищенном виде. Для этого он на ключе k зашифровывает открытый текст X и передает шифрованный текст Y.
- Задача получателя заключается в том, чтобы расшифровать Y и прочитать сообщение X.
- Предполагается, что отправитель имеет свой источник ключа. Сгенерированный ключ заранее по надежному каналу передается получателю.
- Задача злоумышленника заключается в перехвате и чтении передаваемых сообщений, а также в имитации ложных сообщений.

5. Базовые технологии безопасности. Шифрование

- Модель является универсальной — если зашифрованные данные хранятся в компьютере и никуда не передаются, отправитель и получатель совмещаются в одном лице, а в роли злоумышленника выступает некто, имеющий доступ к компьютеру в ваше отсутствие.
- Наиболее популярным стандартным симметричным алгоритмом шифрования данных является DES (Data Encryption Standard). Алгоритм разработан фирмой IBM и в 1976 году был рекомендован Национальным бюро стандартов к использованию в открытых секторах экономики. Суть этого алгоритма заключается в следующем (рис. 6.2).

5. Базовые технологии безопасности. Шифрование

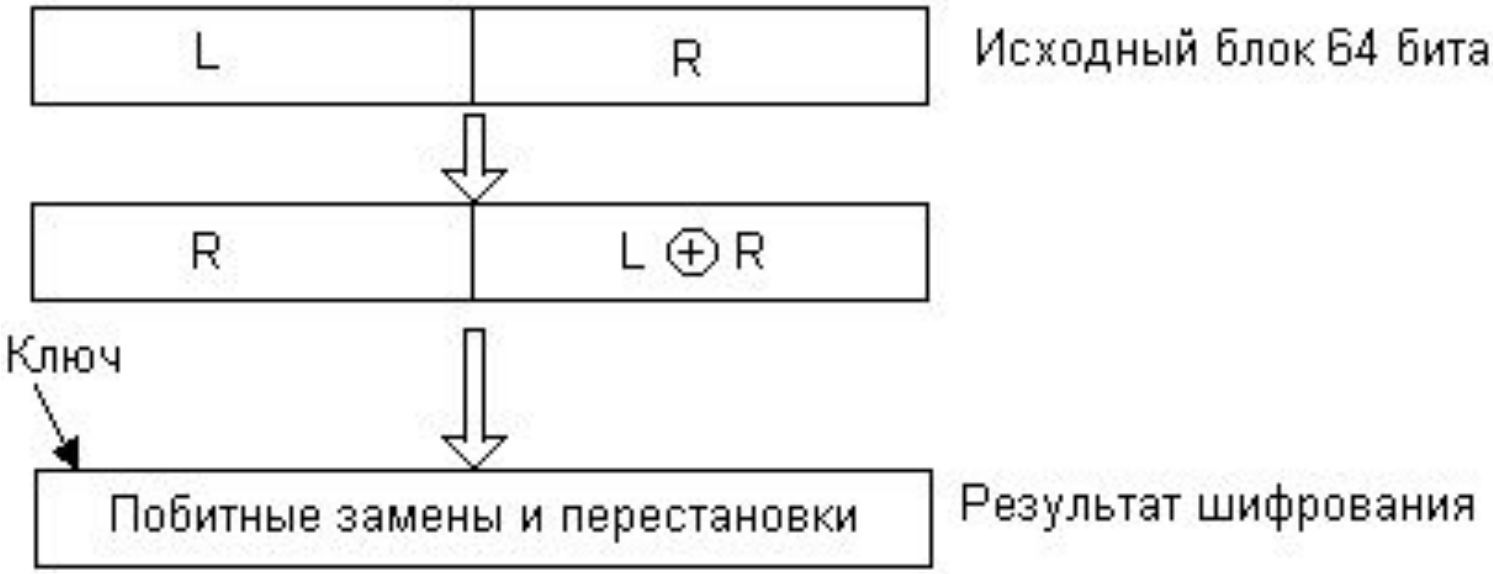

Рис. 6.2. Схема шифрования по алгоритму DES

5. Базовые технологии безопасности. Шифрование

- В алгоритме DES данные шифруются поблочно.
- Перед шифрованием любая форма представления данных преобразуется в числовую. Эти числа получают путем любой открытой процедуры преобразования блока текста в число.
- Например, ими могли бы быть значения двоичных чисел, полученных слиянием ASCII-кодов последовательных символов соответствующего блока текста.
- На вход шифрующей функции поступает блок данных размером 64 бита, он делится пополам на левую (L) и правую (R) части.
- На первом этапе на место левой части результирующего блока помещается правая часть исходного блока.
- Правая часть результирующего блока вычисляется как сумма по модулю 2 (операция XOR) левой и правой частей исходного блока.
- Затем на основе случайной двоичной последовательности по определенной схеме в полученном результате выполняются побитные замены и перестановки. Используемая двоичная последовательность, представляющая собой ключ данного алгоритма, имеет длину 64 бита, из которых 56 действительно случайны, а 8 предназначены для контроля ключа.

5. Базовые технологии безопасности. Шифрование

- Вот уже в течение двух десятков лет алгоритм DES испытывается на стойкость. И хотя существуют примеры успешных попыток «взлома» данного алгоритма, в целом можно считать, что он выдержал испытания. Алгоритм DES широко используется в различных технологиях и продуктах безопасности информационных систем. Для того чтобы повысить криптостойкость алгоритма DES, иногда применяют его усиленный вариант, называемый «тройным DES», который включает троекратное шифрование с использованием двух разных ключей. При этом можно считать, что длина ключа увеличивается с 56 бит до 112 бит, а значит, криптостойкость алгоритма существенно повышается. Но за это приходится платить производительностью — «тройной DES» требует в три раза больше времени, чем «обычный» DES.

5. Базовые технологии безопасности. Шифрование

- **В симметричных алгоритмах главную проблему представляют ключи.**

1. криптостойкость многих симметричных алгоритмов зависит от качества ключа, это предъявляет повышенные требования к службе генерации ключей.
2. принципиальной является надежность канала передачи ключа второму участнику секретных переговоров.

- Проблема с ключами возникает даже в системе с двумя абонентами, а в системе с несколькими абонентами, желающими обмениваться секретными данными по принципу «каждый с каждым», потребуется количество ключей пропорционально квадрату количества абонентов, что при большом числе абонентов делает задачу чрезвычайно сложной.
- Несимметричные алгоритмы, основанные на использовании открытых ключей, снимают эту проблему

5. Базовые технологии безопасности. Шифрование

Несимметричные алгоритмы шифрования

- В середине 70-х двое ученых — Винфилд Диффи и Мартин Хеллман — описали принципы шифрования с открытыми ключами.
- Особенность шифрования на основе открытых ключей состоит в том, что одновременно генерируется уникальная пара ключей, таких, что текст, зашифрованный одним ключом, может быть расшифрован только с использованием второго ключа и наоборот.

5. Базовые технологии безопасности. Шифрование

Рис. 6.1. Модель несимметричного шифрования

5. Базовые технологии безопасности. Шифрование

- В модели криптосхемы с открытым ключом также три участника: отправитель, получатель, злоумышленник (рис. 6.3).
- Задача отправителя заключается в том, чтобы по открытому каналу связи передать некоторое сообщение в защищенном виде.
- Получатель генерирует на своей стороне два ключа: открытый E и закрытый D.
- Закрытый ключ D (часто называемый также личным ключом) абонент должен сохранять в защищенном месте, а открытый ключ E он может передать всем, с кем он хочет поддерживать защищенные отношения.
- Открытый ключ используется для шифрования текста, но расшифровать текст можно только с помощью закрытого ключа.
- Поэтому открытый ключ передается отправителю в незащищенном виде.
- Отправитель, используя открытый ключ получателя, шифрует сообщение X и передает его получателю.
- Получатель расшифровывает сообщение своим закрытым ключом D.

5. Базовые технологии безопасности. Шифрование

- Числа, используемые для шифрования и дешифрирования текста, не могут быть независимыми друг от друга, а значит, есть теоретическая возможность вычисления закрытого ключа по открытому, но это связано с огромным количеством вычислений, которые требуют огромного времени.
- Поясним принципиальную связь между закрытым и открытым ключами следующей аналогией.
- Пусть абонент 1 (рис. 6.4, а) решает вести секретную переписку со своими сотрудниками на малоизвестном языке, например санскрите. Для этого он обзаводится санскритско-русским словарем, а всем своим абонентам посылает русско-санскритские словари. Каждый из них, пользуясь словарем, пишет сообщения на санскрите и посылает их абоненту 1, который переводит их на русский язык, пользуясь доступным только ему санскритско-русским словарем. Очевидно, что здесь роль открытого ключа E играет русско-санскритский словарь, а роль закрытого ключа D — санскритско-русский словарь. Могут ли абоненты 2, 3 и 4 прочитать чужие сообщения S2, S3, S4, которые посылает каждый из них абоненту 1? Вообще-то нет, так как, для этого им нужен санскритско-русский словарь, обладателем которого является только абонент 1. Но теоретическая возможность этого имеется, так как затратив массу времени, можно прямым перебором составить санскритско-русский словарь по русско-санскритскому словарю. Такая процедура, требующая больших временных затрат, является отдаленной аналогией восстановления закрытого ключа по открытому.

5. Базовые технологии безопасности. Шифрование

- На рис. 6.4, б показана другая схема использования открытого и закрытого ключей, целью которой является подтверждение авторства (аутентификация или электронная подпись) посылаемого сообщения. В этом случае поток сообщений имеет обратное направление — от абонента 1, обладателя закрытого ключа D, к его корреспондентам, обладателям открытого ключа E. Если абонент 1 хочет аутентифицировать себя (поставить электронную подпись), то он шифрует известный текст своим закрытым ключом D и передает шифровку своим корреспондентам. Если им удается расшифровать текст открытым ключом абонента 1, то это доказывает, что текст был зашифрован его же закрытым ключом, а значит, именно он является автором этого сообщения. Заметим, что в этом случае сообщения S2, S3, 84, адресованные разным абонентам, не являются секретными, так как все они — обладатели одного и того же открытого ключа, с помощью которого они могут расшифровывать все сообщения, поступающие от абонента 1.

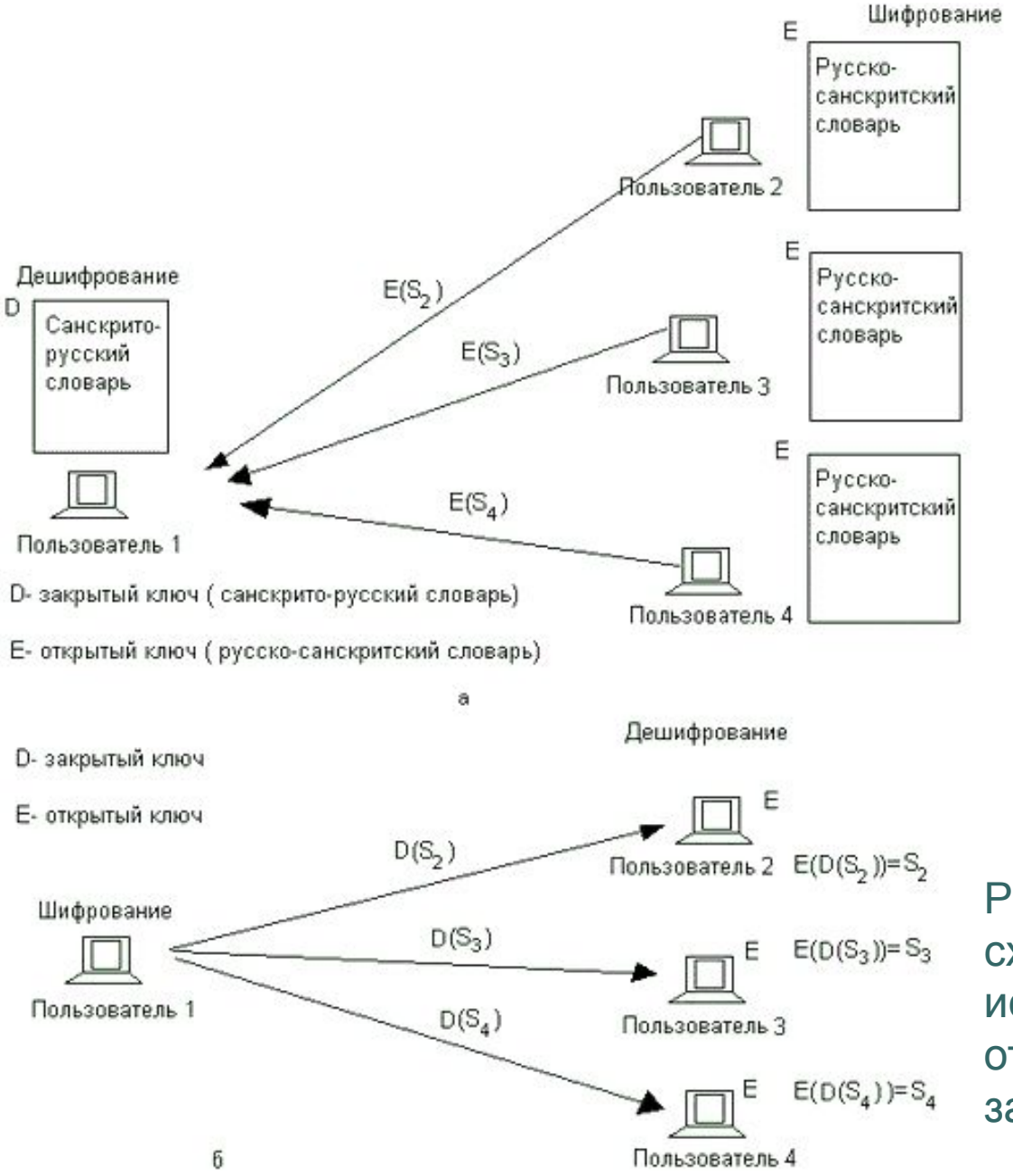

Рис. 6.4. Две схемы использования открытого и закрытого ключей

5. Базовые технологии безопасности. Шифрование

- Для того чтобы в сети все n абонентов имели возможность не только принимать зашифрованные сообщения, но и сами посылать таковые, каждый абонент должен обладать своей собственной парой ключей E и D. Всего в сети будет 2n ключей: n открытых ключей для шифрования и n секретных ключей для дешифрирования. Таким образом, решается проблема масштабируемости — квадратичная зависимость количества ключей от числа абонентов в симметричных алгоритмах заменяется линейной зависимостью в несимметричных алгоритмах. Исчезает и задача секретной доставки ключа. Злоумышленнику нет смысла стремиться завладеть открытым ключом, поскольку это не дает возможности расшифровывать текст или вычислить закрытый ключ.

5. Базовые технологии безопасности. Шифрование

- **Хотя информация об открытом ключе не является секретной, ее нужно защищать от подлогов, чтобы злоумышленник под именем легального пользователя не навязал свой открытый ключ, после чего с помощью своего закрытого ключа он может расшифровывать все сообщения, посылаемые легальному пользователю и отправлять свои сообщения от его имени**. Проще всего было бы распространять списки, связывающие имена пользователей с их открытыми ключами широковещательно, путем публикаций в средствах массовой информации (бюллетени, специализированные журналы и т. п.). Однако при таком подходе мы снова, как и в случае с паролями, сталкиваемся с плохой масштабируемостью. Решением этой проблемы является технология цифровых сертификатов. Сертификат — это электронный документ, который связывает конкретного пользователя с конкретным ключом.
- В настоящее время одним из наиболее популярных криптоалгоритмов с открытым ключом является криптоалгоритм RSA.

5. Базовые технологии безопасности. Шифрование

Криптоалгоритм RSA

- В 1978 году трое ученых (Ривест, Шамир и Адлеман) разработали систему шифрования с открытыми ключами RSA (Rivest, Shamir, Adleman), полностью отвечающую всем принципам Диффи-Хеллмана. Этот метод состоит в следующем:

1. Случайно выбираются два очень больших простых числа p и q.
2. Вычисляются два произведения n=pxq и nr=(p-l)x(q-l).
3. Выбирается случайное целое число E, не имеющее общих сомножителей с m.
4. Находится D, такое, что DE=1 по модулю m.
5. Исходный текст, X, разбивается на блоки таким образом, чтобы 0<X<n.
6. Для шифрования сообщения необходимо вычислить C=XE по модулю n.
7. Для дешифрирования вычисляется X=CD по модулю n.

- Таким образом, чтобы зашифровать сообщение, необходимо знать пару чисел (E, n), а чтобы дешифрировать — пару чисел (D, n). Первая пара — это открытый ключ, а вторая — закрытый.

5. Базовые технологии безопасности. Шифрование

Криптоалгоритм RSA

Зная открытый ключ (E, n), можно вычислить значение закрытого ключа D. Необходимым промежуточным действием в этом преобразовании является нахождение чисел p и q, для чего нужно разложить на простые множители очень большое число n, а на это требуется очень много времени. Именно с огромной вычислительной сложностью разложения большого числа на простые множители связана высокая криптостойкость алгоритма RSA.

В некоторых публикациях приводятся следующие оценки: для того чтобы найти разложение 200-значно-го числа, понадобится 4 миллиарда лет работы компьютера с быстродействием миллион операций в секунду. Однако следует учесть, что в настоящее время активно ведутся работы по совершенствованию методов разложения больших чисел, поэтому в алгоритме RSA стараются применять числа длиной более 200 десятичных разрядов.

5. Базовые технологии безопасности. Шифрование

Криптоалгоритм RSA

Программная реализация криптоалгоритмов типа RSA значительно сложнее и менее производительна, чем реализация классических криптоалгоритмов типа DES. Вследствие сложности реализации операций модульной арифметики криптоалгоритм RSA часто используют только для шифрования небольших объемов информации, например для рассылки классических секретных ключей или в алгоритмах цифровой подписи, а основную часть пересылаемой информации шифруют с помощью симметричных алгоритмов.

- В табл. 6.1 приведены некоторые сравнительные характеристики классического криптоалгоритма DES и криптоалгоритма RSA.

5. Базовые технологии безопасности. Шифрование

Таблица 6.1. Сравнительные характеристики алгоритмов шифрования

Характеристика	DES	RSA
Скорость шифрования	Высокая	Низкая
Используемая функция шифрования	Перестановка и подстановка	Возведение в степень
Длина ключа	56 бит	Более 500 бит
Наименее затратный криптоанализ (его сложность определяет стойкость алгоритма)	Перебор по всему ключевому пространству	Разложение числа на простые множители
Время генерации ключа	Миллисекунды	Минуты
Тип ключа	Симметричный	Асимметричный

5. Базовые технологии безопасности. Шифрование

- **Односторонние функции шифрования**
- Во многих базовых технологиях безопасности используется еще один прием шифрования — шифрование с помощью односторонней функции (one-way function), называемой также хэш-функцией (hash function), или дайджест-функцией (digest function).
- Эта функция, примененная к шифруемым данным, дает в результате значение (дайджест), состоящее из фиксированного небольшого числа байт (рис. 6.5, а). Дайджест передается вместе с исходным сообщением. Получатель сообщения, зная, какая односторонняя функция шифрования (ОФШ) была применена для получения дайджеста, заново вычисляет его, используя незашифрованную часть сообщения. Если значения полученного и вычисленного дайджестов совпадают, то значит, содержимое сообщения не было подвергнуто никаким изменениям. Знание дайджеста не дает возможности восстановить исходное сообщение, но зато позволяет проверить целостность данных

5. Базовые технологии безопасности. Шифрование

- **Односторонние функции шифрования**
- Дайджест является своего рода контрольной суммой для исходного сообщения. Однако имеется и существенное отличие. Использование контрольной суммы является средством проверки целостности передаваемых сообщений по ненадежным линиям связи. Это средство не направлено на борьбу со злоумышленниками, которым в такой ситуации ничто не мешает подменить сообщение, добавив к нему новое значение контрольной суммы. Получатель в таком случае не заметит никакой подмены.
- В отличие от контрольной суммы при вычислении дайджеста требуются секретные ключи. В случае если для получения дайджеста использовалась односторонняя функция с параметром, который известен только отправителю и получателю, любая модификация исходного сообщения будет немедленно обнаружена.

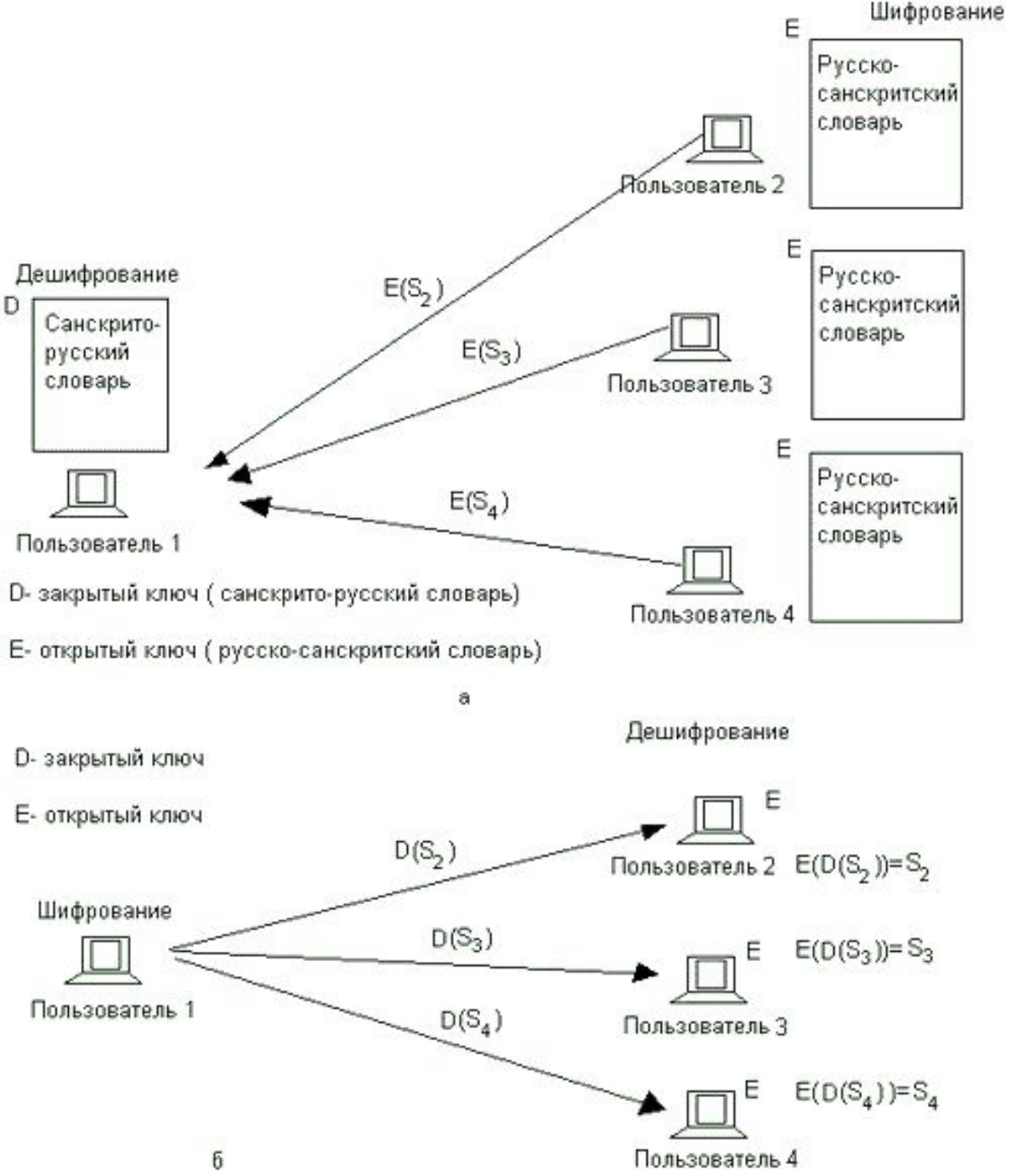

Рис. 6.5. Односторонние функции шифрования

5. Базовые технологии безопасности. Шифрование

- На рис. 6.5, б показан другой вариант использования односторонней функции шифрования для обеспечения целостности данных. В данном случае односторонняя функция не имеет параметра-ключа, но зато применяется не просто к сообщению, а к сообщению, дополненному секретным ключом. Получатель, извлекая исходное сообщение, также дополняет его тем же известным ему секретным ключом, после чего применяет к полученным данным одностороннюю функцию. Результат вычислений сравнивается с полученным по сети дайджестом.
- Помимо обеспечения целостности сообщений дайджест может быть использован в качестве электронной подписи для аутентификации передаваемого документа.

5. Базовые технологии безопасности. Шифрование

- Построение односторонних функций является трудной задачей. Такого рода функции должны удовлетворять двум условиям:
- по дайджесту, вычисленному с помощью данной функции, невозможно каким-либо образом вычислить исходное сообщение;
- должна отсутствовать возможность вычисления двух разных сообщений, для которых с помощью данной функции могли быть вычислены одинаковые дайджесты.
- Наиболее популярной в системах безопасности в настоящее время является серия хэш-функций MD2, MD4, MD5. Все они генерируют дайджесты фиксированной длины 16 байт. Адаптированным вариантом MD4 является американский стандарт SHA, длина дайджеста в котором составляет 20 байт. Компания IBM поддерживает односторонние функции MDC2 и MDC4, основанные на алгоритме шифрования DES.

6. Аутентификация, авторизация, аудит

- **Аутентификация** (authentication) предотвращает доступ к сети нежелательных лиц и разрешает вход для легальных пользователей.
- Термин «аутентификация» в переводе с латинского означает «установление подлинности».
- Аутентификацию следует отличать от идентификации.
- Идентификация заключается в сообщении пользователем системе своего идентификатора, в то время как аутентификация — это процедура доказательства пользователем того, что он есть тот, за кого себя выдает, в частности, доказательство того, что именно ему принадлежит введенный им идентификатор.

6. Аутентификация, авторизация, аудит

В процедуре аутентификации участвуют две стороны:

1. **одна сторона** доказывает свою аутентичность, предъявляя некоторые доказательства, а
2. **другая сторона** — аутентификатор — проверяет эти доказательства и принимает решение. В качестве доказательства аутентичности используются самые разнообразные приемы:

- аутентифицируемый может продемонстрировать знание некоего общего для обеих сторон секрета: слова (пароля) или факта (даты и места события, прозвища человека и т. п.);
- аутентифицируемый может продемонстрировать, что он владеет неким уникальным предметом (физическим ключом), в качестве которого может выступать, например, электронная магнитная карта;
- аутентифицируемый может доказать свою идентичность, используя собственные биохарактеристики: рисунок радужной оболочки глаза или отпечатки пальцев, которые предварительно были занесены в базу данных аутентификатора.

6. Аутентификация, авторизация, аудит

- Сетевые службы аутентификации строятся на основе всех этих приемов, но чаще всего для доказательства идентичности пользователя используются пароли.
- Простота и логическая ясность механизмов аутентификации на основе паролей в какой-то степени компенсирует известные слабости паролей:

1. возможность раскрытия и разгадывания паролей,
2. возможность «подслушивания» пароля путем анализа сетевого трафика.

- Для снижения уровня угрозы от раскрытия паролей администраторы сети, как правило, применяют встроенные программные средства для формирования политики назначения и использования паролей:
  - задание максимального и минимального сроков действия пароля,
  - хранение списка уже использованных паролей,
  - управление поведением системы после нескольких неудачных попыток логического входа и т. п.
  - Перехват паролей по сети можно предупредить путем их шифрования перед передачей в сеть.

6. Аутентификация, авторизация, аудит

- Легальность пользователя может устанавливаться по отношению к различным системам.
- Так, работая в сети, пользователь может проходить процедуру аутентификации и как локальный пользователь, который претендует на использование ресурсов только данного компьютера, и как пользователь сети, который хочет получить доступ ко всем сетевым ресурсам.
- При локальной аутентификации пользователь вводит свои идентификатор и пароль, которые автономно обрабатываются операционной системой, установленной на данном компьютере.
- При логическом входе в сеть данные о пользователе (идентификатор и пароль) передаются на сервер, который хранит учетные записи обо всех пользователях сети.
- Многие приложения имеют свои средства определения, является ли пользователь законным. И тогда пользователю приходится проходить дополнительные этапы проверки.

6. Аутентификация, авторизация, аудит

- В качестве объектов, требующих аутентификации, могут выступать не только пользователи, но и различные устройства, приложения, текстовая и другая информация.
- Так, например, пользователь, обращающийся с запросом к корпоративному серверу, должен доказать ему свою легальность, но он также должен убедиться сам, что ведет диалог действительно с сервером своего предприятия.
- Другими словами, сервер и клиент должны пройти процедуру взаимной аутентификации. Здесь мы имеем дело с аутентификацией на уровне приложений.
- При установлении сеанса связи между двумя устройствами также часто предусматриваются процедуры взаимной аутентификации на более низком, канальном уровне.
- Примером такой процедуры является аутентификация по протоколам PAP и CHAP, входящим в семейство протоколов PPP.
- Аутентификация данных означает доказательство целостности этих данных, а также того, что они поступили именно от того человека, который объявил об этом. Для этого используется механизм электронной подписи

6. Аутентификация, авторизация, аудит

- В вычислительных сетях процедуры аутентификации часто реализуются теми же программными средствами, что и процедуры **авторизации**.
- В отличие от аутентификации, которая распознает легальных и нелегальных пользователей, система авторизации имеет дело только с легальными пользователями, которые уже успешно прошли процедуру аутентификации.
- Цель подсистем авторизации состоит в том, чтобы предоставить каждому легальному пользователю именно те виды доступа и к тем ресурсам, которые были для него определены администратором системы.

6. Аутентификация, авторизация, аудит

- **Авторизация доступа**
- Средства авторизации (authorization) контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые ему были определены администратором.
- Кроме того, система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких как локальный доступ к серверу, установка системного времени, создание резервных копий данных, выключение сервера и т. п.
- Система авторизации наделяет пользователя сети правами выполнять определенные действия над определенными ресурсами. Для этого могут быть использованы различные формы предоставления правил доступа, которые часто делят на два класса:
  - избирательный доступ;
  - мандатный доступ.

6. Аутентификация, авторизация, аудит

- **Избирательные права доступа реализуются в операционных системах универсального назначения**.
- В наиболее распространенном варианте такого подхода определенные операции над определенным ресурсом разрешаются или запрещаются пользователям или группам пользователей, явно указанным своими идентификаторами.

Например, пользователю, имеющему идентификатор User_T, может быть разрешено выполнять операции чтения и записи по отношению к файлу Filet.

- Модификацией этого способа является использование для идентификации пользователей их должностей, или факта их принадлежности к персоналу того или иного производственного подразделения, или еще каких-либо других позиционирующих характеристик.

Примером такого правила может служить следующее: файл бухгалтерской отчетности BUCH могут читать работники бухгалтерии и руководитель предприятия.

6. Аутентификация, авторизация, аудит

- **Мандатный подход к определению прав доступа заключается в том, что вся информация делится на уровни в зависимости от степени секретности, а все пользователи сети также делятся на группы, образующие иерархию в соответствии с уровнем допуска к этой информации**.
- Такой подход используется в известном делении информации на информацию для служебного пользования, «секретно», «совершенно секретно».
- При этом пользователи этой информации в зависимости от определенного для них статуса получают различные формы допуска: первую, вторую или третью.
- В отличие от систем с избирательными правами доступа в системах с мандатным подходом пользователи в принципе не имеют возможности изменить уровень доступности информации.

6. Аутентификация, авторизация, аудит

Процедуры авторизации реализуются программными средствами, которые могут быть встроены в ОС или в приложение, а также могут поставляться в виде отдельных программных продуктов. При этом программные системы авторизации могут строиться на базе двух схем:

- централизованная схема авторизации, базирующаяся на сервере;
- децентрализованная схема, базирующаяся на рабочих станциях.

6. Аутентификация, авторизация, аудит

- **В первой схеме сервер управляет процессом предоставления ресурсов пользователю. Главная цель таких систем — реализовать «принцип единого входа».** В соответствии с централизованной схемой пользователь один раз логически входит в сеть и получает на все время работы некоторый набор разрешений по доступу к ресурсам сети.
- **При втором подходе рабочая станция сама является защищенной — средства защиты работают на каждой машине, и сервер не требуется.** Теоретически доступ к каждому приложению должен контролироваться средствами безопасности самого приложения или же средствами, существующими в той операционной среде, в которой оно работает. В корпоративной сети администратору придется отслеживать работу механизмов безопасности, используемых всеми типами приложений — электронной почтой, службой каталогов локальной сети, базами данных хостов и т. п. Когда администратору приходится добавлять или удалять пользователей, то часто требуется вручную конфигурировать доступ к каждой программе или системе.
- В крупных сетях часто применяется комбинированный подход предоставления пользователю прав доступа к ресурсам сети

6. Аутентификация, авторизация, аудит

- Подчеркнем, что системы аутентификации и авторизации совместно выполняют одну задачу, поэтому необходимо предъявлять одинаковый уровень требований к системам авторизации и аутентификации.
- Ненадежность одного звена здесь не может быть компенсирована высоким качеством другого звена.
- Если при аутентификации используются пароли, то требуются чрезвычайные меры по их защите.
- Однажды украденный пароль открывает двери ко всем приложениям и данным, к которым пользователь с этим паролем имел легальный доступ.

6. Аутентификация, авторизация, аудит

- **Аудит (auditing)** — фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам.
- Подсистема аудита современных ОС позволяет дифференцирование задавать перечень интересующих администратора событий с помощью удобного графического интерфейса.
- Средства учета и наблюдения обеспечивают возможность обнаружить и зафиксировать важные события, связанные с безопасностью, или любые попытки создать, получить доступ или удалить системные ресурсы.
- Аудит используется для того, чтобы засекать даже неудачные попытки «взлома» системы.

6. Аутентификация, авторизация, аудит

- Учет и наблюдение означает способность системы безопасности «шпионить» за выбранными объектами и их пользователями и выдавать сообщения тревоги, когда кто-нибудь пытается читать или модифицировать системный файл.
- Если кто-то пытается выполнить действия, определенные системой безопасности для отслеживания, то система аудита пишет сообщение в журнал регистрации, идентифицируя пользователя.
- Системный менеджер может создавать отчеты о безопасности, которые содержат информацию из журнала регистрации. Для «сверхбезопасных» систем предусматриваются аудио- и видеосигналы тревоги, устанавливаемые на машинах администраторов, отвечающих за безопасность

7. Технология защищенного канала

- Технология защищенного канала призвана обеспечивать безопасность передачи данных по открытой транспортной сети, например по Интернету. Защищенный канал подразумевает выполнение трех основных функций:
  - взаимную аутентификацию абонентов при установлении соединения, которая может быть выполнена, например, путем обмена паролями;
  - защиту передаваемых по каналу сообщений от несанкционированного доступа, например, путем шифрования;
  - подтверждение целостности поступающих по каналу сообщений, например, путем передачи одновременно с сообщением его дайджеста.
- Совокупность защищенных каналов, созданных предприятием в публичной сети для объединения своих филиалов, часто называют виртуальной частной сетью (Virtual Private Network, VPN).

7. Технология защищенного канала

- В зависимости от места расположения программного обеспечения защищенного канала различают две схемы его образования:
- схему с конечными узлами, взаимодействующими через публичную сеть (рис. 6.6, а);
- схему с оборудованием поставщика услуг публичной сети, расположенным на границе между частной и публичной сетями (рис. 6.6, б).

7. Технология защищенного канала

- В первом случае защищенный канал образуется программными средствами, установленными на двух удаленных компьютерах, принадлежащих двум разным локальным сетям одного предприятия и связанных между собой через публичную сеть.
- Преимуществом этого подхода является полная защищенность канала вдоль всего пути следования, а также возможность использования любых протоколов создания защищенных каналов, лишь бы на конечных точках канала поддерживался один и тот же протокол.
- Недостатки заключаются в избыточности и децентрализованности решения.
- Избыточность состоит в том, что вряд ли стоит создавать защищенный канал на всем пути прохождения данных: уязвимыми для злоумышленников обычно являются сети с коммутацией пакетов, а не каналы телефонной сети или выделенные каналы, через которые локальные сети подключены к территориальной сети.
- Децентрализация заключается в том, что для каждого компьютера, которому требуется предоставить услуги защищенного канала, необходимо отдельно устанавливать, конфигурировать и администрировать программные средства защиты данных. Подключение каждого нового компьютера к защищенному каналу требует выполнения этих трудоемких работ заново.

7. Технология защищенного канала

- Во втором случае клиенты и серверы не участвуют в создании защищенного канала — он прокладывается только внутри публичной сети с коммутацией пакетов, например, внутри Интернета.
- Канал может быть проложен, например, между сервером удаленного доступа поставщика услуг публичной сети и пограничным маршрутизатором корпоративной сети.
- Это хорошо масштабируемое решение, управляемое централизованно как администратором корпоративной сети, так и администратором сети поставщика услуг. Для компьютеров корпоративной сети канал прозрачен — программное обеспечение этих конечных узлов остается без изменений.
- Такой гибкий подход позволяет легко образовывать новые каналы защищенного взаимодействия между компьютерами независимо от их места расположения.
- Реализация этого подхода сложнее — нужен стандартный протокол образования защищенного канала, требуется установка у всех поставщиков услуг программного обеспечения, поддерживающего такой протокол, необходима поддержка протокола производителями пограничного коммуникационного оборудования.
- Однако вариант, когда все заботы по поддержанию защищенного канала берет на себя поставщик услуг публичной сети, оставляет сомнения в надежности защиты:
  - незащищенными оказываются каналы доступа к публичной сети,
  - потребитель услуг чувствует себя в полной зависимости от надежности поставщика услуг. И, тем не менее, специалисты прогнозируют, что именно вторая схема в ближайшем будущем станет основной в построении защищенных каналов.

7. Технология защищенного канала

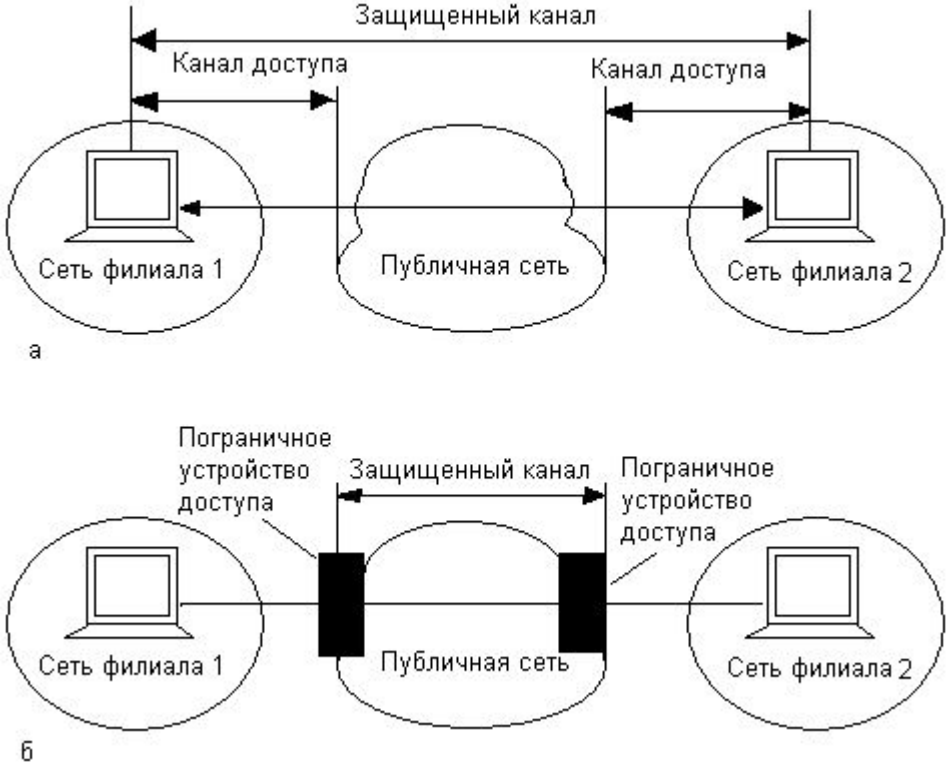

Рис. 6.6. Два способа образования защищенного канала

8. Технологии аутентификации
8.1. Сетевая аутентификация на основе многоразового пароля

- В соответствии с базовым принципом «единого входа», когда пользователю достаточно один раз пройти процедуру аутентификации, чтобы получить доступ ко всем сетевым ресурсам, в современных ОС предусматриваются централизованные службы аутентификации.
- Такая служба поддерживается одним из серверов сети и использует для своей работы базу данных, в которой хранятся учетные данные (иногда называемые бюджетами) о пользователях сети.
- Учетные данные содержат наряду с другой информацией идентификаторы и пароли пользователей.
- Однако такая упрощенная схема имеет большой изъян. А именно при передаче пароля с клиентского компьютера на сервер, выполняющий процедуру аутентификации, этот пароль может быть перехвачен злоумышленником. Поэтому в разных ОС применяются разные приемы, чтобы избежать передачи пароля по сети в незащищенном виде.

8.2. Аутентификация с использованием одноразового пароля

- Алгоритмы аутентификации, основанные на многоразовых паролях, не очень надежны.
- Более надежными оказываются схемы, использующие одноразовые пароли.
- С другой стороны, одноразовые пароли намного дешевле и проще биометрических систем аутентификации, таких как сканеры сетчатки глаза или отпечатков пальцев.
- Все это делает системы, основанные на одноразовых паролях, очень перспективными.
- Следует иметь в виду, что, как правило, системы аутентификации на основе одноразовых паролей рассчитаны на проверку только удаленных, а не локальных пользователей.

8.2. Аутентификация с использованием одноразового пароля

- Генерация одноразовых паролей может выполняться либо программно, либо аппаратно.
- Некоторые реализации аппаратных устройств доступа на основе одноразовых паролей представляют собой миниатюрные устройства со встроенным микропроцессором, похожие на обычные пластиковые карточки, используемые для доступа к банкоматам (аппаратные ключи).
- Аппаратные ключи могут быть также реализованы в виде присоединяемого к разъему устройства, которое располагается между компьютером и модемом, или в виде карты (гибкого диска), вставляемой в дисковод компьютера.

8.2. Аутентификация с использованием одноразового пароля

- Существуют и программные реализации средств аутентификации на основе одноразовых паролей (программные ключи).
- Программные ключи размещаются на сменном магнитном диске в виде обычной программы, важной частью которой является генератор одноразовых паролей.
- Применение программных ключей и присоединяемых к компьютеру карточек связано с некоторым риском, так как пользователи часто забывают гибкие диски в машине или не отсоединяют карточки от ноутбуков.

Технологии аутентификации

- Независимо от того, какую реализацию системы аутентификации на основе одноразовых паролей выбирает пользователь, он, как и в системах аутентификации с использованием многоразовых паролей, сообщает системе свой идентификатор, однако вместо того, чтобы вводить каждый раз один и тот же пароль, он указывает последовательность цифр, сообщаемую ему аппаратным или программным ключом.
- Через определенный небольшой период времени генерируется другая последовательность — новый пароль.
- Аутентификационный сервер проверяет введенную последовательность и разрешает пользователю осуществить логический вход.
- Аутентификационный сервер может представлять собой отдельное устройство, выделенный компьютер или же программу, выполняемую на обычном сервере.

8.3. Аутентификация на основе сертификатов

- Аутентификация с применением цифровых сертификатов является альтернативой использованию паролей и представляется естественным решением в условиях, когда число пользователей сети измеряется миллионами.
- В таких обстоятельствах процедура предварительной регистрации пользователей, связанная с назначением и хранением их паролей, становится крайне обременительной, опасной, а иногда и просто нереализуемой.
- При использовании сертификатов сеть, которая дает пользователю доступ к своим ресурсам, не хранит никакой информации о своих пользователях — они ее предоставляют сами в своих запросах в виде сертификатов, удостоверяющих личность пользователей.
- Сертификаты выдаются специальными уполномоченными организациями — центрами сертификации (Certificate Authority, CA). Поэтому задача хранения секретной информации (закрытых ключей) возлагается на самих пользователей, что делает это решение гораздо более масштабируемым, чем вариант с использованием централизованной базы паролей.

8.3. Аутентификация на основе сертификатов

- **Схема использования сертификатов**
- Сертификат представляет собой электронную форму, в которой содержится следующая информация:
  - открытый ключ владельца данного сертификата;
  - сведения о владельце сертификата, такие, например, как имя, адрес электронной почты, наименование организации, в которой он работает, и т. п.;
  - наименование сертифицирующей организации, выдавшей данный сертификат.
  - Кроме того, сертификат содержит электронную подпись сертифицирующей организации — зашифрованные закрытым ключом этой организации данные, содержащиеся в сертификате.

Использование сертификатов основано на предположении, что сертифицирующих организаций немного и их открытые ключи могут быть всем известны каким-либо способом, например, из публикаций в журналах.

8.3. Аутентификация на основе сертификатов

- Когда пользователь хочет подтвердить свою личность, он предъявляет свой сертификат в двух формах — открытой (то есть такой, в которой он получил его в сертифицирующей организации) и зашифрованной с применением своего закрытого ключа (рис. 6.8).
- Сторона, проводящая аутентификацию, берет из открытого сертификата открытый ключ пользователя и расшифровывает с помощью него зашифрованный сертификат.
- Совпадение результата с открытым сертификатом подтверждает факт, что предъявитель действительно является владельцем закрытого ключа, парного с указанным открытым.
- Затем с помощью известного открытого ключа указанной в сертификате организации проводится расшифровка подписи этой организации в сертификате.
- Если в результате получается тот же сертификат с тем же именем пользователя и его открытым ключом — значит, он действительно прошел регистрацию в сертификационном центре, является тем, за кого себя выдает, и указанный в сертификате открытый ключ действительно принадлежит ему.

8.3. Аутентификация на основе сертификатов

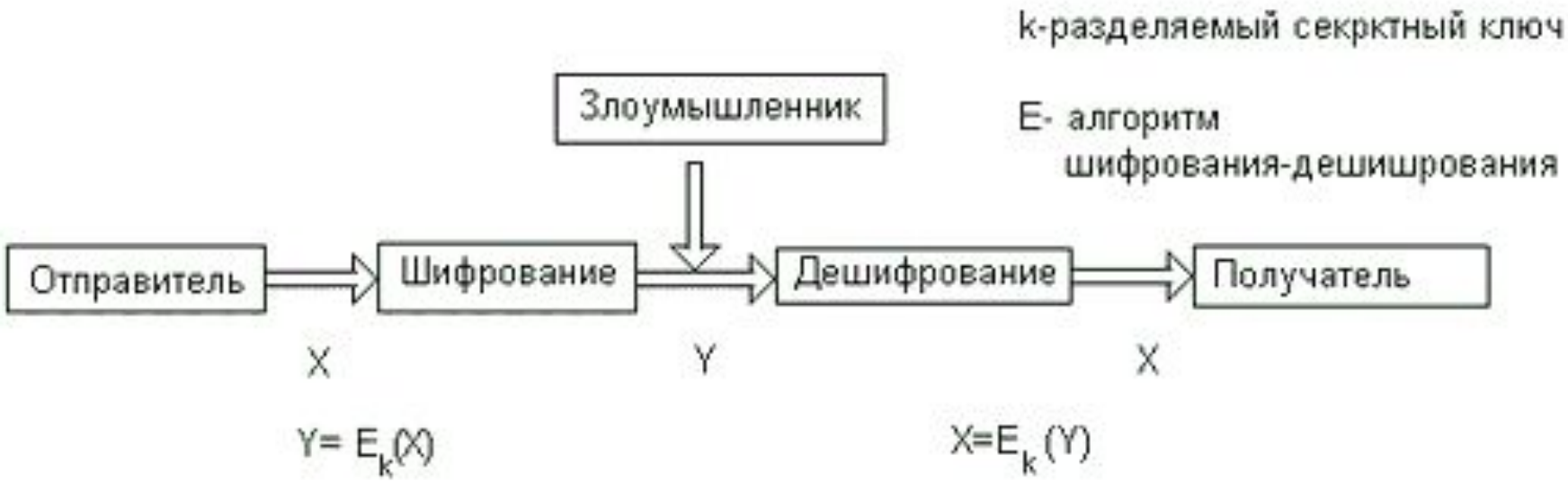

Рис. 6.8. Аутентификация пользователей на основе сертификатов

8.3. Аутентификация на основе сертификатов

- Сертификаты можно использовать не только для аутентификации, но и для предоставления избирательных прав доступа.
- Для этого в сертификат могут вводиться дополнительные поля, в которых указывается принадлежность его владельцев той или иной категории пользователей. Эта категория назначается сертифицирующей организацией в зависимости от условий, на которых выдается сертификат.

Например, организация, поставляющая через Интернет на коммерческой основе информацию, может выдавать сертификаты определенной категории пользователям, оплатившим годовую подписку на некоторый бюллетень, а Web-сервер будет предоставлять доступ к страницам бюллетеня только пользователям, предъявившим сертификат данной категории.

- Сертификат является не только удостоверением личности, но и удостоверением принадлежности открытого ключа. Цифровой сертификат устанавливает и гарантирует соответствие между открытым ключом и его владельцем. Это предотвращает угрозу подмены открытого ключа.
- Если некоторому абоненту поступает открытый ключ в составе сертификата, то он может быть уверен, что этот открытый ключ гарантированно принадлежит отправителю, адрес и другие сведения о котором содержатся в этом сертификате.

Сертифицирующие центры

- Сертификат является средством аутентификации Пользователя при его обращении к сетевым ресурсам, роль аутентифицирующей стороны играют при этом информационные серверы корпоративной сети или Интернета.
- В то же время и сама процедура получения сертификата включает этап аутентификации, здесь аутентификатором выступает сертифицирующая организация.
- Для получения сертификата клиент должен сообщить сертифицирующей организации свой открытый ключ и те или иные сведения, удостоверяющие его личность. Все эти данные клиент может отправить по электронной почте или принести на гибком диске лично.
- Перечень необходимых данных зависит от типа получаемого сертификата.
- Сертифицирующая организация проверяет доказательства подлинности, помещает свою цифровую подпись в файл, содержащий открытый ключ, и посылает сертификат обратно, подтверждая факт принадлежности данного конкретного ключа конкретному лицу.
- После этого сертификат может быть встроен в любой запрос на использование информационных ресурсов сети.

Сертифицирующие центры

Функции сертифицирующей организации могут выполнять:

- само предприятие. В этом случае упрощается процедура первичной аутентификации при выдаче сертификата. Предприятия уже достаточно осведомлены о своих сотрудниках, чтобы брать на себя задачу подтверждения их личности. Для автоматизации процесса генерации, выдачи и обслуживания сертификатов предприятия могут использовать готовые программные продукты, например компания Netscape Communications выпустила сервер сертификатов, который организации могут у себя устанавливать для выпуска своих собственных сертификатов.
- независимые центры по выдаче сертификатов, работающие на коммерческой основе, например сертифицирующий центр компании Verisign. Сертификаты компании Verisign выполнены в соответствии с международным стандартом X.509 и используются во многих продуктах защиты данных, в том числе в популярном протоколе защищенного канала SSL. Любой желающий может обратиться с запросом на получение сертификата на Web-сервер этой компании. Сервер Verisign предлагает несколько типов сертификатов, отличающихся уровнем возможностей, которые получает владелец сертификата.

Сертифицирующие центры

- **Сертификаты класса 1** предоставляют пользователю самый низкий уровень полномочий. Они могут быть использованы для отправки и получения шифрованной электронной почты через Интернет. Чтобы получить сертификат этого класса, пользователь должен сообщить серверу Verisign свой адрес электронной почты или свое уникальное имя.
- **Сертификаты класса 2** дают возможность их владельцу пользоваться внутрикорпоративной электронной почтой и принимать участие в подписных интерактивных службах. Чтобы получить сертификат этого более высокого уровня, пользователь должен организовать подтверждение своей личности сторонним лицом, например своим работодателем. Такой сертификат с информацией от работодателя может быть эффективно использован для деловой корреспонденции.
- **Сертификаты класса 3** предоставляют владельцу все те возможности, которые имеет обладатель сертификата класса 2, плюс возможность участия в электронных банковских операциях, электронных сделках по покупке товаров и некоторые другие возможности. Для доказательства своей аутентичности соискатель сертификата должен явиться лично и предоставить подтверждающие документы.
- **Сертификаты класса 4** используются при выполнении крупных финансовых операций. Поскольку такой сертификат наделяет владельца самым высоким уровнем доверия, сертифицирующий центр Verisign проводит тщательное изучение частного лица или организации, запрашивающей сертификат.

Сертифицирующие центры

- Механизм получения пользователем сертификата хорошо автоматизируется в сети в модели клиент-сервер, когда браузер выполняет роль клиента, а в сертифицирующей организации установлен специальный сервер выдачи сертификатов.
- Браузер вырабатывает для пользователя пару ключей, оставляет закрытый ключ у себя и передает частично заполненную форму сертификата серверу. Для того чтобы неподписанный еще сертификат нельзя было подменить при передаче по сети, браузер ставит свою электронную подпись, зашифровывая сертификат выработанным закрытым ключом.
- Сервер сертификатов подписывает полученный сертификат, фиксирует его в своей базе данных и возвращает его каким-либо способом владельцу. Очевидно, что при этом может выполняться еще и неформальная процедура подтверждения пользователем своей личности и права на получение сертификата, требующая участия оператора сервера сертификатов. Это могут быть доказательства оплаты услуги, доказательства принадлежности к той или иной организации — все случаи жизни предусмотреть и автоматизировать нельзя.
- После получения сертификата браузер сохраняет его вместе с закрытым ключом и использует при аутентификации на тех серверах, которые поддерживают такой процесс.

8.4. Аутентификация информации

- Под аутентификацией информации в компьютерных системах понимают установление подлинности данных, полученных по сети, исключительно на основе информации, содержащейся в полученном сообщении.
- Если конечной целью шифрования информации является обеспечение защиты от несанкционированного ознакомления с этой информацией, то конечной целью аутентификации информации является обеспечение защиты участников информационного обмена от навязывания ложной информации.
- Концепция аутентификации в широком смысле предусматривает установление подлинности информации как при условии наличия взаимного доверия между участниками обмена, так и при его отсутствии.

8.4. Аутентификация информации

В компьютерных системах выделяют два вида аутентификации информации:

- аутентификация хранящихся массивов данных и программ — установление того факта, что данные не подвергались модификации;
- аутентификация сообщений — установление подлинности полученного сообщения, в том числе решение вопроса об авторстве этого сообщения и установление факта приема.

9. Цифровая подпись

- Для решения задачи аутентификации информации используется концепция цифровой (или электронной) подписи.
- «Цифровая подпись» — методы , позволяющие устанавливать подлинность автора сообщения (документа) при возникновении спора относительно авторства этого сообщения.
- Основная область применения цифровой подписи — это финансовые документы, сопровождающие электронные сделки, документы, фиксирующие международные договоренности и т. п.

9. Цифровая подпись

- До настоящего времени наиболее часто для построения схемы цифровой подписи использовался алгоритм RSA.
- В основе этого алгоритма лежит концепция Диффи-Хеллмана.
- Она заключается в том, что каждый пользователь сети имеет свой закрытый ключ, необходимый для формирования подписи; соответствующий этому секретному ключу открытый ключ, предназначенный для проверки подписи, известен всем другим пользователям сети.
- На рис. 6.9 показана схема формирования цифровой подписи по алгоритму RSA.
- Подписанное сообщение состоит из двух частей: *незашифрованной части*, в которой содержится исходный текст T, и *зашифрованной части*, представляющей собой цифровую подпись.

9. Цифровая подпись

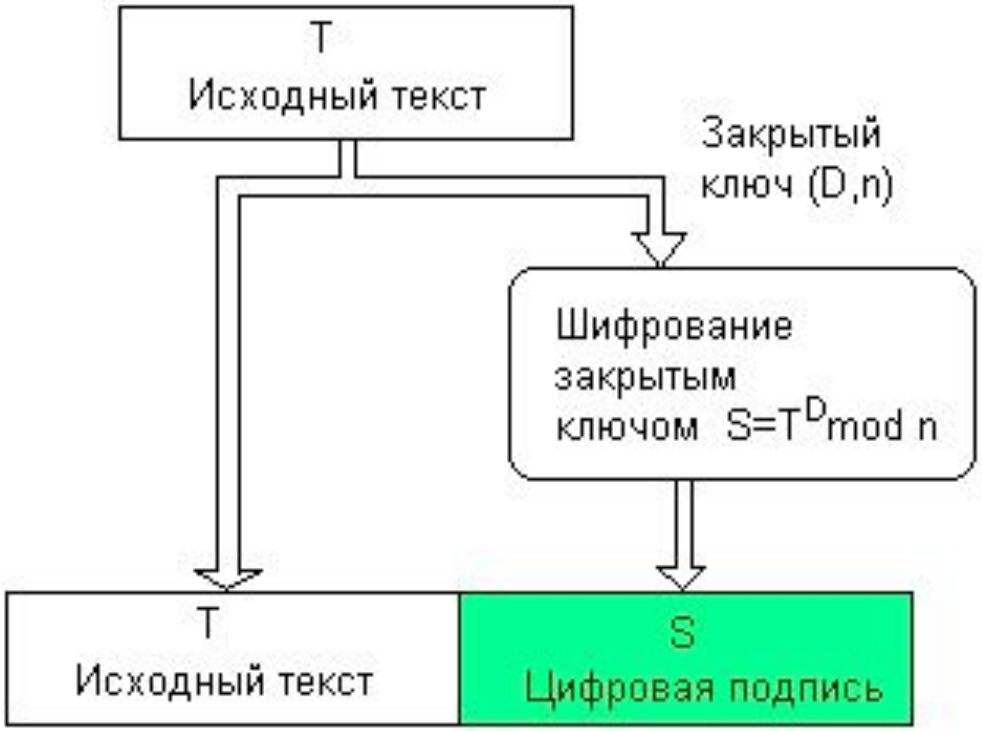

Рис. 6.9. Схема формирования цифровой подписи по алгоритму RSA

9. Цифровая подпись

- Если результат расшифровки цифровой подписи совпадает с открытой частью сообщения, то считается, что документ подлинный, не претерпел никаких изменений в процессе передачи, а автором его является именно тот человек, который передал свой открытый ключ получателю.
- Если сообщение снабжено цифровой подписью, то получатель может быть уверен, что оно не было изменено или подделано по пути.
- Такие схемы аутентификации называются асимметричными.
- К недостаткам данного алгоритма можно отнести то, что длина подписи в этом случае равна длине сообщения, что не всегда удобно.

9. Цифровая подпись

- Цифровые подписи применяются к тексту до того, как он шифруется.
- Если помимо снабжения текста электронного документа цифровой подписью надо обеспечить его конфиденциальность, то вначале к тексту применяют цифровую подпись, а затем шифруют все вместе: и текст, и цифровую подпись.
- Другие методы цифровой подписи основаны на формировании соответствующей сообщению контрольной комбинации с помощью классических алгоритмов типа DES.
- Учитывая более высокую производительность алгоритма DES по сравнению с алгоритмом RSA, он более эффективен для подтверждения аутентичности больших объемов информации.
- А для коротких сообщений типа платежных поручений или квитанций подтверждения приема, лучше подходит алгоритм RSA.

10. Аутентификация программных кодов

- Компания Microsoft разработала средства для доказательства аутентичности программных кодов, распространяемых через Интернет.
- Пользователю важно иметь доказательства, что программа, которую он загрузил с какого-либо сервера, действительно содержит коды, разработанные определенной компанией.
- Протоколы защищенного канала типа SSL помочь здесь не могут, так как позволяют удостоверить только аутентичность сервера. Microsoft разработала технологию аутентикода (Authenticode), суть которой сострит в следующем.
- Организация, желающая подтвердить свое авторство на программу, должна встроить в распространяемый код так называемый подписывающий блок (рис. 6.10).
- Этот блок состоит из двух частей:
  - сертификат этой организации, полученный обычным образом от какого-либо, сертифицирующего центра.
  - зашифрованный дайджест, полученный в результате применения односторонней функции к распространяемому коду. Шифрование дайджеста выполняется с помощью закрытого ключа организации.

10. Аутентификация программных кодов

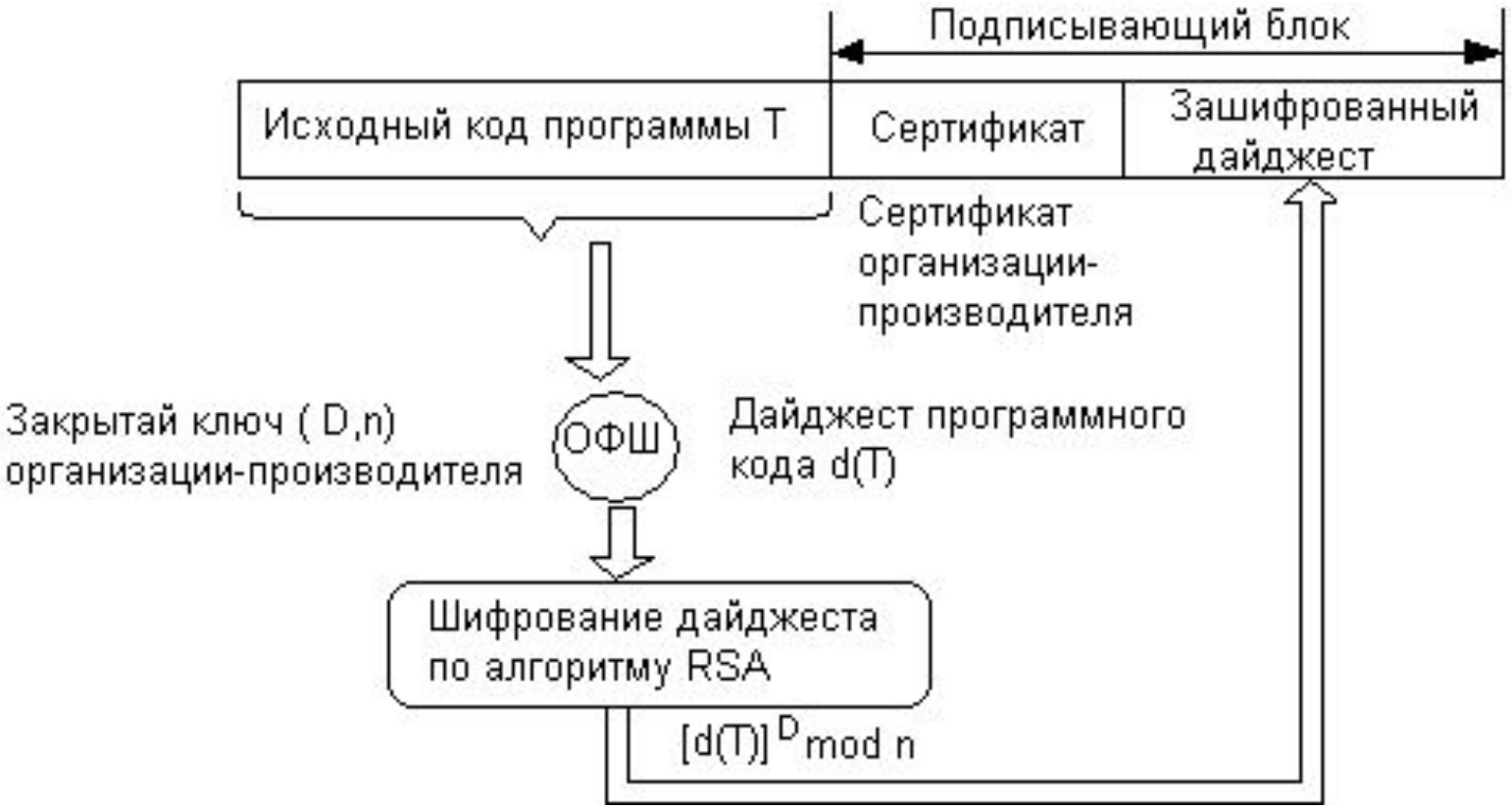

Рис. 6.10. Схема получения аутентикода