Аппаратное и программное обеспечение ЭВМ и сетей

Тема_6-36_Сетевая безопасность. Шифрование . Аутентификация, авторизации, аудит

Методы обеспечения информационной безопасности

Обеспечение информационной безопасности — это деятельность, направленная на достижение состояния защищенности информационной среды, прогнозирование, предотвращение и смягчение последствий воздействий, результатом которых может явиться нанесение ущерба информации, ее владельцам или поддерживающей инфраструктуре.

Методы обеспечения информационной безопасности:

- **технические средства;**
- **«не технические»** (юридические, административные);
- **физические средства защиты.**

Различные средства защиты должны применяться совместно и под централизованным управлением.

Методы обеспечения информационной безопасности

- ***Общие принципы безопасности:***

1. Комплексный подход.
2. Многоуровневая защита.
3. Предоставление сотруднику минимально достаточного уровня привилегий.
4. Принцип единого контрольно-пропускного пункта (весь входящий и исходящий трафик проходит через единственный узел сети).
5. Использование только таких средств, которые при **отказе переходят в состояние максимальной защиты.**
6. Баланс возможного ущерба от реализации угрозы и затрат на ее предотвращение.

Шифрование

Шифрование — это средство обеспечения конфиденциальности данных, хранящихся в памяти компьютера или передаваемых по сети.

Пара процедур — шифрование и дешифрирование — называется криптосистемой, предусматривающей наличие секретного ключа.

Классы криптосистем:

- **Симметричные**. Секретный ключ шифрования совпадает с секретным ключом дешифрирования. В
- **Асимметричные**. Открытый ключ шифрования не совпадает с секретным ключом дешифрирования.

Шифрование

Алгоритм DES

- Наиболее популярный симметричный алгоритмом — DES (Data Encryption Standard), разработанный фирмой IBM.
- Открытый текст шифруется блоками по 64 бита.
- Алгоритм состоит из 19 этапов:

  1) Независимая перестановка 64 разрядов открытого текста.

  2-17) 64-разрядный блок делится пополам на левую (L_{i-1}) и правую (R_{i-1}) части. Правая часть вычисляется с помощью функции $f(L_{i-1}, Ki)$, где Li-1 — исходная левая часть:

  a) из 32 разрядов правой части, с помощью фиксированной перестановки и дублирования формируется 48-разрядное число E;

  b) число E и ключ Ki- складываются по модулю 2;

  c) выход разделяется на восемь групп по шесть разрядов, каждая из которых преобразуется независимым S-блоком в 4-разрядные группы;

  d) эти 8 · 4 разряда пропускаются через P- блок.

  18) Меняет местами левые и правые 32 разряда.

  19) Обратная перестановка.

- На каждом из 16 этапов используются различные функции исходного ключа.
- Этапы при расшифровке выполняются в обратном порядке.

Шифрование

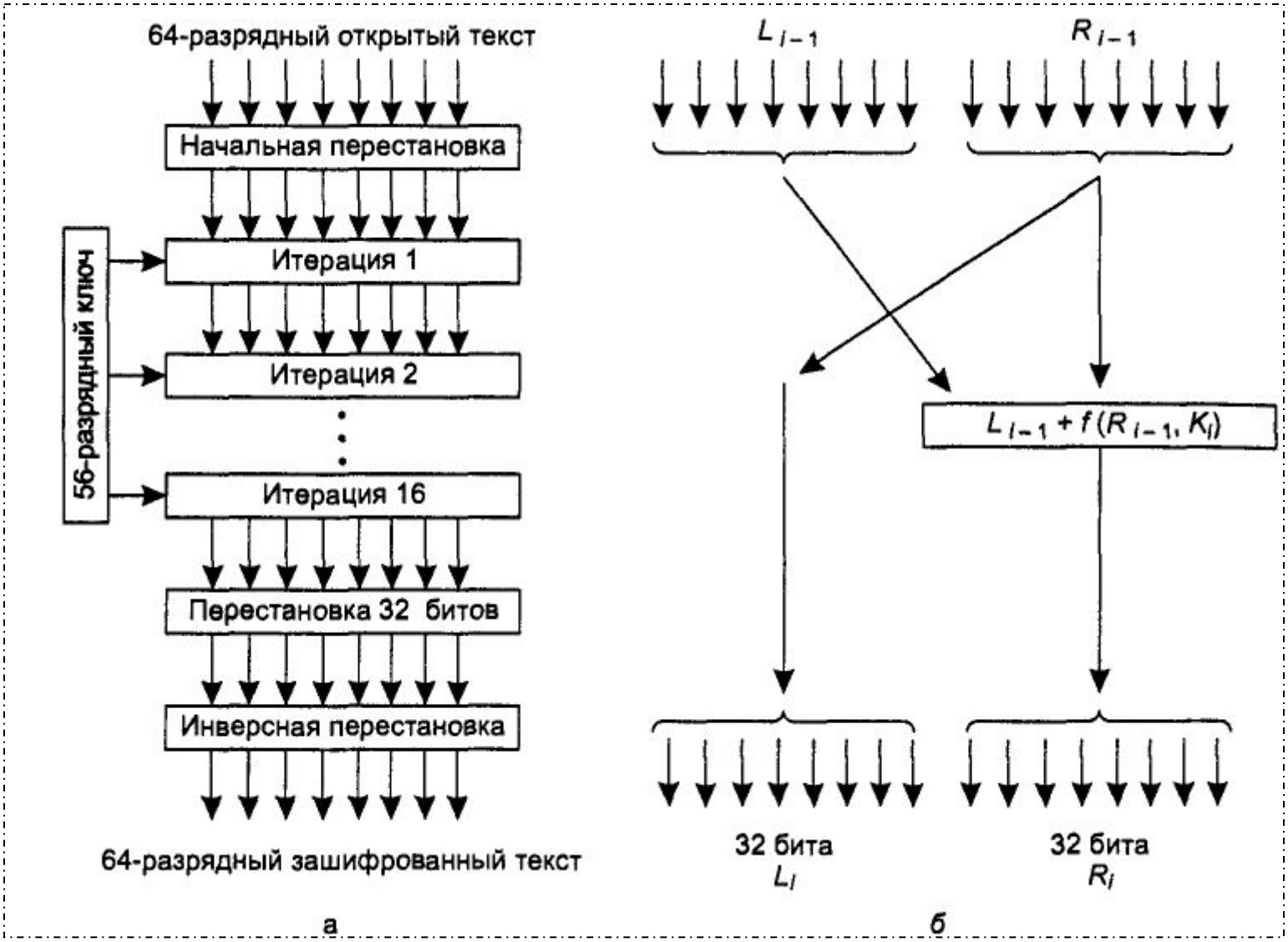


Рис. 6.36-2. Стандарт шифрования данных DES: общий вид (а); детализация одного из этапов (б)

Шифрование ***Алгоритм DES***

Начальная перестановка

Исходный текст T (блок 64 бит) преобразуется с помощью начальной перестановки IP которая определяется таблицей:

По таблице первые 3 бита результирующего блока IP(T) после начальной перестановки IP являются битами 58, 50, 42 входного блока T, а его 3 последние бита являются битами 23, 15, 7 входного

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Шифрование ***Алгоритм DES***

Циклы шифрования

Полученный после начальной перестановки 64-битовый блок IP(T) участвует в 16-циклах преобразования Фейстеля.

16 циклов преобразования Фейстеля:

Разбить IP(T) на две части L0,R0, где L0,R0 — соответственно 32 старших битов и 32 младших битов блокаT0 IP(T)= L0R0

Пусть Ti − 1 = Li − 1Ri − 1 результат (i-1) итерации, тогда результат i-ой итерации Ti = LiRi определяется:

Li = Ri − 1

Левая половина Li равна правой половине предыдущего вектора Li − 1Ri − 1. А правая половина Ri — это битовое сложение Li − 1 и f(Ri − 1,ki) по модулю 2. В 16-циклах преобразования Фейстеля функция f играет роль шифрования.

Конечная перестановка

Конечная перестановка IP − 1 действует на T16 и используется для восстановления позиции. Она является обратной к перестановке IP. Конечная перестановка определяется таблицей:

Шифрование ***Алгоритм DES***

Конечная таблица перестановок.

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Шифрование

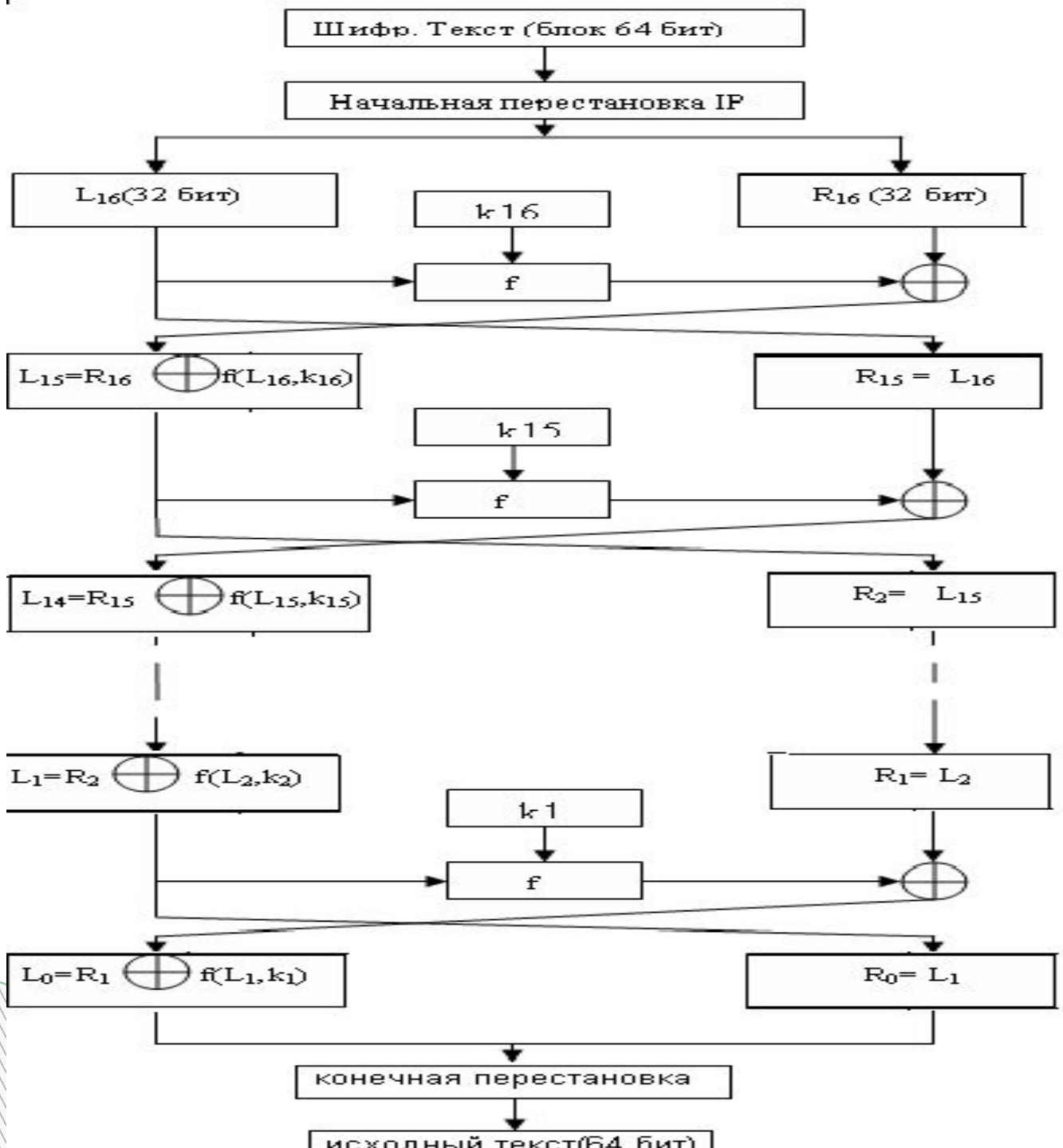
При расшифровании данных все действия выполняются в обратном порядке. В 16 циклах расшифрования, в отличие от шифрования с помощью прямого преобразования сетью Фейстеля, здесь используется обратное преобразование сетью Фейстеля.

$Ri - 1 = Li$

Схема расшифрования указана на рисунке справа.

Ключ ki, i=1,…,16, функция f, перестановка IP и $IP - 1$ такие же как и в процессе шифрования.

Схема расшифрования



Шифрование

- В 2001 году был разработан стандарт симметричного шифрования AES (Advanced Encryption Standard), в основу которого положен алгоритм Rijndael.
- AES обеспечивает лучшую защиту, так как также может работать со 128-, 192- и 256-битными ключами и имеет высокую скорость работы, кодируя за один цикл 128-битный блок в отличие от 64-битного блока DES.

- В симметричных алгоритмах главную проблему представляют ключи: например, в системе с n абонентами требуется $n \times (n - 1)/2$ ключей, сгенерированных и распределенных надежным образом.
- Несимметричные алгоритмы снимают эту проблему.

Шифрование

Односторонние функции шифрования

- Во многих технологиях безопасности используется шифрование с помощью односторонней функции (хэш-функции, дайджест-функции).
- Эта функция дает значение, называемое дайджестом, которое состоит из небольшого и не зависящего от длины шифруемого текста числа байтов (16-20).
- Знание дайджеста позволяет проверить целостность данных.
- В отличие от контрольной суммы дайджест вычисляется с использованием секретного ключа, известного только отправителю и получателю, т.е. любая модификация исходного сообщения будет обнаружена.
- Дайджест может быть использован в качестве электронной подписи для аутентификации передаваемого документа.
- Такого рода функции должны удовлетворять двум условиям:
  - по дайджесту должно быть невозможно вычислить исходное сообщение;
  - должна отсутствовать возможность вычисления двух разных сообщений, для которых могли быть вычислены одинаковые дайджесты.

Шифрование

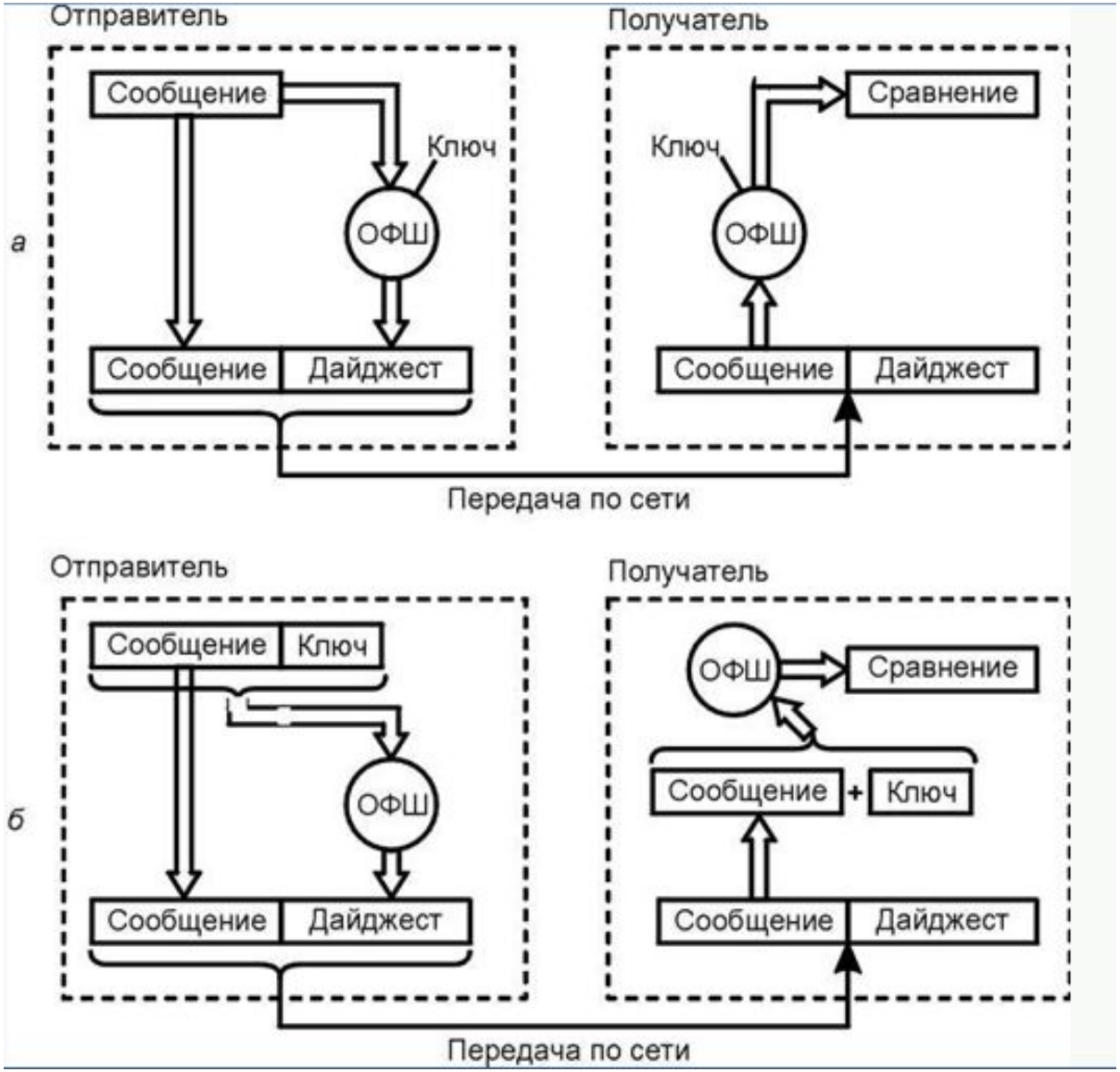


Рис. 6.36 6. Использование односторонних функций шифрования для контроля целостности

Шифрование

- На рис. 6.36-6, б показан другой вариант использования односторонней функции шифрования для обеспечения целостности данных. Здесь односторонняя функция не имеет параметра-ключа, но зато применяется не просто к сообщению, а к сообщению, дополненному секретным ключом.
- 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.

Аутентификация, авторизации, аудит

Понятие аутентификации

Аутентификация — это процедура установления подлинности, применимая как к людям, так и другим объектам (программам, устройствам, документам).

- Доказательства аутентичности:
  - знание общего для обеих сторон секрета: слова или факта;
  - владение уникальным предметом, например, электронной магнитной картой;
  - био- характеристики: рисунок радужной оболочки глаза, отпечатки пальцев.

- Для снижения угрозы раскрытия и разгадывания паролей применяют задание максимального и минимального сроков действия пароля, хранение списка уже использованных паролей, управление поведением системы после нескольких неудачных попыток входа и т. п.

Аутентификация, авторизации, аудит

- **Аутентификация на уровне приложений.**
- Пользователь, обращающийся к веб-серверу, должен доказать свою легальность и убедиться, что ведет диалог с веб-сервером своего предприятия. То есть пройти процедуру взаимной аутентификации.
- При установлении связи между двумя устройствами предусматриваются процедуры взаимной аутентификации устройств на канальном уровне.
- Аутентификация данных — доказательство целостности данных и того, что они поступили от того человека.

Аутентификация, авторизации, аудит

Авторизация доступа

- Авторизация — предоставление каждому пользователю именно тех прав, которые ему были определены администратором.

- Классы правил доступа:
  - Избирательный. Определенные операции разрешаются или запрещаются пользователям или группам пользователей, явно указанным своими идентификаторами.
  - Мандатный. Вся информация делится на уровни секретности. Пользователи также делятся на группы в соответствии с уровнем допуска к этой информации. Пользователи более высокого уровня не могут изменить уровень доступности информации для пользователей более низкого уровня.

- Системы аутентификации и авторизации могут строиться на базе двух схем:
  - Централизованная, базирующаяся на сервере. Пользователь логически входит в сеть и получает на все время работы набор разрешений по доступу к ресурсам сети.
  - Децентрализованная. Средства авторизации работают на каждой машине.

Аутентификация, авторизации, аудит

Аудит

- Аудит — набор процедур мониторинга и учета всех событий, представляющих потенциальную угрозу для безопасности системы.
- Если кто-то пытается выполнить действия, выбранные системой безопасности для мониторинга, то система аудита пишет сообщение в журнал регистрации, идентифицируя пользователя.
- Эта информация позволяет предотвратить повторение атак путем устранения уязвимых мест в системе защиты.

Аутентификация, авторизации, аудит

Строгая аутентификация на основе многоразового пароля в протоколе CHAP

- Протокол аутентификации по квитированию вызова (Challenge Handshake Authentication Protocol, CHAP) используется, например, при аутентификации удаленных пользователей, подключенных к Интернету по коммутируемому каналу.
- При заключении договора клиент получает от провайдера пароль (parol), который хранится в базе данных провайдера в виде дайджеста Z = d(parol).

- Аутентификация:
  - 1. Клиент активизирует программу удаленного доступа к серверу провайдера, вводя имя и пароль. Имя («Moscow») передается провайдеру в составе запроса на соединение.
  - 2. Сервер, получив запрос, генерирует псевдослучайное слово-вызов («challenge») и передает его клиенту вместе со значением, идентифицирующем сообщение в рамках данного сеанса (ID), и собственным именем (здесь «Paris»). Это сообщение типа Challenge (вызов).
  - 3. Программа клиента извлекает слово-вызов, добавляет к нему идентификатор и вычисленный локально дайджест Z = d/(parol), вычисляет дайджест Y= d{(ID), challenge,Z} и посылает серверу провайдера в пакете Response (ответ).
  - 4. Сервер сравнивает полученный дайджест Y со значением, которое он получил, локально применив ту же хэш-функцию к компонентам, хранящимся в его памяти.
  - 5. Если результаты совпадают, то аутентификация считается успешной и аутентификатор посылает партнеру пакет Success (успех). В противном случае, Failure (ошибка).

Аутентификация, авторизации, аудит

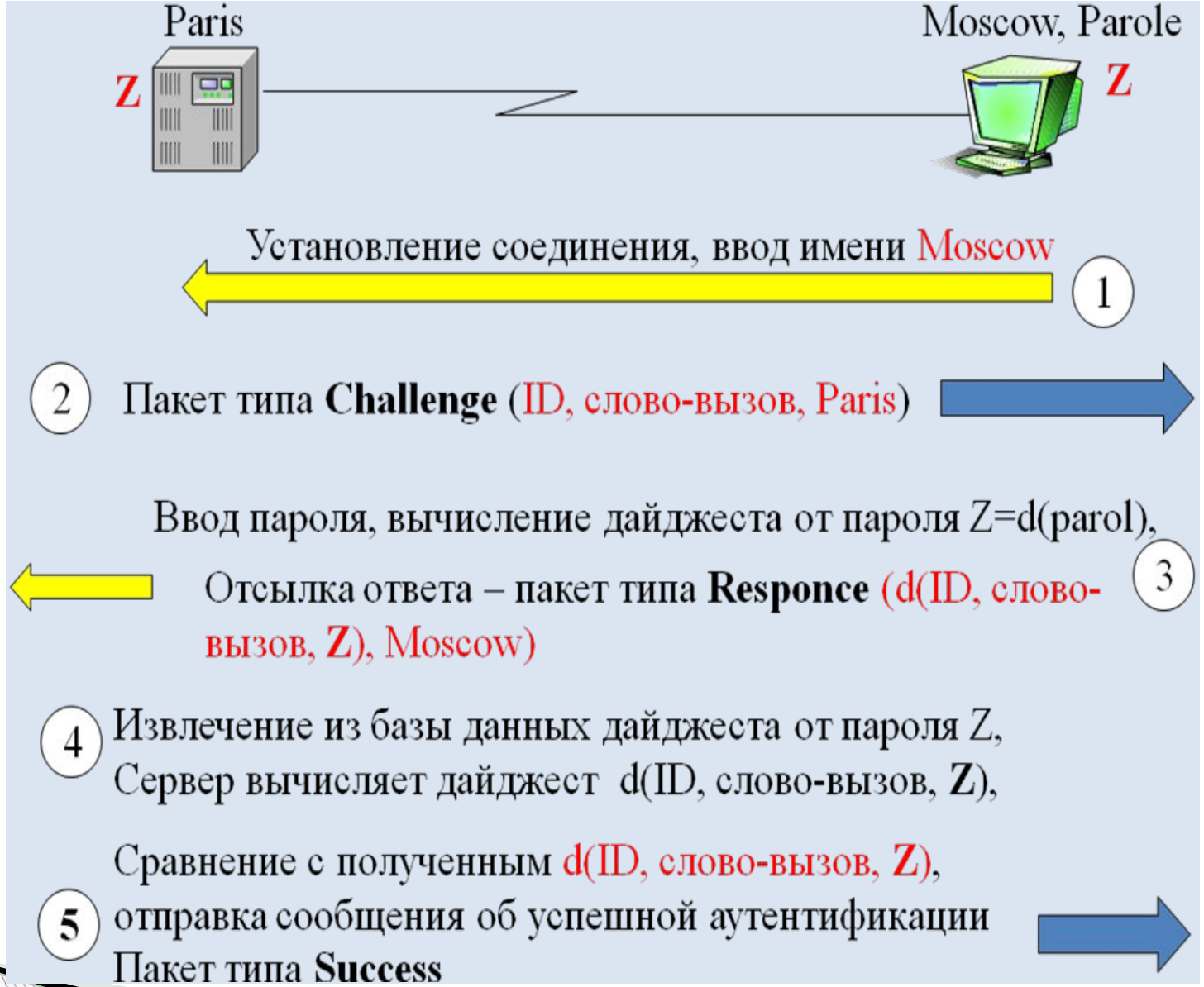


Рис. 6.36-7. Аутентификация по протоколу CHAP

Аутентификация, авторизации, аудит

Аутентификация на основе одноразового пароля

- Генерацию одноразовых паролей могут выполнять:
- - аппаратные ключи, представляющие собой миниатюрные устройства со встроенным микропроцессором, похожие либо на пластиковые карточки, либо на карманные калькуляторы, либо в виде присоединяемого к разъему компьютера устройства.
- - программные ключи — программы с генератором одноразовых паролей, размещенная на внешнем носителе.

Пользователь сообщает системе свой идентификатор и указывает последовательность цифр, сообщаемую ему аппаратным или программным ключом. Затем генерируется новый пароль. Сервер аутентификации проверяет введенную последовательность и разрешает пользователю осуществить логический вход.

Аутентификация, авторизации, аудит

Аутентификация на основе сертификатов

- Применяется, когда число пользователей сети (пусть и потенциальных) измеряется миллионами.
- Сеть не хранит информацию о своих пользователях — они ее предоставляют сами в запросах в виде сертификатов, удостоверяющих личность пользователей.
- Сертификаты выдаются специальными уполномоченными организациями — центрами сертификации (**Certificate Authority, CA**).

- Сертификат представляет собой электронную форму, в которой содержится следующая информация:

1. открытый ключ владельца данного сертификата;
2. сведения о владельце (имя, адрес электронной почты и т. п.);
3. наименование организации, выдавшей сертификат;
4. электронная подпись сертифицирующей организации.

Аутентификация, авторизации, аудит

- Пользователь предъявляет сертификат в **двух формах**: ***открытой*** и ***зашифрованной*** с применением своего закрытого ключа (рис. 6.36-11).
- Аутентификатор берет из незашифрованного сертификата открытый ключ и расшифровывает зашифрованный сертификат. Совпадение подтверждает, что предъявитель является владельцем закрытого ключа, соответствующего открытому.
- С помощью открытого ключа организации проводится расшифровка ее подписи. Если получается тот же сертификат с тем же именем пользователя и его открытым ключом, значит, он является тем, за кого себя выдает.

- Сертификаты можно использовать для предоставления избирательных прав доступа. Для этого в него вводятся дополнительные поля, в которых указывается принадлежность владельцев к той или иной категории пользователей.

Сертифицирующие центры

- 1) Задачу обеспечения сотрудников сертификатами может взять на себя само предприятие. В этом случае упрощается процедура первичной аутентификации при выдаче сертификата.
- 2) Независимые центры по выдаче сертификатов (например, сертифицирующий центр компании Verisign).

Аутентификация, авторизации, аудит

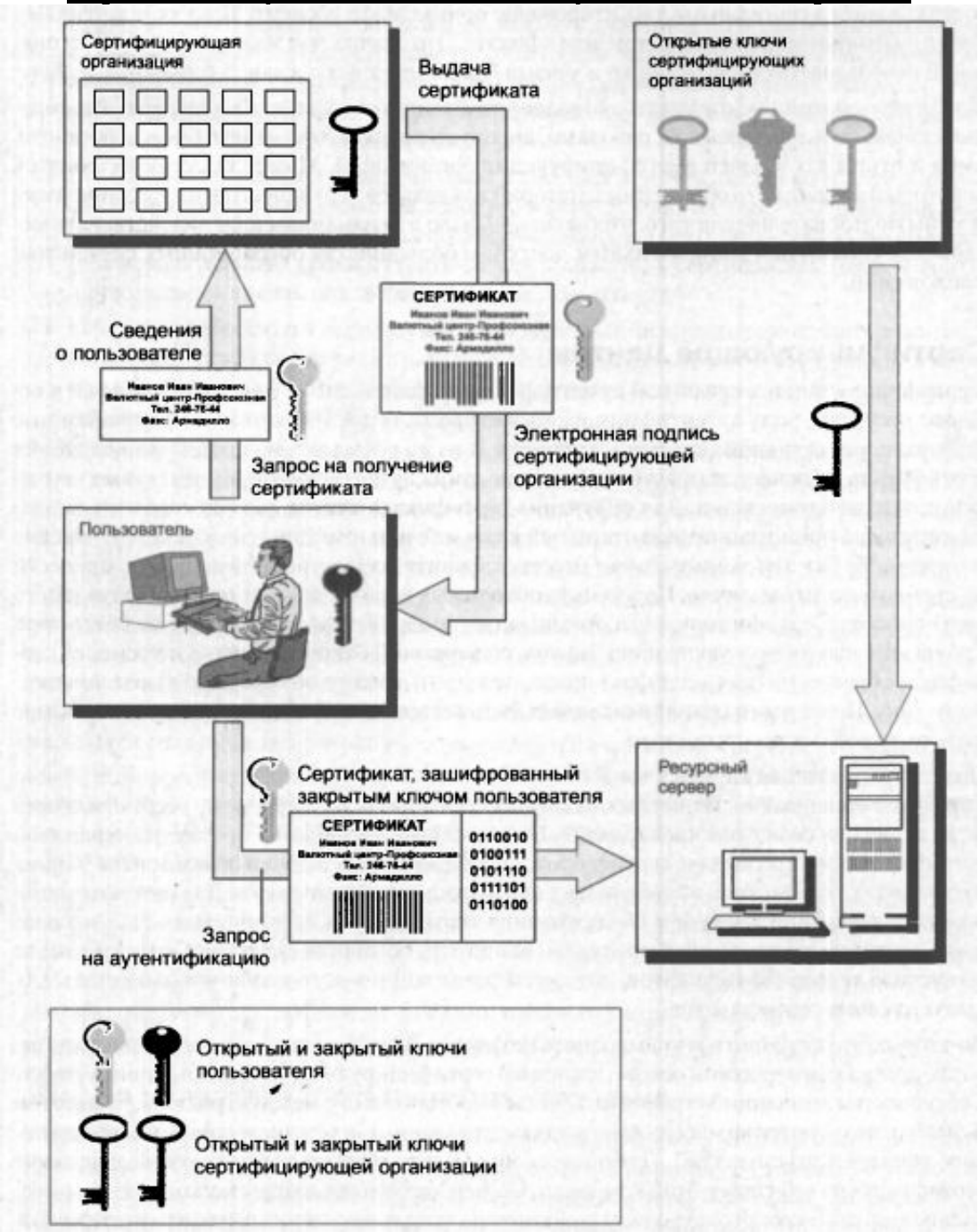


Рис. 6.36-11. Аутентификация пользователей на основе сертификатов

Аутентификация, авторизации, аудит

Классы сертификатов:

- Класс 1. Предоставляют самый низкий уровень полномочий (отправка и получение электронной почты через Интернет)
- Класс 2. Дают возможность его владельцу пользоваться внутрикорпоративной электронной почтой и принимать участие в подписных интерактивных службах.
- Класс 3. Предоставляют возможности класса 2 плюс возможность участия в электронных банковских операциях, электронных сделках и др.
- Класс 4. Используются при выполнении крупных финансовых операций.

Аутентификация, авторизации, аудит

Аутентификация информации

- Аутентификация информации — установление подлинности полученных по сети данных исключительно на основе информации, содержащейся в полученном сообщении.
- Ее цель — защита участников информационного обмена от навязывания ложной информации.

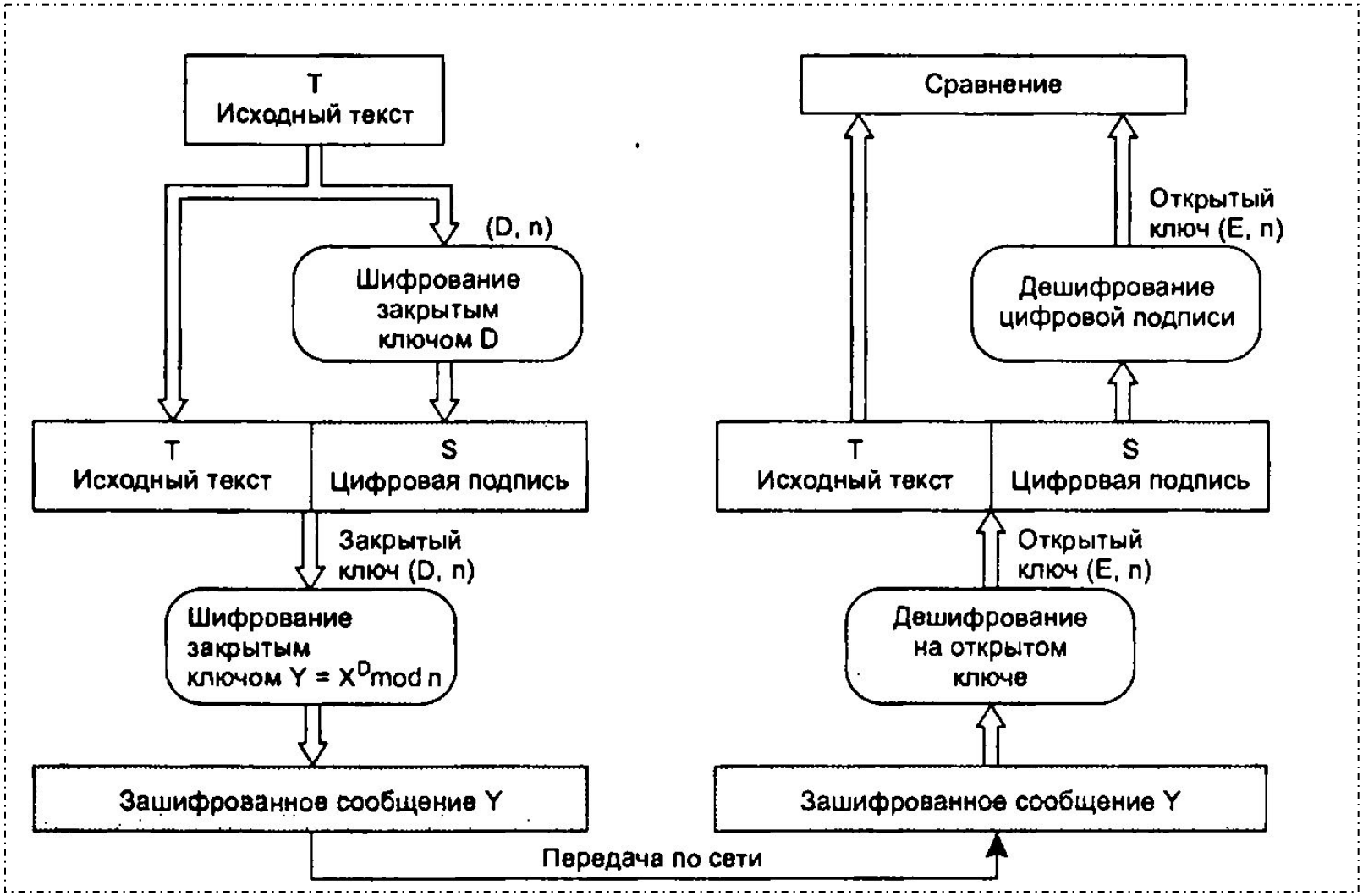
- Виды аутентификации информации:
  - аутентификация хранящихся массивов данных и программ — установление факта того, что данные не подвергались модификации;
  - аутентификация сообщений — установление подлинности полученного сообщения.

Аутентификация, авторизации, аудит

Цифровая подпись

- Цифровая подпись — методы, позволяющие устанавливать подлинность автора сообщения (документа) при возникновении спора относительно авторства.
- Чаще всего для построения схемы цифровой подписи используются алгоритмы RSA и DES.
- DES более эффективен для подтверждения аутентичности больших объемов информации. А для коротких сообщений (платежных поручений, квитанций) лучше подходит алгоритм RSA.

Аутентификация, авторизации, аудит



- Рис. 6.36-14. Обеспечение конфиденциальности документа с цифровой подписью

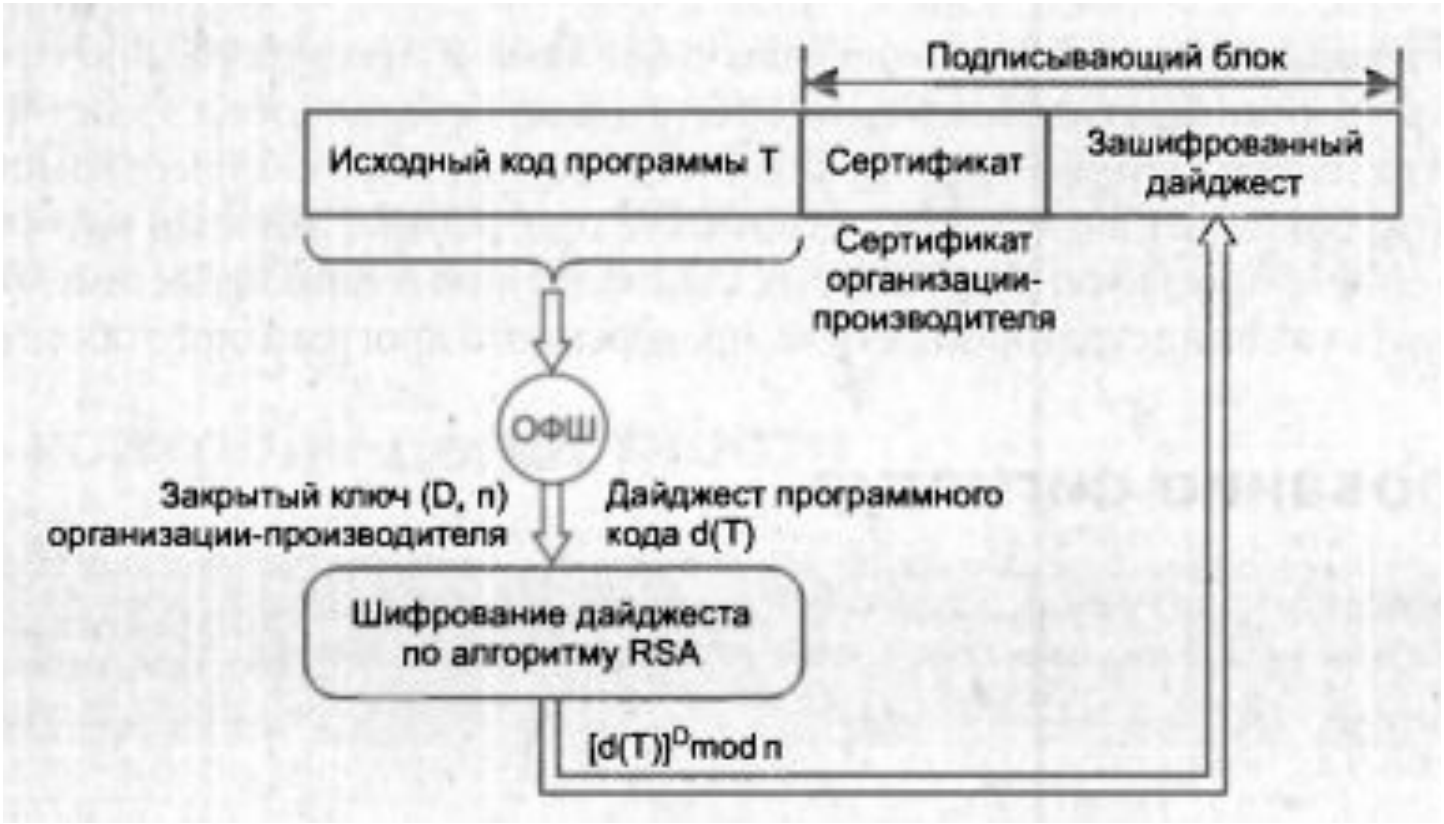
Аутентификация, авторизации, аудит

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.

- Организация, желающая подтвердить свое авторство на программу, должна встроить в распространяемый код подписывающий блок (рис. 6.36-15).
- Этот блок состоит из двух частей: сертификата этой организации и дайджеста, зашифрованного с помощью закрытого ключа организации.

Аутентификация, авторизации, аудит



- Рис. 6.36-15. Схема получения аутентикода

Список использованных источников

- В.Г. Олифер, Н.А. Олифер Компьютерные сети, 3-е издание, 2009г.