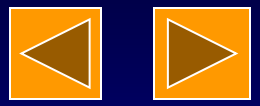
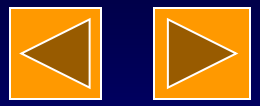
Операционные среды, системы и оболочки

Тема 6. Безопасность, диагностика и восстановление ОС после отказов

Автор : доктор технических наук, профессор Назаров С.В.





6.7. Базовые технологии безопасности

6.7.1. Шифрование

6.7.2. Аутентификация, пароли, авторизация, аудит

6.7.3. Технология защищенного канала

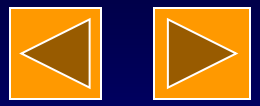
6.8. Технологии аутентификации

6.8.1. Сетевая аутентификация на основе многоразового пароля

6.8.2. Аутентификация с использованием одноразового пароля

6.8.3. Аутентификация информации

6.9. Система Kerberos



6.1. Понятие безопасности. Требования безопасности

Безопасность – совокупность проблем, связанных с использованием информации для решения задач пользователей компьютерной системы

Безопасность информационных систем включает:

1) безопасность отдельных компьютеров – защита данных, хранящихся и обрабатывающихся компьютером, рассматриваемым как автономная система; 2) сетевая безопасность – защита данных при передаче по линиям связи и защита от несанкционированного доступа в сеть

Безопасной является система, удовлетворяющая следующим требованиям:

1. Конфиденциальность – гарантия того, что информация будет доступна только авторизованным пользователям (легальным).

2. Целостность – гарантия сохранности данными правильных значений.

3. Доступность – постоянная готовность системы к обслуживанию авторизованных пользователей.

4. Аутентичность – способность системы проверять идентичность пользователя.

Защита информации от несанкционированного доступа – одна из главных задач операционных систем

6.2. Угрозы безопасности. Классификация

Угроза – любое действие, направленное на нарушение конфиденциальности, целостности и/или доступности информации, а также нелегальное использование ресурсов информационной системы.

Атака – реализованная угроза.

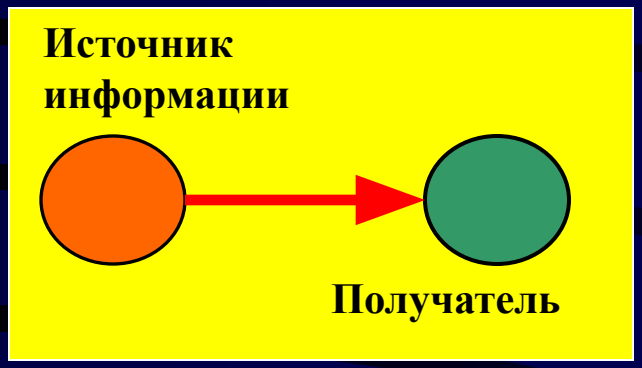
Риск – вероятностная оценка величины возможного ущерба в результате успешно проведенной атаки.

Неумышленные угрозы – угрозы, вызванные ошибочными действиями лояльных сотрудников по причине их низкой квалификации или безответственности, а также последствиями ненадежной работы аппаратных и программных средств компьютерной системы, в том числе операционной системы.

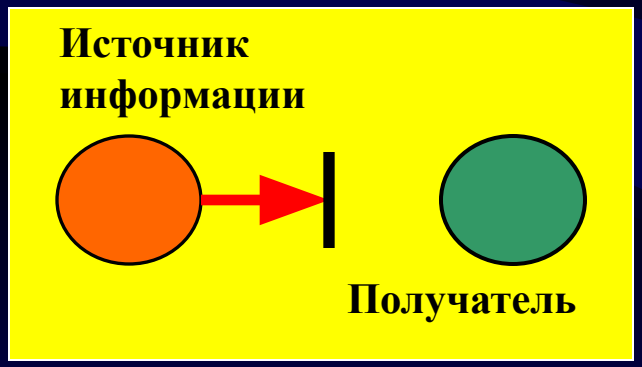
Умышленные угрозы – пассивное чтение данных, мониторинг системы, активные действия – нарушение целостности и доступности информации, приведение в нерабочее состояние приложений и устройств системы.

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.

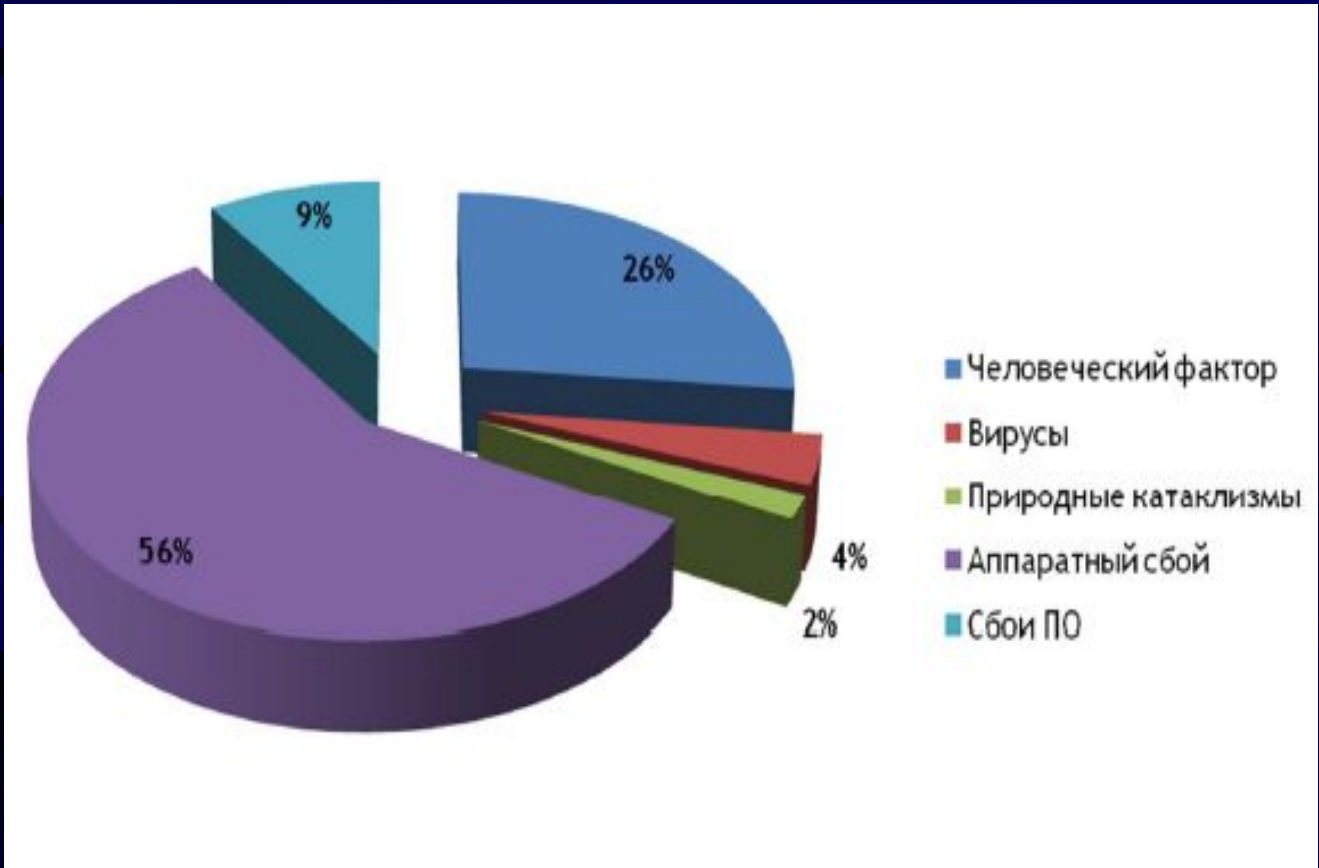


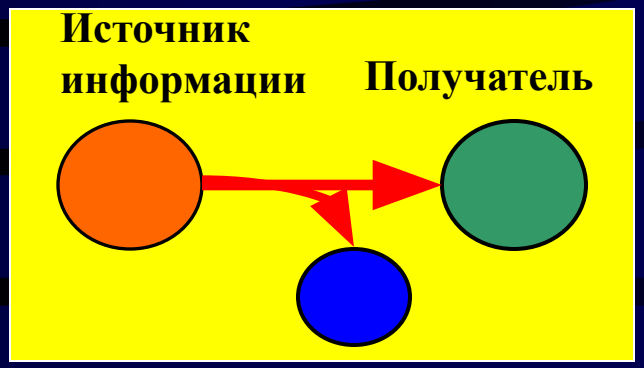
Нормальная передача. Информации от источника информации к получателю.



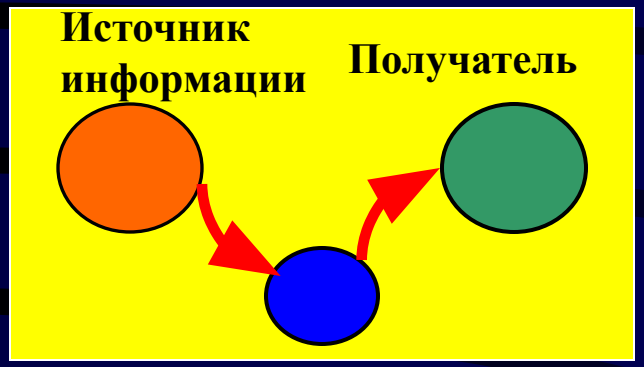
Прерывание. Компоненты системы выходят из строя, становятся недоступными или непригодными. Это атака , целью которой является **нарушение доступности.**

Причины потери данных

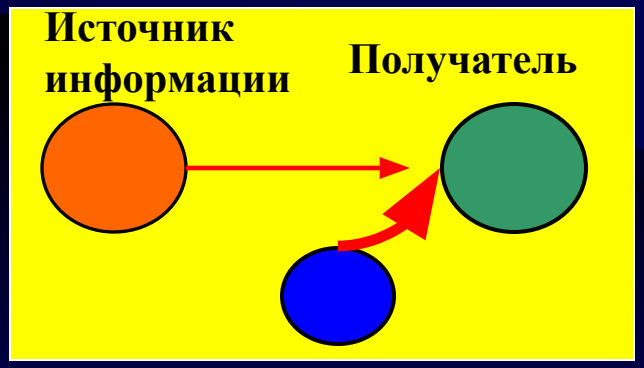




Перехват. Это атака, целью которой является нарушение конфиденциальности, в результате чего доступ к компонентам системы получают несанкционированные стороны



Изменение. Несанкционированная сторона не только получает доступ к системе, но и вмешивается в работу ее компонентов. Целью атаки является нарушение целостности.



Подделка. Несанкционированная сторона помещает в систему поддельные объекты. Целью этой атаки является нарушение аутентичности.

6.2.1. Атаки изнутри системы. Злоумышленники. Взломщики

Злоумышленник – нелегальный пользователь, сумевший зарегистрироваться в системе. **Пассивный злоумышленник** пытается прочитать то, что ему не положено. **Активный злоумышленник** пытается незаконно изменить данные с различными целями, вплоть до разрушения системы (хакеры, кракеры).

Категории злоумышленников (по нарастанию негативных последствий):

1. Случайные любопытные пользователи, не применяющие специальных технических и программных средств.
2. Притворщик – лицо, не обладающее полномочиями по использованию компьютера, проникающее систему путем использования учетной записи законного пользователя.
3. Правонарушитель – законный пользователь, получающий доступ к ресурсам, к которым у него нет доступа, или тот, у которого есть такой доступ, но он злоупотребляет своими привилегиями.
4. Тайный пользователь – лицо, завладевшее управлением в режиме суперпользователя и использующее его, чтобы избежать аудита и преодолеть контроль доступа.
5. Лица, занимающиеся коммерческим или военным шпионажем.
6. Взломщики.

Защита пользовательских паролей

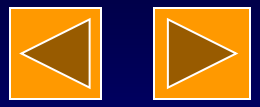
- Одностороннее (необратимое) шифрование. Пароль используется для генерации ключа для функции шифрования.

- Контроль доступа к файлу с паролями. Доступ ограничен одной учетной записью или малым числом учетных записей (администраторы).

6.2.2. Методы вторжения

1. Попытка применить пароли стандартных учетных записей, которые устанавливаются по умолчанию (например, Guest).
2. Настойчивый перебор всех коротких паролей.
3. Перебор слов из подключенного к системе или специального списка слов, чаще всего применяемых в качестве пароля.
4. Сбор такой информации о пользователях, как их полные имена, имена супругов и детей, названия книг в офисе, хобби пользователей.
5. Использование в качестве вероятного пароля дат рождения , номеров комнат, номеров различных удостоверений и т. д.
6. Использование в качестве вероятного пароля номеров автомобилей.

7. Обход ограничений доступа с помощью троянских коней.
8. Перехват сообщений, которыми обмениваются удаленный пользователь и узел системы. Комбинация автодозвона и алгоритма подбора паролей. Атака по Интернету (перебор IP-адресов, ping w.x.y.z - соединение через telnet w.x.y.z + перебор порта – подбор имен и паролей – сбор статистики – суперпользователь – сетевой анализатор пакетов – и т. д.).



ПОЛЬЗОВАТЕЛИ и ИХ ИДЕНТИФИКАТОРЫ

Управление и контроль доступа

"Как мой бизнес может выиграть от управления цифровыми ID?"

Ситуации

- Непонимание задач управления ID
- Цена администрирования пользователей и их ID силами компании
- Невозможность контроля привилегированных пользователей
- Использование идентификаторов уволенных сотрудников или общих учетных записей
- Прохождение аудита

Предложения IBM

- ***Identity Lifecycle Management:*** Tivoli Identity and Access Management solutions,
- ***High-Assurance Digital Identities:*** Trusted Identity Initiative
- ***Identity Audit:*** Tivoli Security Compliance Insight Manager, Tivoli zSecure Audit
- **Identity & Access** Design and Implementation Services
- **ISS Managed Identity Services**
- **GBS Security Services**

Выгода

- Снижение затрат, увеличение эффективности и подконтрольный процесс прихода/увольнения сотрудников и аудит их доступа
- Снижение риска внутренних мошенничеств, утечек данных и остановки операций
- Единое управление идентификаторами по всему миру
- Использование последних технологий таких как single sign-on

ПРИЛОЖЕНИЯ и ПРОЦЕССЫ

Защита Web приложений

"Какие выгоды получит бизнес от контроля за безопасностью приложений?"

Ситуации

- В WEB приложениях хакеры ищут уязвимости в первую очередь
- Приложения разворачиваются с уязвимостями
- Недостаточно безопасная настройка приводит к потерям для бизнеса
- Стандарт PCI требует защиты приложений
- 80% времени тратят разработчики на поиск и исправление дефектов
- Реальные и даже секретные данные доступны свободно через тестовые сегменты, где работают партнеры и аутсорсеры

IBM Security Offerings

- ***Application Vulnerabilities***: Rational AppScan, ISS Managed Security Services, ISS Application Risk Assessment services
- ***Application Access Controls***: Tivoli Access Manager
- ***Messaging Security***: Lotus Domino Messaging, IBM ISS Mail security solutions
- ***Security for SOA***: WebSphere DataPower, Tivoli Security Policy Manager, Tivoli Federated Identity Manager
- **Application Security Assessment** services
- **GBS** Security Services

Выгода

- Снижение риска простоев, подмены данных на веб-сайтах
- Глобальный контроль и мониторинг соответствия законодательным требованиям
- Один из шагов к соответствию требованиям стандартов ИБ
- Возможность объединить важные для бизнеса приложения
- Автоматические тестирование и контроль за процессом разработки, снижение расходов на безопасность

СЕТЬ, СЕРВЕР и РАБОЧИЕ СТАНЦИИ

Управление безопасностью инфраструктуры

"Какие выгоды получает мой бизнес от защиты инфраструктуры?"

Ситуации

- Множество качественных платных и автоматизированных средств для атаки
- Скрытые, сложные к удалению угрозы и атаки
- Слабое понимание рисков в новых технологиях и приложениях, включая виртуализацию и облачные вычисления
- Слабый контроль за приложениями
- Недостаточно умения и понимания в управлении устройствами безопасности
- Общая стоимость управления складывается из постоянно растущего массива различных технологий
- Неизвестны все инциденты в силу неправомерного использования привилегированного доступа

IBM Security Offerings

- ***Threat Mitigation***: ISS Network, Server and Endpoint Intrusion Detection and Prevention products powered by X-Force®, Managed Intrusion Prevention and Detection, Network Mail Security, Managed firewall services, Vulnerability Management and Scanning
- ***SIEM***: Tivoli Compliance Insight Manager, Security Event and Log Management services
- ***Security Governance***: Regulatory assessments and remediation solutions, Security architecture and policy development
- ***Incident Response***: Incident Management and Emergency Response services
- ***Consulting and Professional Security Services***: Security Intelligence and Advisory Services
- **GBS Consulting Services**

Выгода

- Снижение операционных расходов на процедуры безопасности, включая запросы в HelpDesk, установку патчей
- Повышение доступности внутренних ресурсов и гарантия производительности, SLA на гарантированную защиту
- Повышенная продуктивность из за снижения рисков заражения вредоносным ПО
- Снижение числа спама, снижение нагрузки на каналы связи
- Быстрое разрешение причин инцидентов
- Готовность к соответствию требованиям стандартов

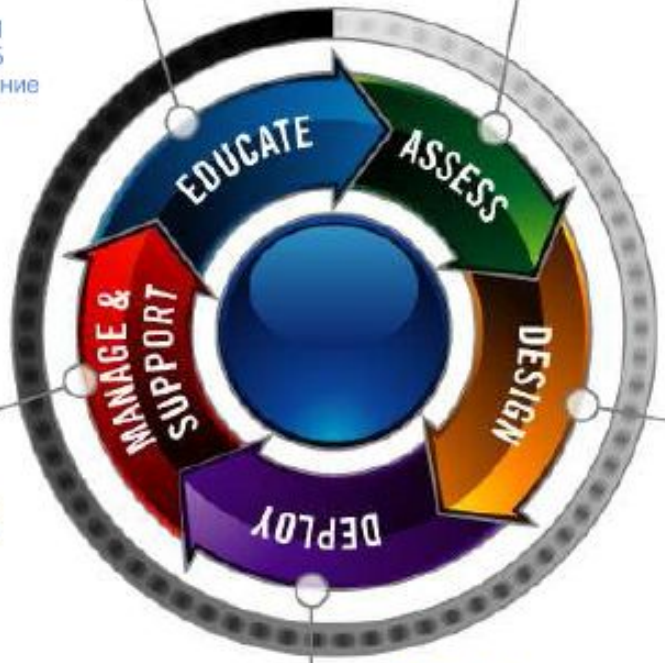
Professional Security Services (PSS)

Phase 5. Обучение

- Обучение по продуктам IBM
- Семинары и тренинги по ИБ
- Безопасное программирование

Phase 1. Оценка

- Аудит безопасности приложений
- Аудит информационной безопасности
- Аудит беспроводных сетей
- Анализ рисков
- Тест на взлом
- Аудит PCI DSS, HIPPA, SCADA, SOX



Phase 4. Управление и поддержка

- Система управления ИБ
- Расследование инцидентов
- Подбор и оценка персонала

Phase 2. Дизайн

- Планирование внедрения
- Дизайн безопасности сетевой инфраструктуры
- Разработка политик информационной безопасности
- Разработка стандартов и процедур

Phase 3. Внедрение

- Внедрение решений
- Миграция

Почему надо заниматься безопасностью WEB приложений

Хакеры изучают уязвимости WEB приложений

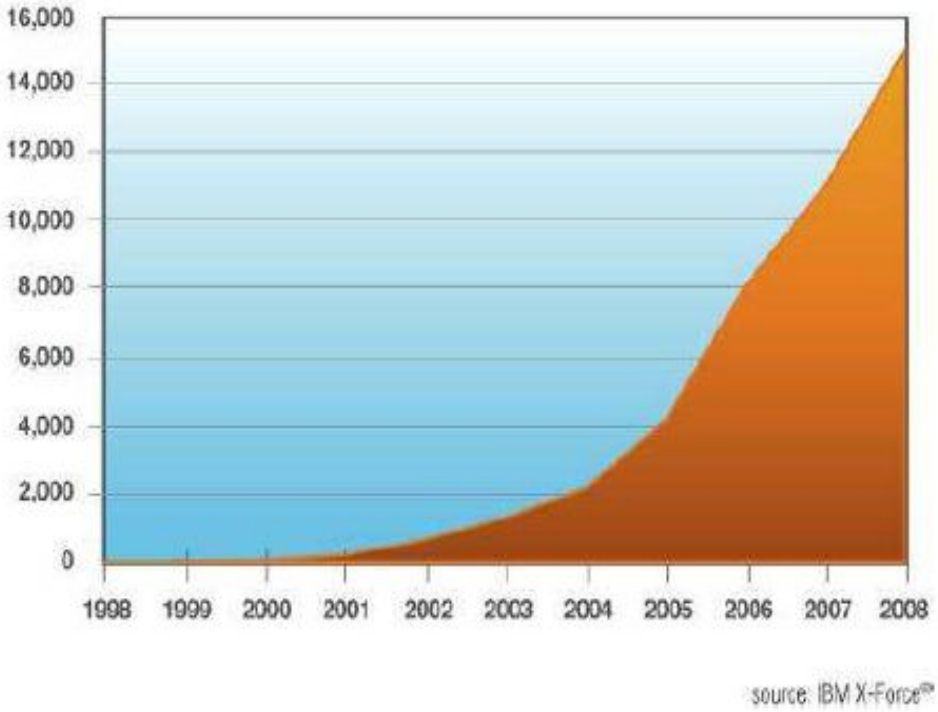
- **54.9%** от ВСЕХ найденных в 2008 уязвимостей – уязвимости WEB приложений
- **74%** от всех уязвимостей Web приложений в 2008 так и не были исправлены до конца года
- Атаки типа SQL injection выросли **в 30 раз** за последние 6 месяцев

Требование законодательства

- Стандарт PCI DSS требует защиты WEB приложений
- Закон 152-ФЗ распространяется на WEB приложения, например, внутренний WEB портал

… это открытая и легкая точка для доступа и можно получить достаточно важных данных

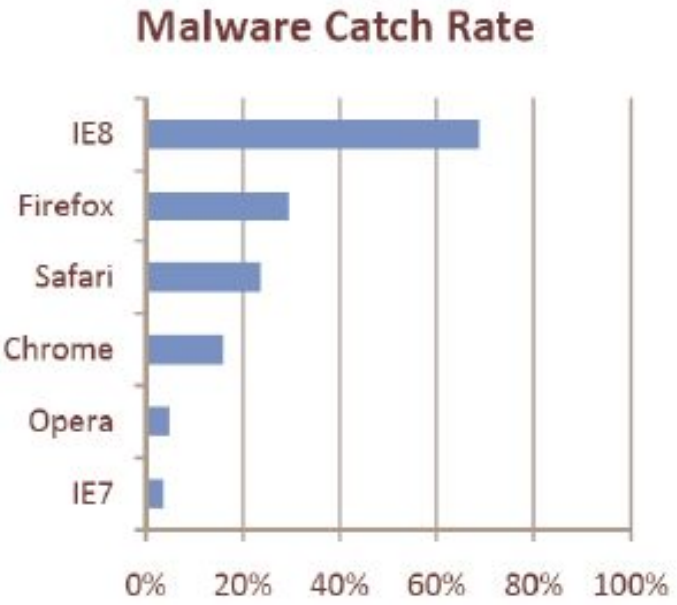
Рост уязвимостей WEB приложений с 1998 до 2008 года



50% заражений происходит через Web браузер

Эффективность защиты браузеров:

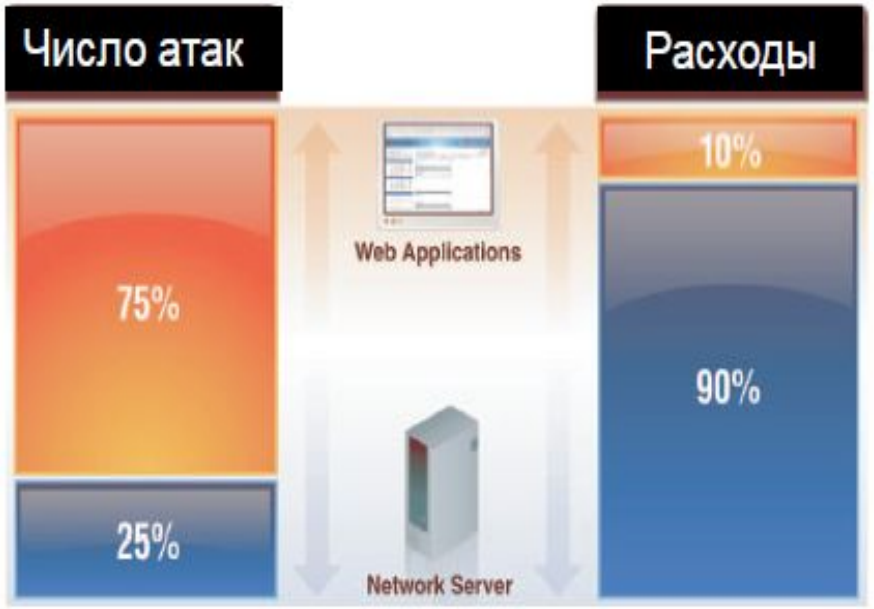
	Effectiveness
Microsoft IE8 (RC1)	69%
Mozilla Firefox v3.07	30%
Apple Safari v3	24%
Google Chrome v1.0.154	16%
Opera v9.64	5%
Microsoft IE7	4%



Тест NSS, 12 марта, 2009

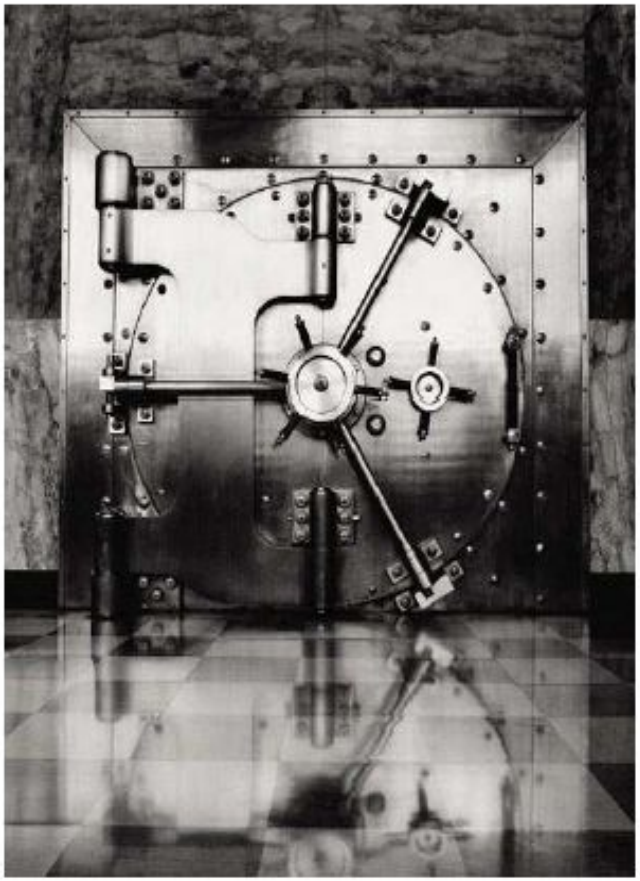
Традиционные решения упускают из вида или неэффективно защищают WEB приложения

- Сканеры безопасности
  - Традиционные сканеры безопасности упускают из виду WEB приложения
- Тесты на взлом
  - Эффективно находят один раз уязвимости, но не могут постоянно контролировать ситуацию
- Межсетевые экраны
  - Содержат простейшие методы защиты WEB серверов, но упускают из вида многие виды атак
- Специализированный firewall WEB приложений
  - Дорого установить и дорого обслуживать
  - Настроить такую защиту равноценно работе по исправлению уязвимости



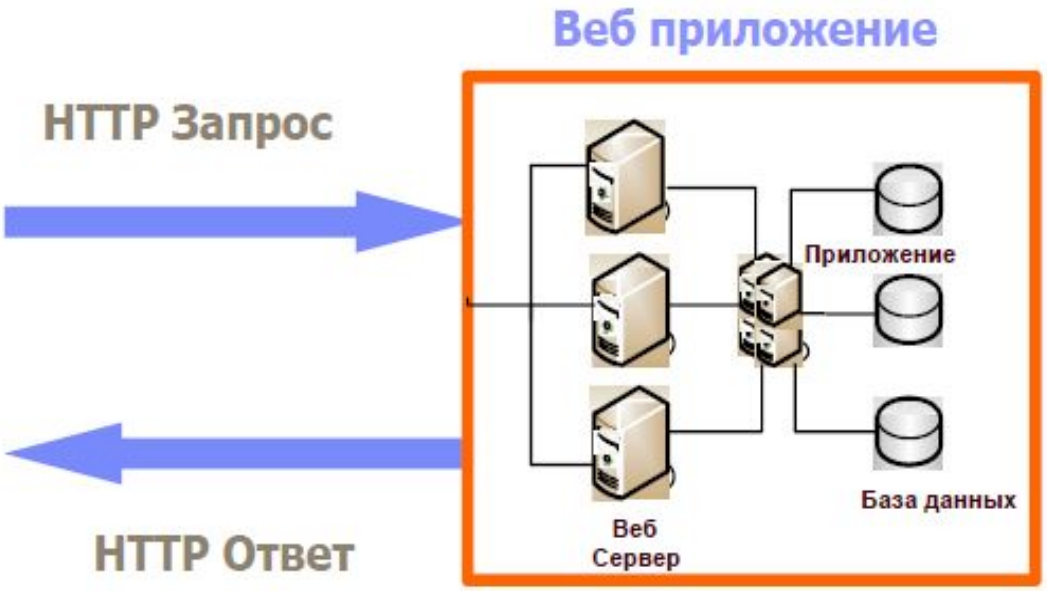
Превентивная защита: IBM Rational AppScan

- Несомненный лидер в сканировании уязвимостей Web приложений
  - Самая большая доля рынка по мнению IDC
- Автоматически сканирует web приложения и ищет уязвимости
  - SQL Injection
  - Cross-site Scripting
- Дает точные рекомендации как исправить уязвимость
- Проверяет Web сайты на наличие встроенного вредоносного кода
  - Защищает ваш web сайт от распространения следующего Conficker для каждого посетителя сайта
  - Использует защиту от вредоносного кода разработанную X-Force



Как работает Rational AppScan

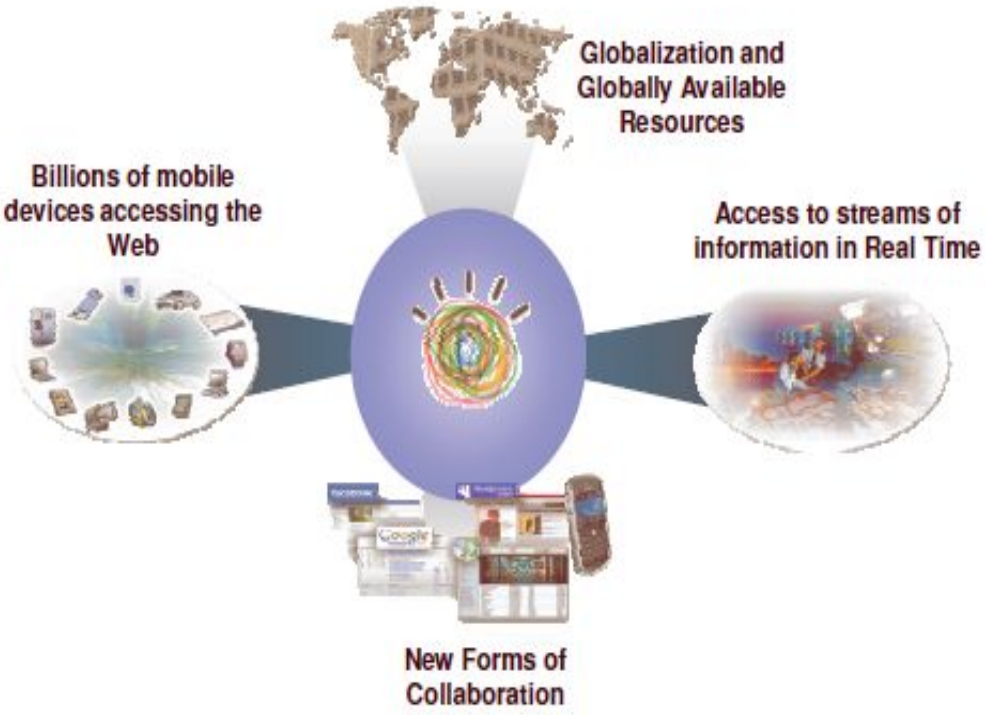
- Подход к приложению как к “черному ящику”
- Обследование веб приложения и построение модели сайта
- Определить векторы атак основываясь на выбранной политике тестирования
- Тестирование посредством посылки модифицированных HTTP запросов приложению и проверка HTTP ответов в соответствии с правилами проверки




Rational AppScan
Proventia Web app protection
WebSphere DataPower
Web app firewall
Разработка безопасного кода
Поиск уязвимостей в веб приложениях
Информация как исправить уязвимости
Блокирование атак на уязвимости
Блоикирование атак на Oracle, MySQL, MS SQL
Блокирование DoS атак
Построение своих правил для защиты
Обновление правил защиты
Блокирование атак на серверную ОС
Блокирование атак на веб браузер
Расшифрование SSL для анализа атак
Безопасность SOA
© 2009 IBM Corporation

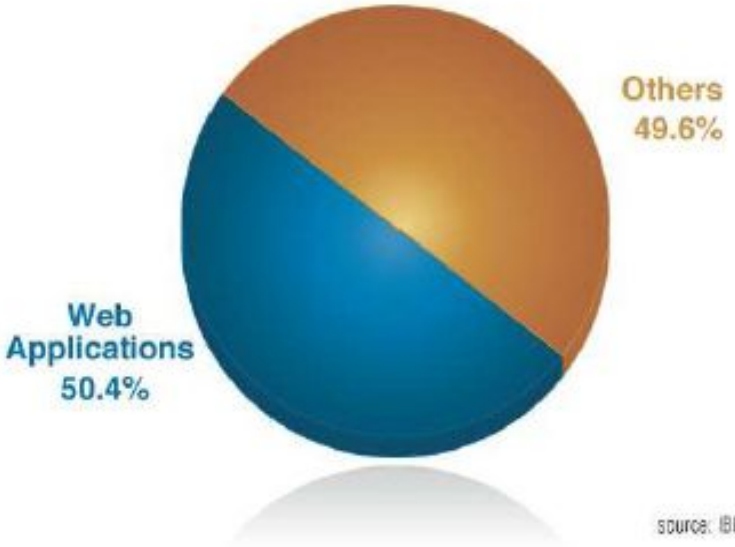
Таким образом, защита WEB приложений от IBM это

- **Интеграция полного комплекта решений**
  - Появление безопасности уже на этапе разработки приложений
  - Обнаружение вредоносного кода и управление уязвимостями
  - Блокирование атак в реальном времени
  - Безопасность и производительность для SOA
- **Безопасность данных и целостность бизнес-процессов на базе WEB**
  - Онлайновые платежи
  - Доверенные транзакции между партнерами
  - Базы данных
- **Соответствие требованиям**
  - Соответствие PCI DSS 6.6 (30 июня 2008)



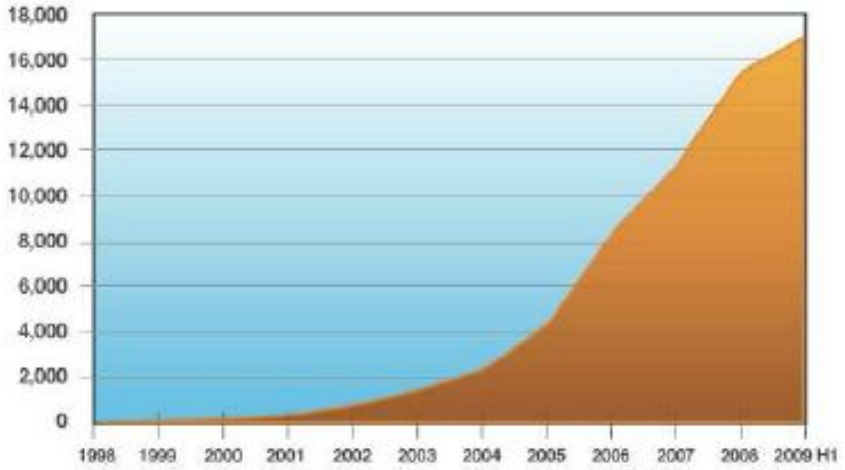
80% компаний пострадают от проблем с безопасностью WEB приложений к 2010 году

Больше половины уязвимостей в первой половине 2009 года опять в WEB приложениях



source: IBM X-Force®

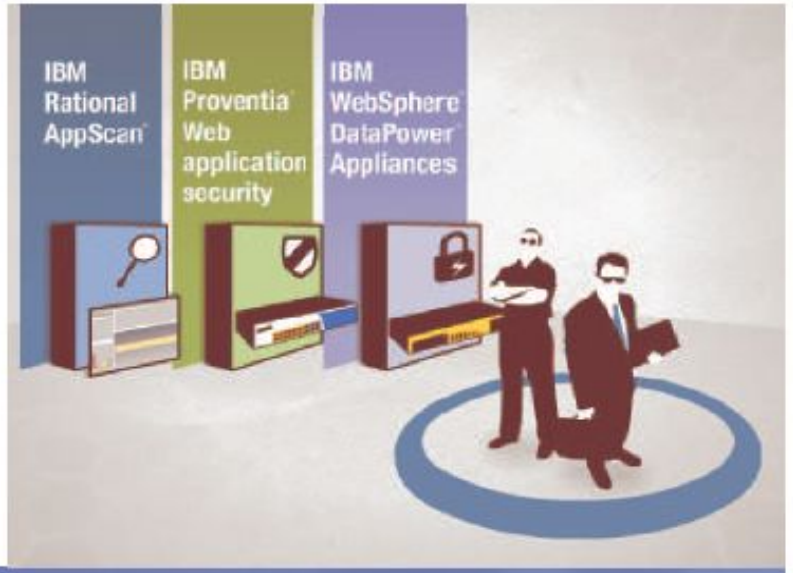
Уязвимостей WEB приложений находят все больше и больше



source: IBM X-Force®

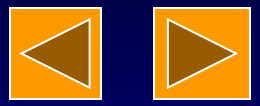
Что делать?

- Проведите оценку рисков и обновите политику безопасности
- Настройте защиту, если у вас уже есть эти продукты
- Переходите из режима просмотра атак, в режим блокирования атак
- Добавьте недостающие элементы защиты
- Включите процессы контроля за работой системы ИБ
- Обучите пользователей

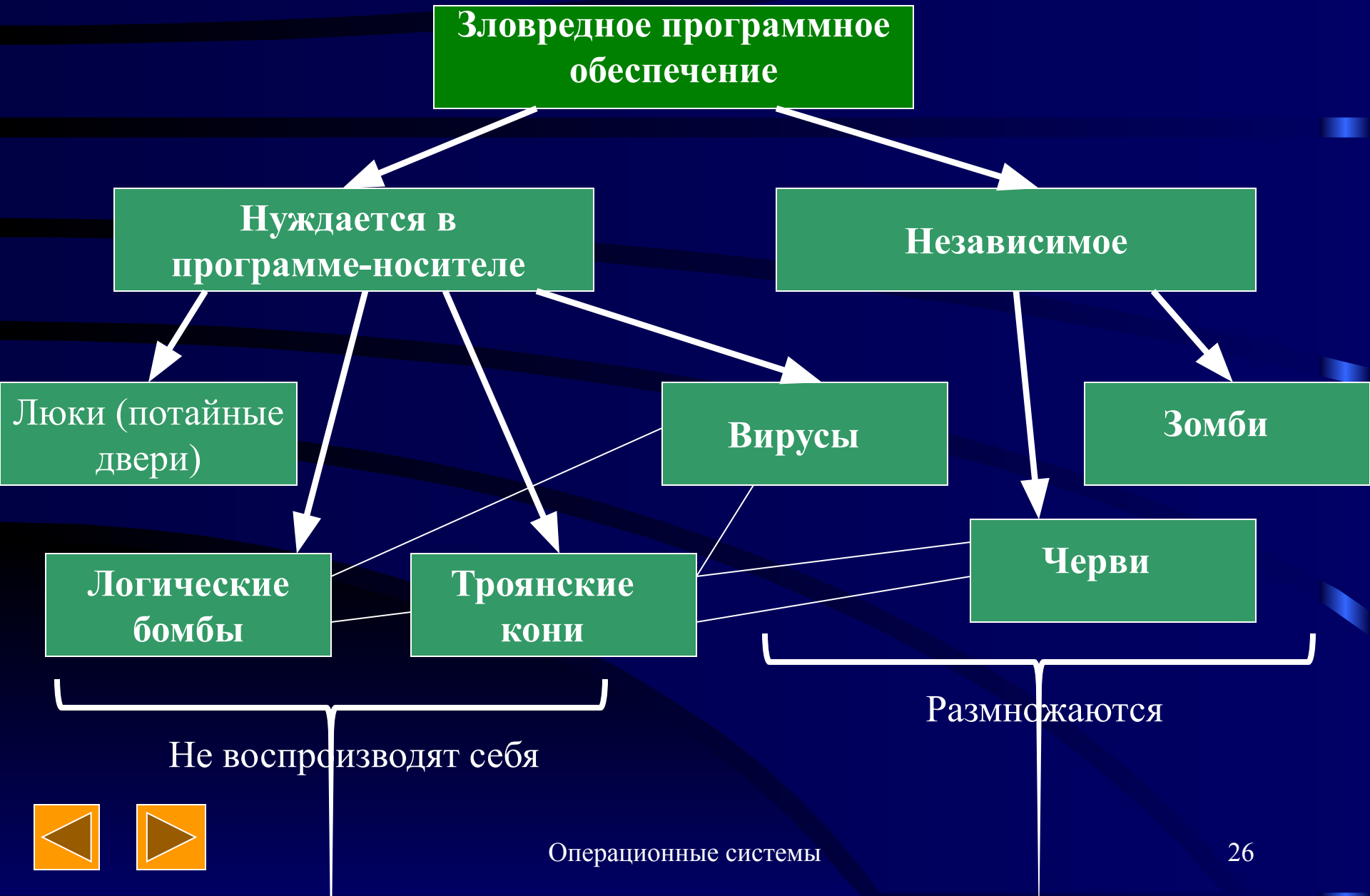


6.2.3. Случайная потеря данных

1. **Форс-мажор: пожары, наводнения, землетрясения, войны, восстания, крысы, изгрызшие кабели, магнитные ленты или гибкие диски.**
2. **Аппаратные и программные ошибки, сбои центрального процессора, нечитаемые диски или ленты, ошибки в программах (в том числе в операционной системе), ошибки при передаче данных.**
3. **Человеческий фактор: неправильный ввод данных, неверно установленные диски или ленты, запуск не той программы, потерянный диск, невыполненное резервное копирование и т. п.**

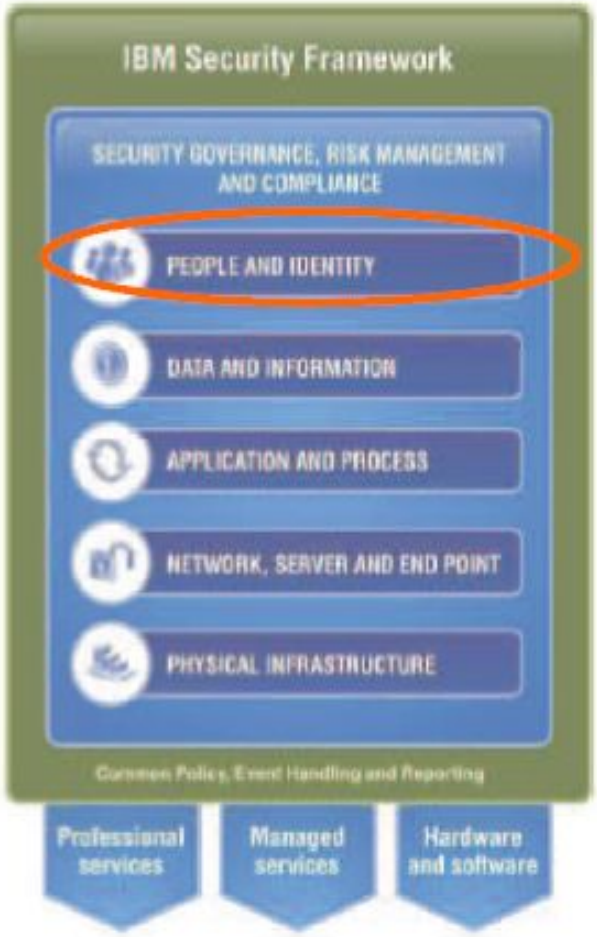


6.3. Атаки на систему снаружи



Люди и идентификаторы

- Внутренние и внешние пользователи
- Работники по контракту
- Управление идентификаторами
- Разграничение доступа
- Расширенная аутентификация
- Аудит действий сотрудников
- Доверенные отношения с контрагентами



Как быть с полномочиями?

Источник внутренних инцидентов*

КАК?

* Источник: USSS/CET Insider Threat Survey

Постоянный контроль

Процесс создания и согласования учетных записей

1. Отслеживание изменений в **базе** службы отдела кадров
2. Определение необходимых ролей и прав **доступа**
3. Проверка **соблюдения** правил разделения обязанностей
4. Сбор необходимых утверждений
5. Создание необходимых учетных записей
6. Периодическое согласование учетных записей.
7. Tivoli Compliance Insight Manager (TCIM) Централизованный аудит действий пользователей

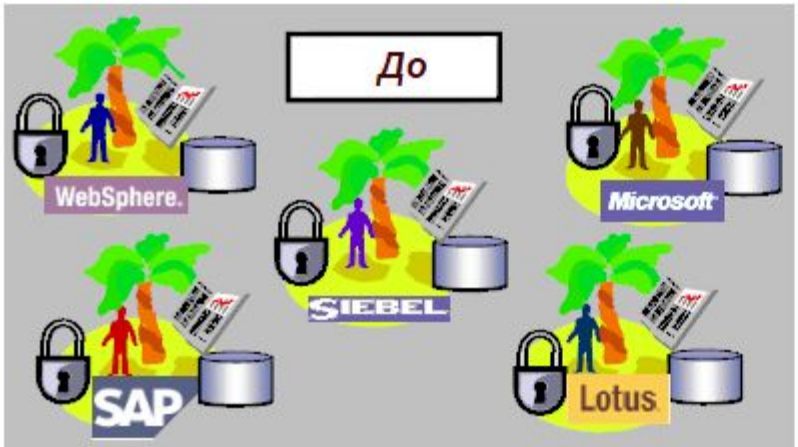
Tivoli software

Адаптер

Бизнес-приложения

Tivoli software

Управления доступом для электронного бизнеса



- Много паролей
- Много администраторов, различные средства управления
- Информация о пользователях и правах доступа рассредоточена

- Web SSO
- Один администратор (делегирование), единое средство управления
- Данные о пользователях и правах доступа централизованы и ясны

= Политика безопасности = Пользователи и группы = Аудит

6.4. Системный подход к обеспечению безопасности

1. Морально-этические средства защиты – нормы, сложившиеся по мере распространения вычислительных средств в обществе (аморальность покушений на чужие информационные ресурсы).
2. Законодательные средства защиты – законы, постановления, нормативные акты и стандарты, которыми регламентируются правила использования и обработки информации, а также вводятся меры ответственности за их нарушение.
3. Административные меры – действия руководства предприятия для обеспечения информационной безопасности.
4. Психологические меры безопасности.
5. Физические средства защиты.
6. Технические средства информационной безопасности – программное и аппаратное обеспечение системы, контроль доступа, аутентификация и авторизация, аудит, шифрование информации, антивирусная защита контроль сетевого трафика и т. п.
7. Надежная работа программных и аппаратных средств системы, средства обеспечения отказоустойчивости и восстановления операционной системы, целостности и доступности приложений и баз данных.

На основе системного подхода разрабатывается политика безопасности

Безопасность как бизнес-процесс

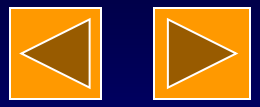
Обеспечение безопасности

6.5. Политика безопасности

ВОПРОСЫ: 1) какую информацию защищать? 2) какой ущерб понесет предприятие при потере или раскрытии тех или иных данных? 3) кто или что является возможным источником угроз? 4) какого рода атаки на безопасность системы могут быть предприняты ? 5) какие средства использовать для защиты каждого вида информации?

Базовые принципы безопасности:

1. **Минимальный уровень привилегий на доступ к данным.**
2. **Комплексный подход к обеспечению безопасности.**
3. **Баланс надежности защиты всех уровней.**
4. **Использование средств, обеспечивающих максимальную защиту при атаке (например, полная блокировка автоматического пропускного пункта при его отказе, полная блокировка входа в сеть и др.).**
5. **Единый контрольно-пропускной путь – весь трафик через один узел сети (firewall).**
6. **Баланс возможного ущерба от угрозы и затрат на ее предотвращение.**
7. **Ограничение служб, методов доступа для лиц, имеющих доступ в Интернет и из Интернета во внутреннюю сеть предприятия. Политика доступа к службам Интернет и политика доступа к ресурсам внутренней сети.**



Безопасность – это не способ избежать риска. Это способ овладения риском.

6.6. Выявление вторжений

Вторая линия обороны

1. Быстрое обнаружение вторжения позволяет идентифицировать и изгнать взломщика прежде, чем он причинит вред.
2. Эффективная система обнаружения вторжений служит сдерживающим средством, предотвращающим вторжения.
3. Обнаружение вторжений позволяет собирать информацию о методах вторжения, которую можно использовать для повышения надежности средств защиты.

Подходы к выявлению вторжений

1. Выявление статистических отклонений (пороговое обнаружение –пороги частот различных событий, профильное обнаружение). Эффективно против притворщиков, бессильно против правонарушителей.

2. Выявление на основе правил (выявление отклонений от обычных характеристик, идентификация проникновения –поиск подозрительного поведения). Эффективно против взломщиков.

Основной инструмент выявления вторжений – записи данных аудита.

6.7. Базовые технологии безопасности

(Аутентификаций, авторизация, аудит, технология защищенного канала)

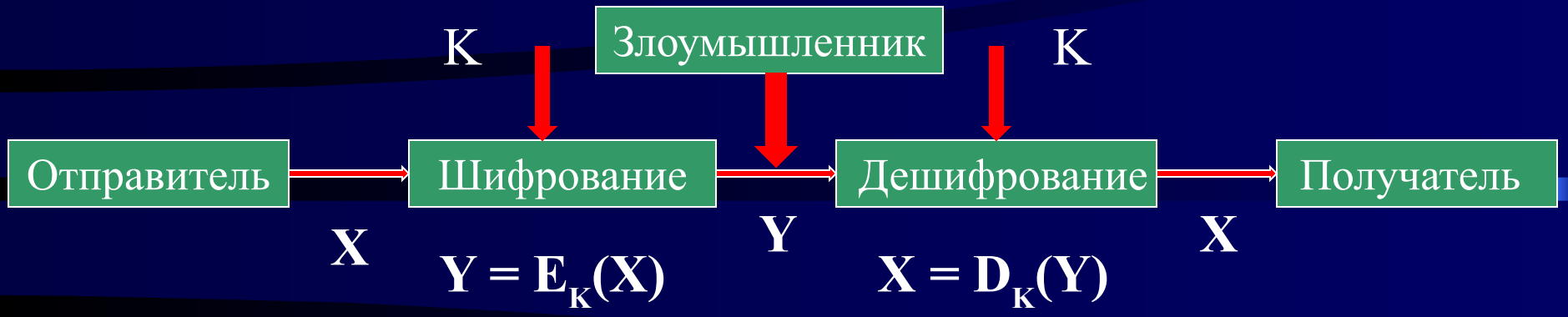
6.7.1. Шифрование

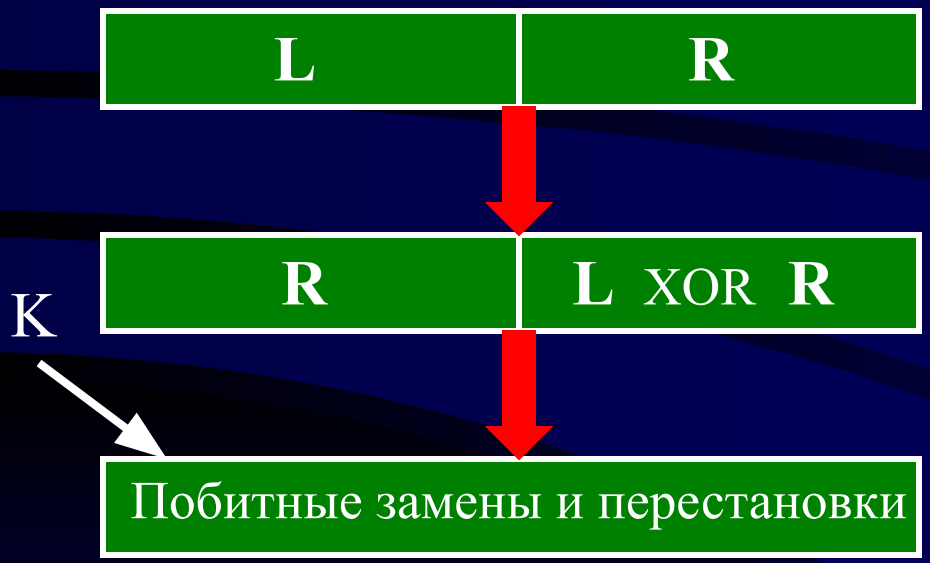
Пара процедур – шифрование и дешифрование – называется криптосистемой.

(симметричные и асимметричные)

Алгоритм шифрования считается раскрытым, если найдена процедура, позволяющая подобрать ключ за реальное время. **Правило Керкхоффа: стойкость шифра должна определяться только секретностью ключа.**

Модель симметричного шифрования (1949 г. – Клод Шеннон)





Результат шифрования

Ключ К содержит 56 сл. Битов и 8 контрольных (112 и 16)

Исходный блок 64 бита

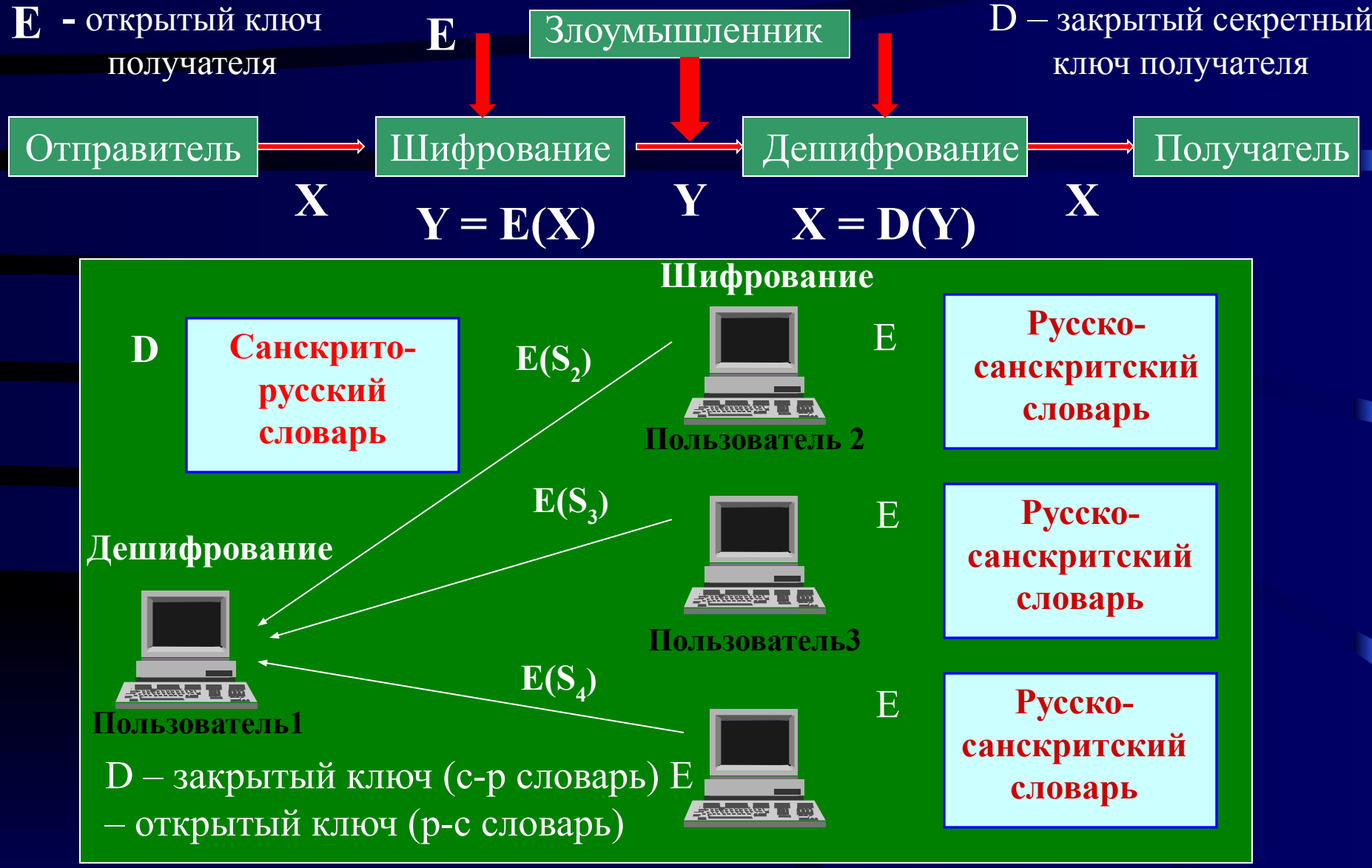
Схема шифрования по алгоритму DES (Data Encryption Standard)

K - разделяемый секретный ключ,
E, D – алгоритмы шифрования-дешифрования, разработаны фирмой IBM в 1976 году.

Основная проблема – ключи (надежность генерации, передачи и сохранения).

Модель несимметричного шифрования

(Винфилд Диффи и Мартин Хеллман – середина 70-х г. 20 века)



Подтверждение авторства посылаемого сообщения (электронная подпись)

Дешифрование

D – закрытый ключ

E – открытый ключ

Пользователь 2 $E(D(S_2)) = S_2$

$D(S_2)$

$D(S_3)$

Шифрование

Пользователь1

Пользователь 3 $E(D(S_3)) = S_3$

$D(S_4)$

Пользователь4

$E(D(S_4)) = S_4$

Для полного сетевого обмена необходимо иметь 2 N ключей (N закрытых и N открытых)

Криптоалгоритм RSA (1978 год)

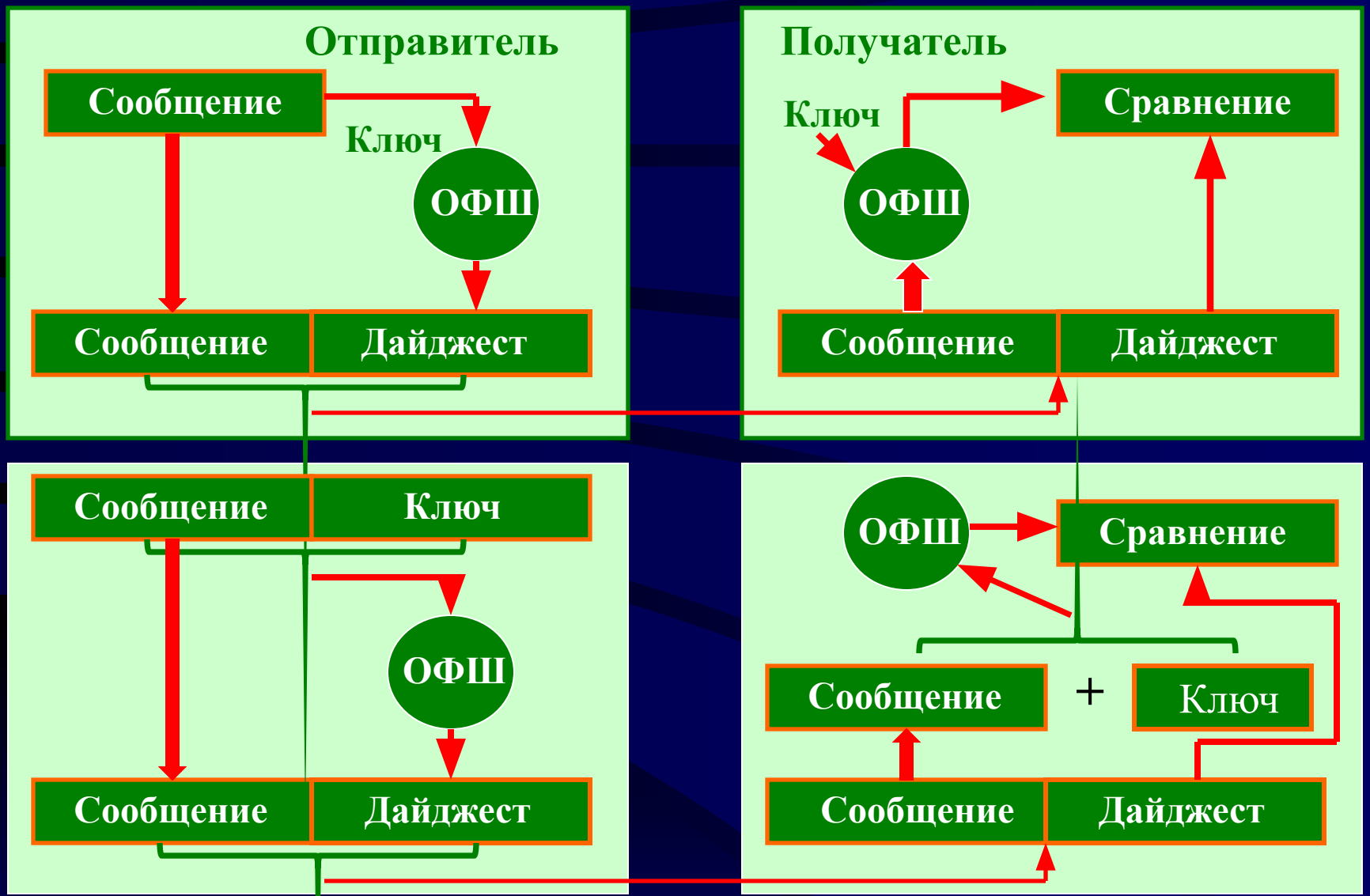
Разработан Ривестом, Шамиром и Адлеменом (Rivest, Shamir,Adleman)

1. Случайно выбирается два очень больших простых числа p и q.
2. Вычисляется два произведения $n = p \times q$ и $m = (p - 1) \times (q - 1)$.
3. Выбирается случайное целое число E, не имеющее общих сомножителей с m.
4. Находится D, такое, что $D \times E \mod m = 1$.
5. Исходный текст X разбивается на блоки таким образом, чтобы $0 < X < n$.
6. Для шифрования сообщения необходимо вычислить $C = X^E \mod n$.
7. Для дешифрования вычисляется $X = C^D \mod n$.

Таким образом, чтобы зашифровать сообщение, необходимо знать пару чисел (E, n), а чтобы дешифровать – пару чисел (D, m). Первая пара – открытый ключ, вторая – закрытый.

Для разложения 200-значного числа на простые множители нужно 4 миллиарда лет работы компьютера с быстродействием 1 млн. оп. в с.

Односторонние функции шифрования (one-way function, hash function, digest function)



6.7.2. Аутентификация, пароли, авторизация, аудит

1. **Аутентификация (authentification) предотвращает доступ к сети нежелательных лиц и разрешает вход для легальных пользователей.**

Доказательства аутентичности:

1) знание некоего общего для обеих сторон секрета: пароля или факта (дата, место события и др.);

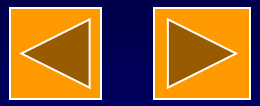
2) владение уникальным предметом (физическим ключом, электронной магнитной картой);

3) собственные биохарактеристики: радужная оболочка глаза, отпечатки пальцев, голос и т. д.

Чаще всего для доказательства аутентичности используются пароли. С целью снижения уровня угрозы раскрытия паролей администраторы применяют встроенные программные средства операционных систем для формирования политики назначения и использования паролей. Аутентификация взаимная: клиент – сервер, приложение – пользователь и т. д.

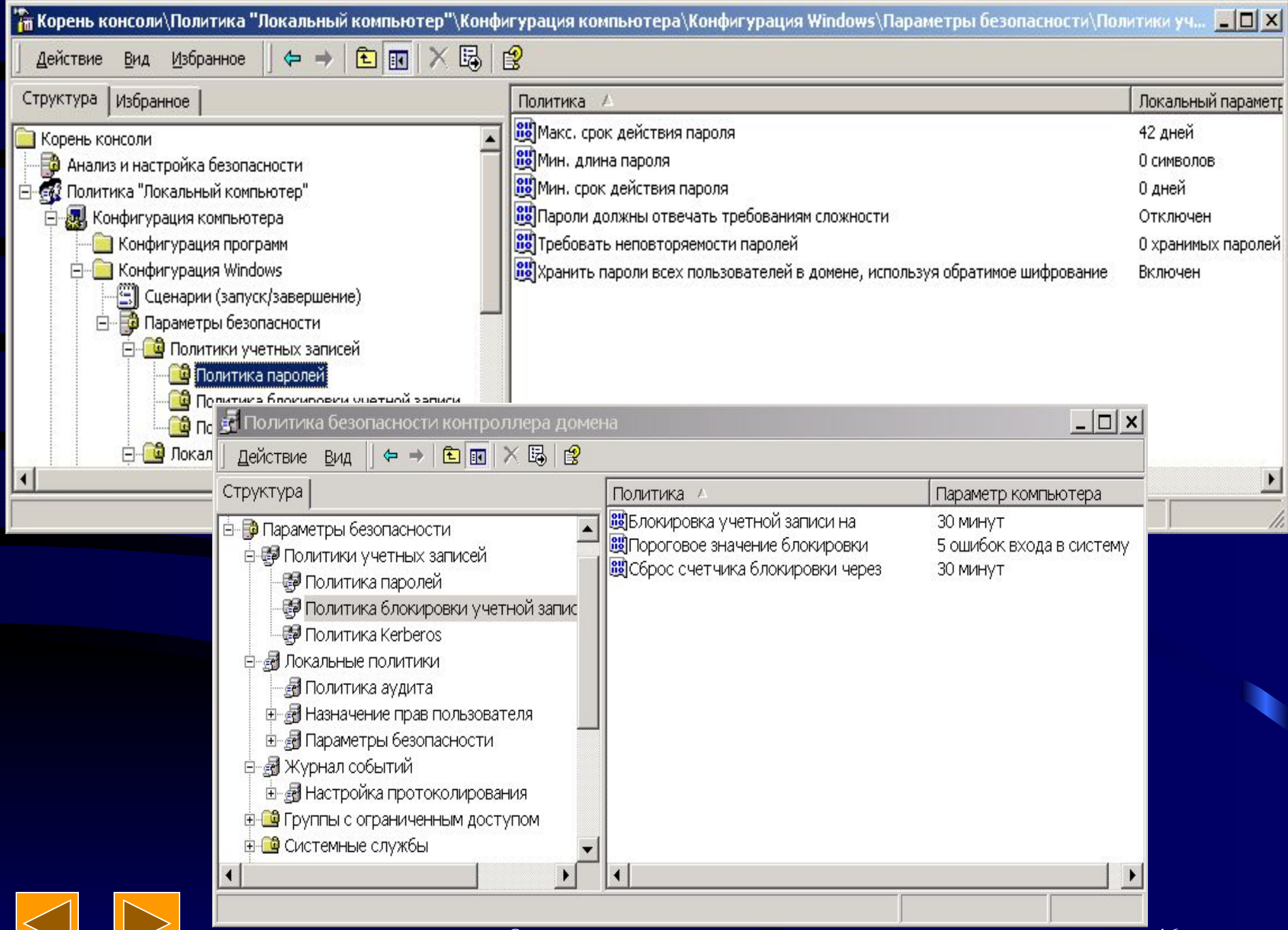
Политика паролей

Параметр	По умолчанию	Рекомендация
Enforce password history	Помнить 1 пароль	Помнить 24 пароля
Maximum password age	42 дня	42 дня
Minimum password age	0 дней	2 дня
Minimum password length	0 символов	8 символов
Password must meet complexity requirements	Disabled	Enabled



Политика блокировки учетной записи

Параметр	По умолчанию	Рекомендация
Account Lockout Duration	Not Defined	30 минут
Account Lockout Threshold	0	5 попыток
Reset Account Lockout after	Not Defined	30 минут


Корень консоли\Политика "Локальный компьютер"\Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики уч...
Действие Вид Избранное
Структура Избранное
Корень консоли
Анализ и настройка безопасности
Политика "Локальный компьютер"
Конфигурация компьютера
Конфигурация программ
Конфигурация Windows
Сценарии (запуск/завершение)
Параметры безопасности
Политики учетных записей
Политика паролей
Политика
Локальный параметр
Макс. срок действия пароля 42 дней
Мин. длина пароля 0 символов
Мин. срок действия пароля 0 дней
Пароли должны отвечать требованиям сложности Отключен
Требовать неповторяемости паролей 0 хранимых паролей
Хранить пароли всех пользователей в домене, используя обратимое шифрование Включен
Политика безопасности контроллера домена
Действие Вид
Структура
Параметры безопасности
Политики учетных записей
Политика паролей
Политика блокировки учетной запис
Политика Kerberos
Локальные политики
Политика аудита
Назначение прав пользователя
Параметры безопасности
Журнал событий
Настройка протоколирования
Группы с ограниченным доступом
Системные службы
Политика
Параметр компьютера
Блокировка учетной записи на 30 минут
Пороговое значение блокировки 5 ошибок входа в систему
Сброс счетчика блокировки через 30 минут

Авторизация доступа

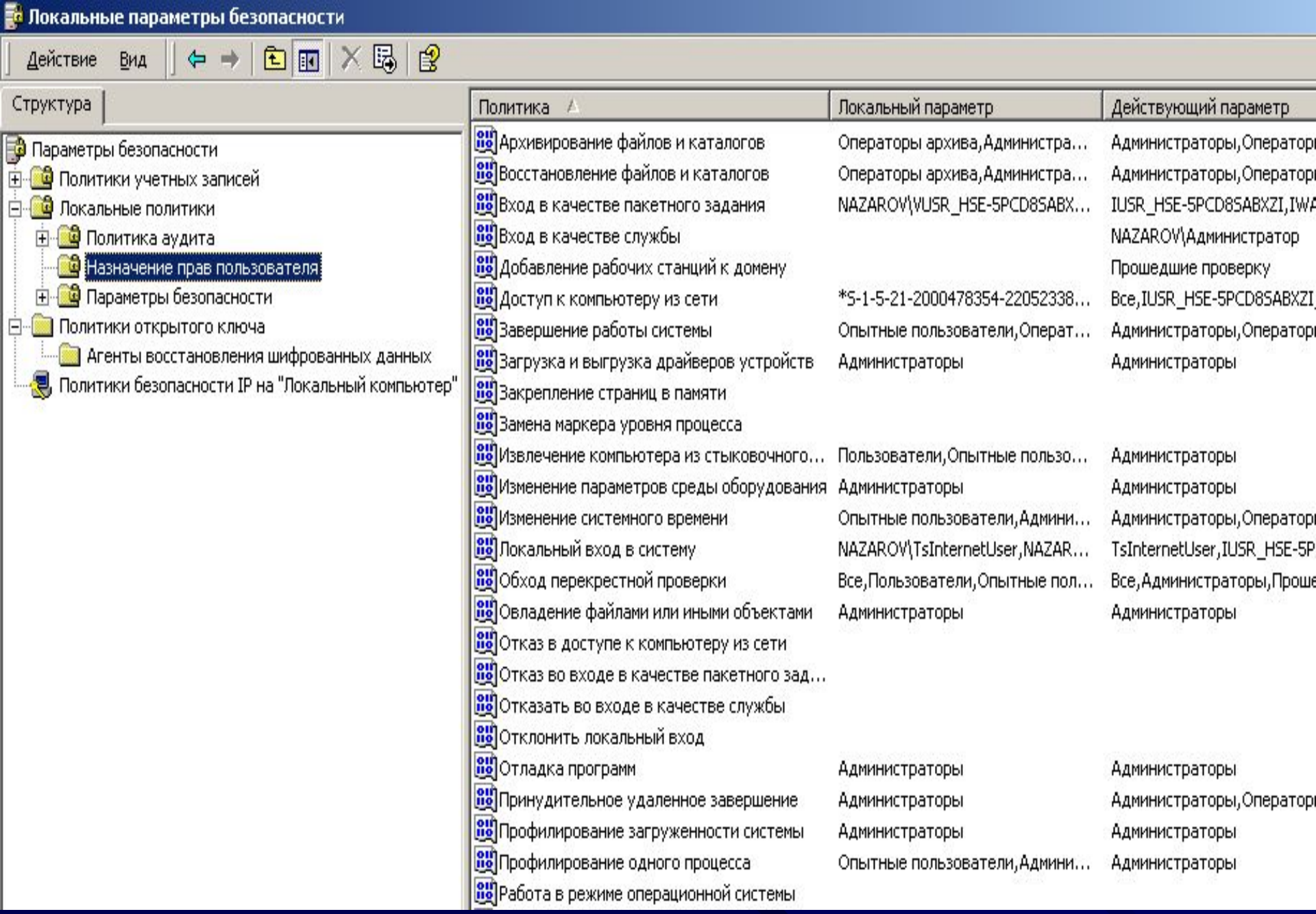
1. Система авторизации имеет дело только с легальными пользователями, которые успешно прошли процедуру аутентификации.

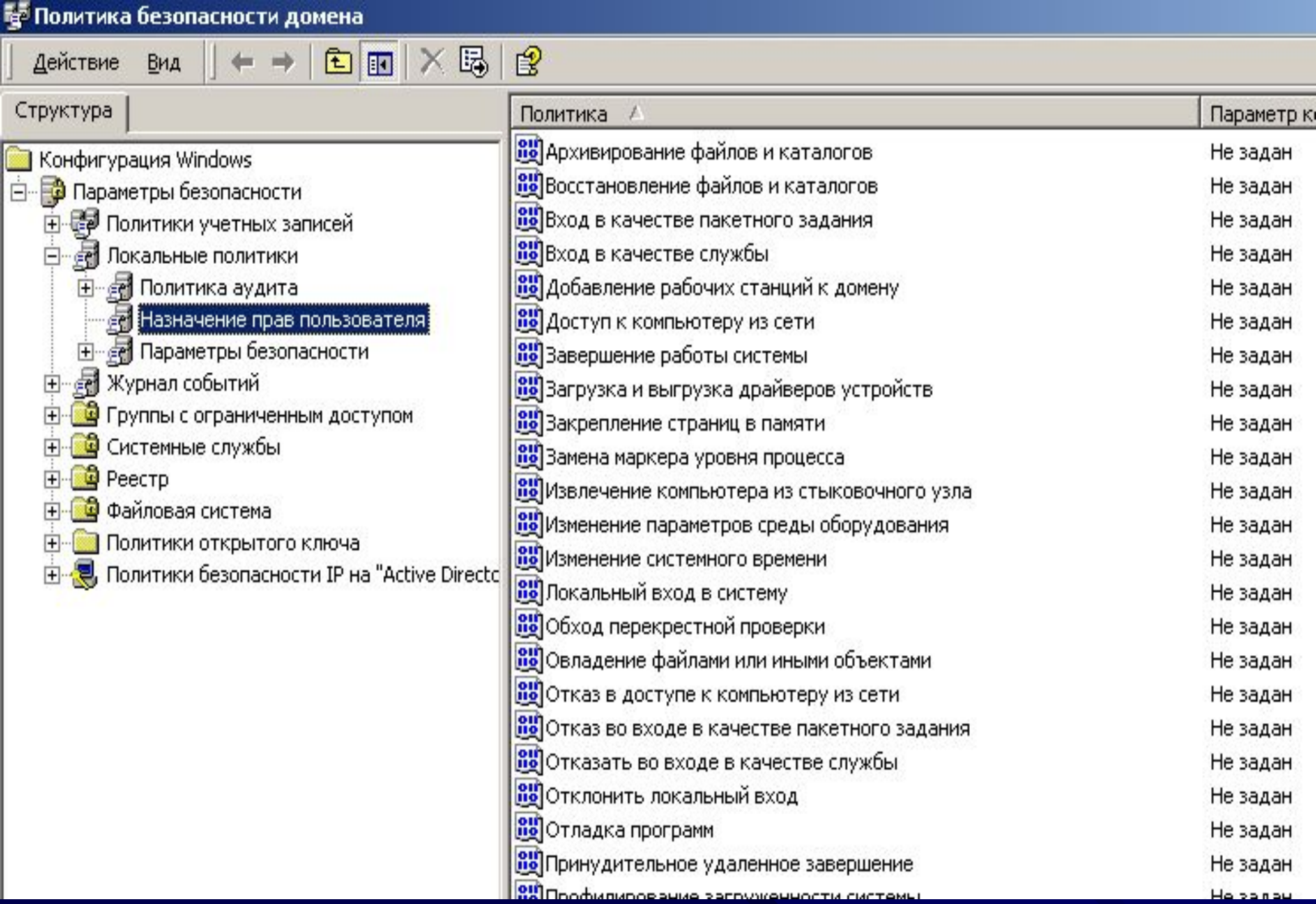
2. Цель подсистемы авторизации – предоставить каждому легальному пользователю те виды доступа и к тем ресурсам, которые были для него определены администратором системы.

3. Система авторизации использует различные формы правил доступа к ресурсам: а) избирательные права – в операционных системах универсального назначения; б) мандатный подход – деление информации на уровни в зависимости от степени ее секретности (для служебного пользования, секретно, сов. секретно, особой важности) и пользователей по форме допуска (первая, вторая, третья).

4. Процедуры авторизации реализуются программными средствами операционных систем или отдельными программными продуктами.

5. Схемы авторизации: децентрализованные (на рабочих станциях), централизованные (на серверах), комбинированные.


Локальные параметры безопасности
Действие
Вид
Структура
Параметры безопасности
Политики учетных записей
Локальные политики
Политика аудита
Назначение прав пользователя
Параметры безопасности
Политики открытого ключа
Агенты восстановления шифрованных данных
Политики безопасности IP на "Локальный компьютер"
Политика
Локальный параметр
Действующий параметр
Архивирование файлов и каталогов
Операторы архива,Администра...
Администраторы,Операторы
Восстановление файлов и каталогов
Операторы архива,Администра...
Администраторы,Операторы
Вход в качестве пакетного задания
NAZAROV\IUSR_HSE-5PCD8SABX...
IUSR_HSE-5PCD8SABXZI,IWA
Вход в качестве службы
NAZAROV\Администратор
Добавление рабочих станций к домену
Прошедшие проверку
Доступ к компьютеру из сети
*S-1-5-21-2000478354-22052338...
Все,IUSR_HSE-5PCD8SABXZI
Завершение работы системы
Опытные пользователи,Операт...
Администраторы,Операторы
Загрузка и выгрузка драйверов устройств
Администраторы
Администраторы
Закрепление страниц в памяти
Замена маркера уровня процесса
Извлечение компьютера из стыковочного...
Пользователи,Опытные пользо...
Администраторы
Изменение параметров среды оборудования
Администраторы
Администраторы
Изменение системного времени
Опытные пользователи,Админи...
Администраторы,Операторы
Локальный вход в систему
NAZAROV\TsInternetUser,NAZAR...
TsInternetUser,IUSR_HSE-5P
Обход перекрестной проверки
Все,Пользователи,Опытные пол...
Все,Администраторы,Прошед
Овладение файлами или иными объектами
Администраторы
Администраторы
Отказ в доступе к компьютеру из сети
Отказ во входе в качестве пакетного зад...
Отказать во входе в качестве службы
Отклонить локальный вход
Отладка программ
Администраторы
Администраторы
Принудительное удаленное завершение
Администраторы
Администраторы,Операторы
Профилирование загруженности системы
Администраторы
Администраторы
Профилирование одного процесса
Опытные пользователи,Админи...
Администраторы
Работа в режиме операционной системы


Политика безопасности домена
Действие
Вид
Структура
Конфигурация Windows
Параметры безопасности
Политики учетных записей
Локальные политики
Политика аудита
Назначение прав пользователя
Параметры безопасности
Журнал событий
Группы с ограниченным доступом
Системные службы
Реестр
Файловая система
Политики открытого ключа
Политики безопасности IP на "Active Directc
Политика
Параметр к
Архивирование файлов и каталогов
Не задан
Восстановление файлов и каталогов
Не задан
Вход в качестве пакетного задания
Не задан
Вход в качестве службы
Не задан
Добавление рабочих станций к домену
Не задан
Доступ к компьютеру из сети
Не задан
Завершение работы системы
Не задан
Загрузка и выгрузка драйверов устройств
Не задан
Закрепление страниц в памяти
Не задан
Замена маркера уровня процесса
Не задан
Извлечение компьютера из стыковочного узла
Не задан
Изменение параметров среды оборудования
Не задан
Изменение системного времени
Не задан
Локальный вход в систему
Не задан
Обход перекрестной проверки
Не задан
Овладение файлами или иными объектами
Не задан
Отказ в доступе к компьютеру из сети
Не задан
Отказ во входе в качестве пакетного задания
Не задан
Отказать во входе в качестве службы
Не задан
Отклонить локальный вход
Не задан
Отладка программ
Не задан
Принудительное удаленное завершение
Не задан

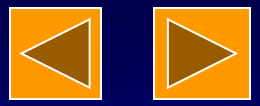
Аудит (auditing) – фиксация в системном журнале событий, происходящих в операционной системе, имеющих отношение к безопасности и связанных с доступом к защищаемым системным ресурсам.

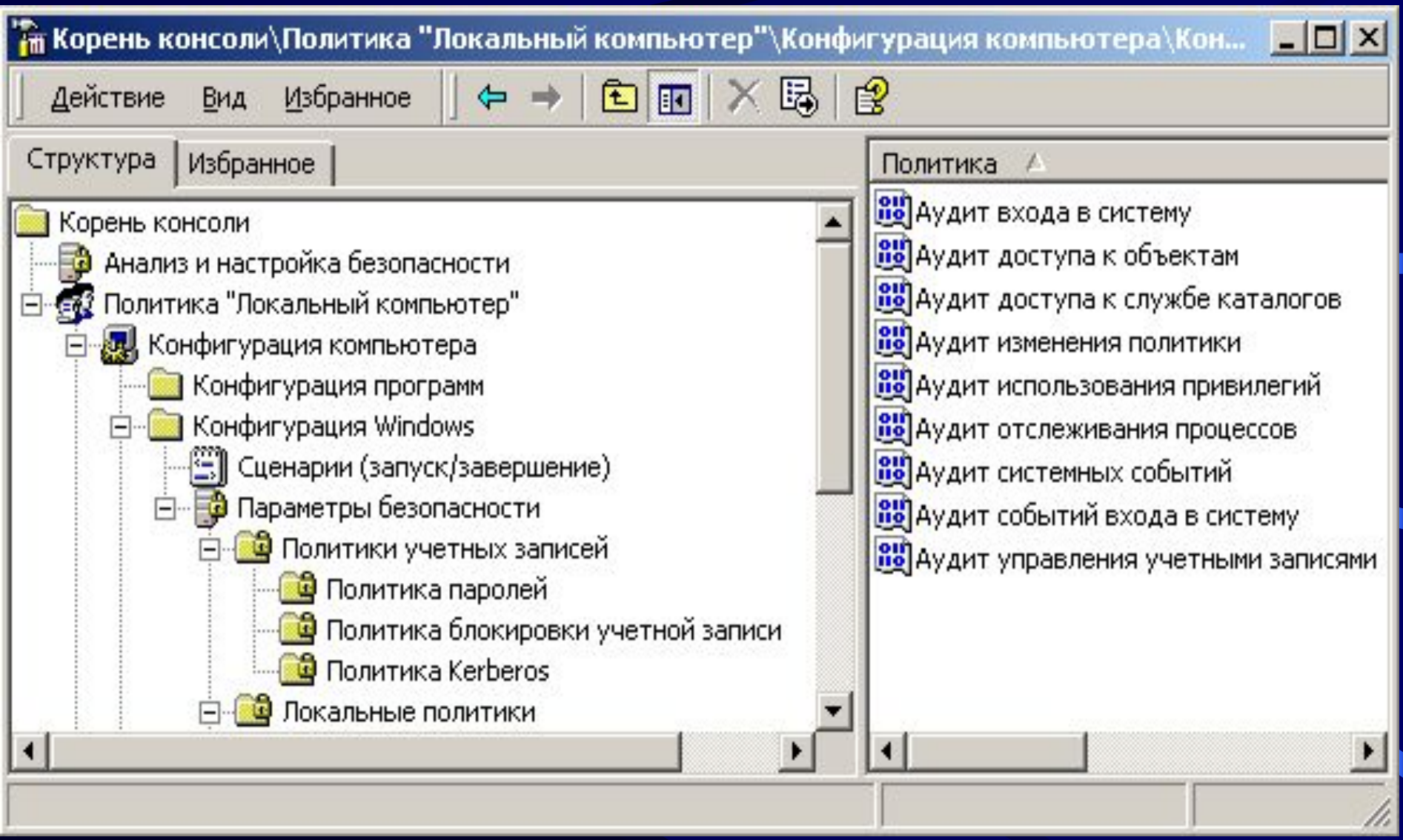
Регистрация успешных и неуспешных действий:

- **Регистрация в системе;**
- **Управление учетной записью;**
- **Доступ к службе каталогов;**
- **Доступ к объекту;**
- **Использование привилегий;**
- **Изменение политики;**
- **Исполнение процессов и системные события.**

Аудит включается в локальной (групповой) политике аудита.

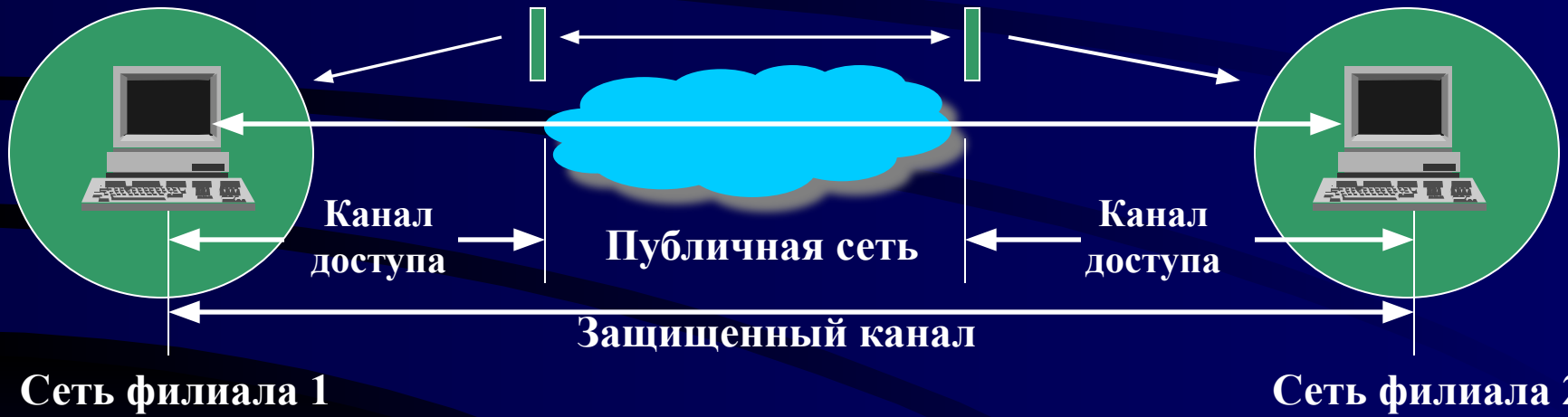
Журнал безопасности содержит записи, связанные с системой безопасности.




Корень консоли\Политика "Локальный компьютер"\Конфигурация компьютера\Кон...
Действие
Вид
Избранное
Структура
Избранное
Корень консоли
Анализ и настройка безопасности
Политика "Локальный компьютер"
Конфигурация компьютера
Конфигурация программ
Конфигурация Windows
Сценарии (запуск/завершение)
Параметры безопасности
Политики учетных записей
Политика паролей
Политика блокировки учетной записи
Политика Kerberos
Локальные политики
Политика
Аудит входа в систему
Аудит доступа к объектам
Аудит доступа к службе каталогов
Аудит изменения политики
Аудит использования привилегий
Аудит отслеживания процессов
Аудит системных событий
Аудит событий входа в систему
Аудит управления учетными записями

6.7.3. Технология защищенного канала

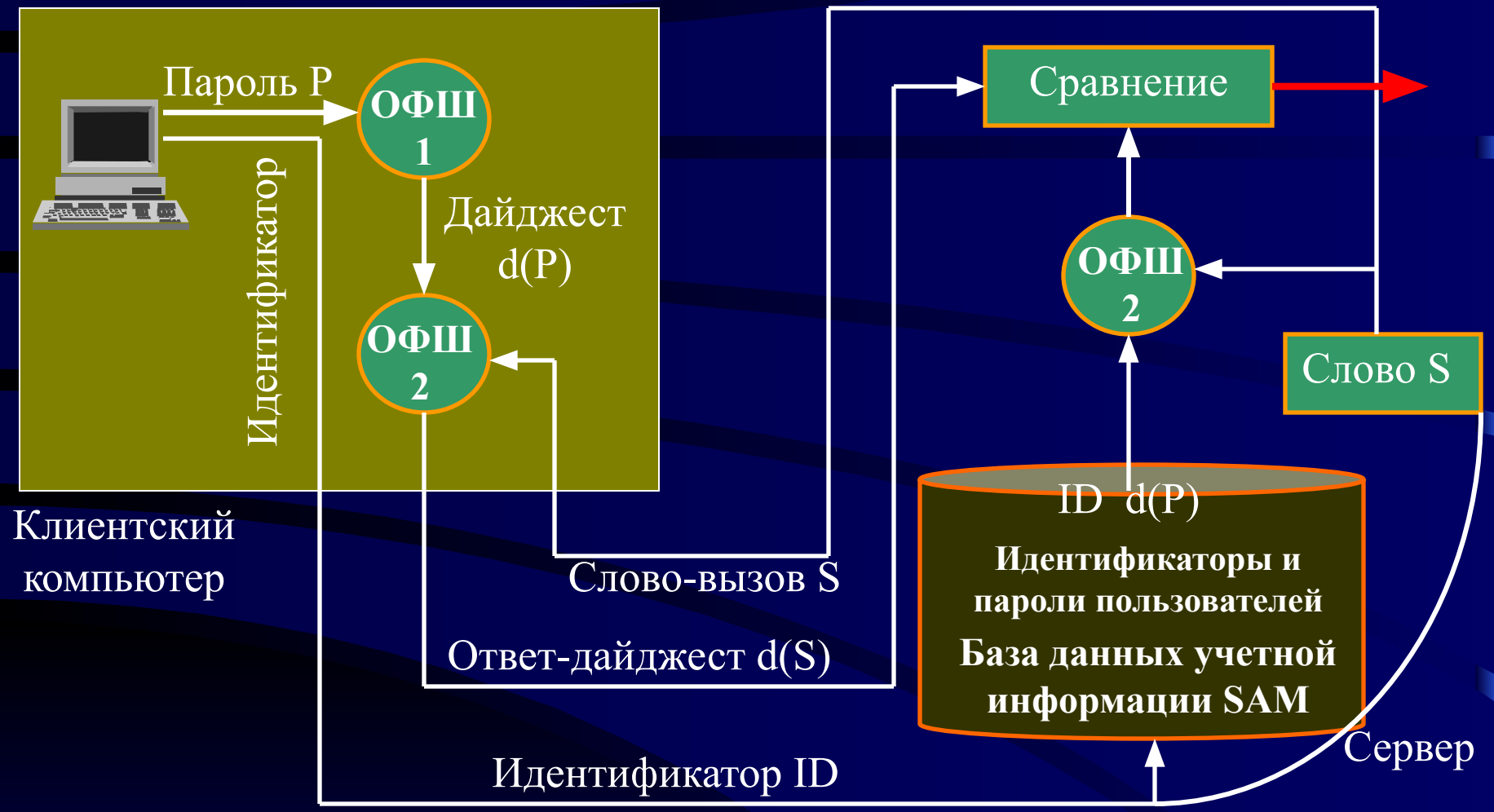
Функции защищенного канала: 1.
Взаимная аутентификация абонентов при установлении соединения (например, обменом паролями);
2. Защита передаваемых по каналу сообщений от несанкционированного доступа путем шифрования;
3. Подтверждение целостности поступающих по каналу сообщений (например, передачей с сообщением его дайджеста).



Схемы образования защищенного канала: 1. Программными средствами , установленными на удаленных компьютерах ЛВС предприятия.
2. Оборудованием поставщика услуг публичной сети, расположенным на границе между частной и публичной сетями.

6.8. Технологии аутентификации

6.8.1. Сетевая аутентификация на основе многоразового пароля



S – слово-вызов - случайное число случайной длины, меняется при каждом вызове.
SAM – Security Accounts Manager – менеджер учетных записей.
ОФШ2 – параметрическая функция одностороннего шифрования.

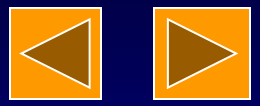
6.8.2. Аутентификация с использованием одноразового пароля

1. Программная или аппаратная генерация паролей с помощью карточек со встроенным микропроцессором (аппаратный ключ), подключаемых к устройству клиентской станции.

2. Алгоритм (Лесли Лампорт) основан на необратимой функции Y = f (X), для которой по заданному X легко найти Y, но по известному Y подобрать X невозможно. Вход и выход должны иметь одинаковую длину (например, 128 битов).

Пользователь выбирает секретный пароль S и целое число n (n >> 1), означающее количество одноразовых паролей. Пусть n = 4, тогда первый пароль получается n-кратным применением необратимой функции f (X), т.е. $P_1 = f(f(f(f(S))))$, $P_2 = f(f(f(S)))$ и т. д. , таким образом, $P_{i-1} = f(P_i)$. По известному P_2 легко найти P_1, но невозможно определить P_3.

На сервере хранится число $P_0 = f(P_1)$, имя пользователя и число 1, указывающее, что следующий пароль равен $f(P_1)$.



Алгоритм входа в сеть:

1. Пользователь посылает на сервер свое имя.
2. Сервер высылает в ответ число 1.
3. Машина пользователя отвечает числом P_1, вычисляемым из S, вводимым пользователем.
4. Сервер вычисляет $f(P_1)$ и сравнивает его со значением P_0, хранящимся в файле паролей.
5. Если значения совпадают, регистрация разрешается, целое число увеличивается на 1, а P_1 записывается в файл поверх P_0.

При следующем входе в систему сервер посылает пользователю число 2, машина пользователя вычисляет P_2, сервер вычисляет $f(P_2)$ и сравнивает его с хранящемся в файле значением P_1. Если эти значения совпадают, регистрация разрешается, целое число увеличивается на 1, а P_2 записывается в файл паролей поверх P_1 и т. д.

6.8.3. Аутентификация информации

(Установление подлинности данных, т.е. защита от навязывания ложной информации)

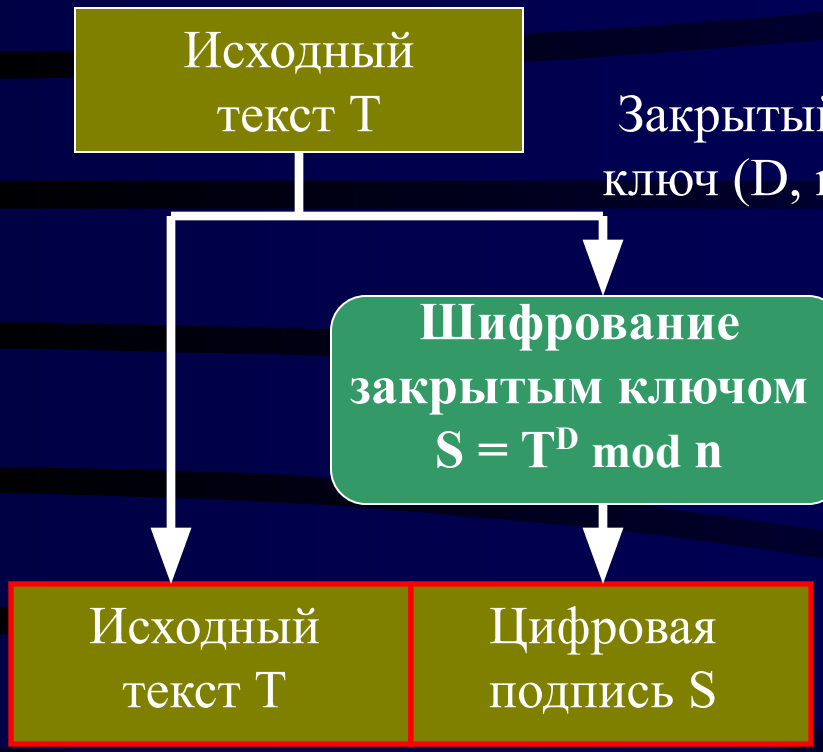


Схема формирования цифровой подписи по алгоритму RSA (асимметричная схема аутентификации)

Сообщение посылается в виде пары (T, S). Пользователь, имеющий открытый ключ (E, n), отделяет открытую часть T, расшифровывает цифровую подпись S и проверяет равенство $T = S^E \bmod n$.

Если результат расшифровки цифровой подписи совпадает с открытой частью сообщения, то считается , что документ подлинный.

Недостаток: длина подписи равна длине сообщения.

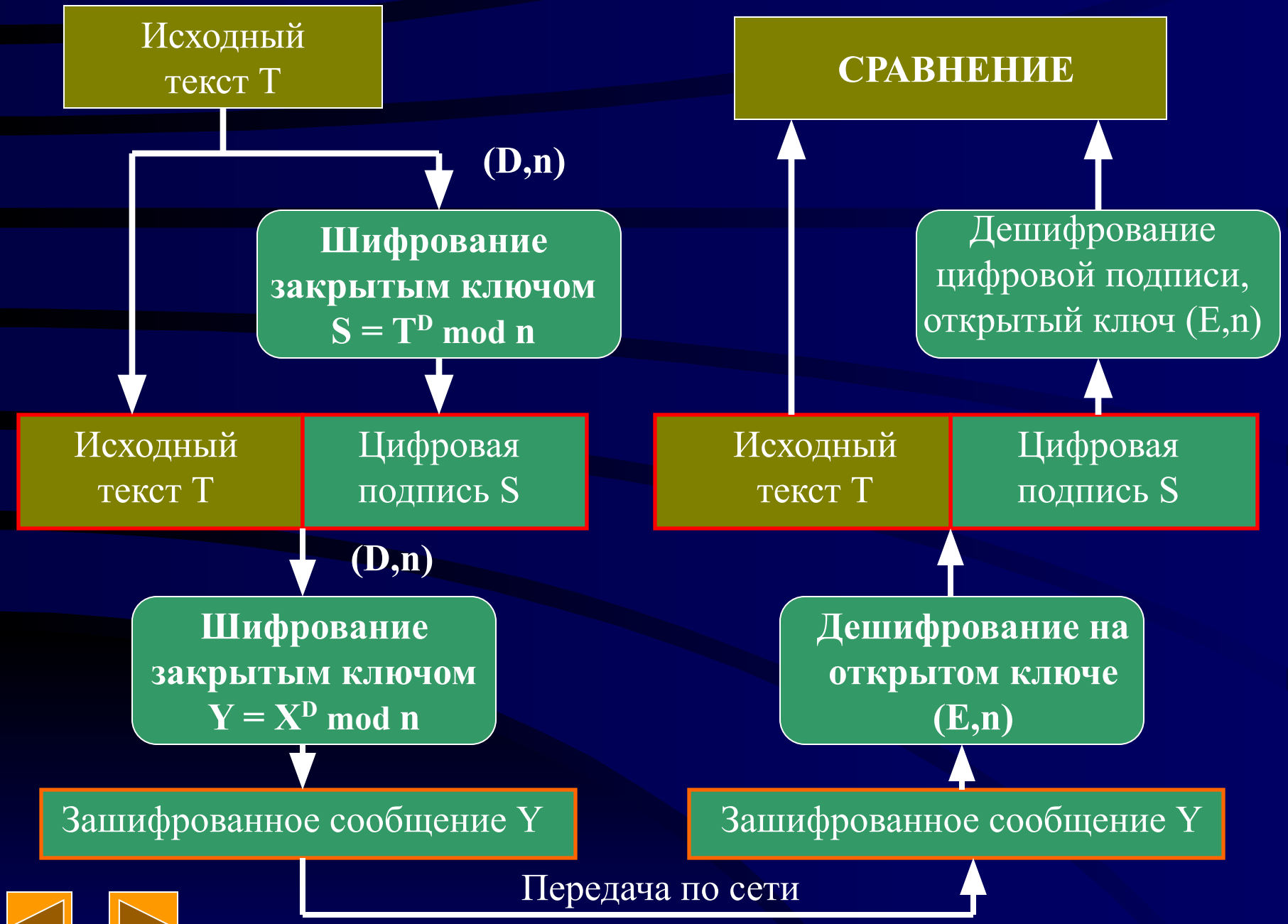
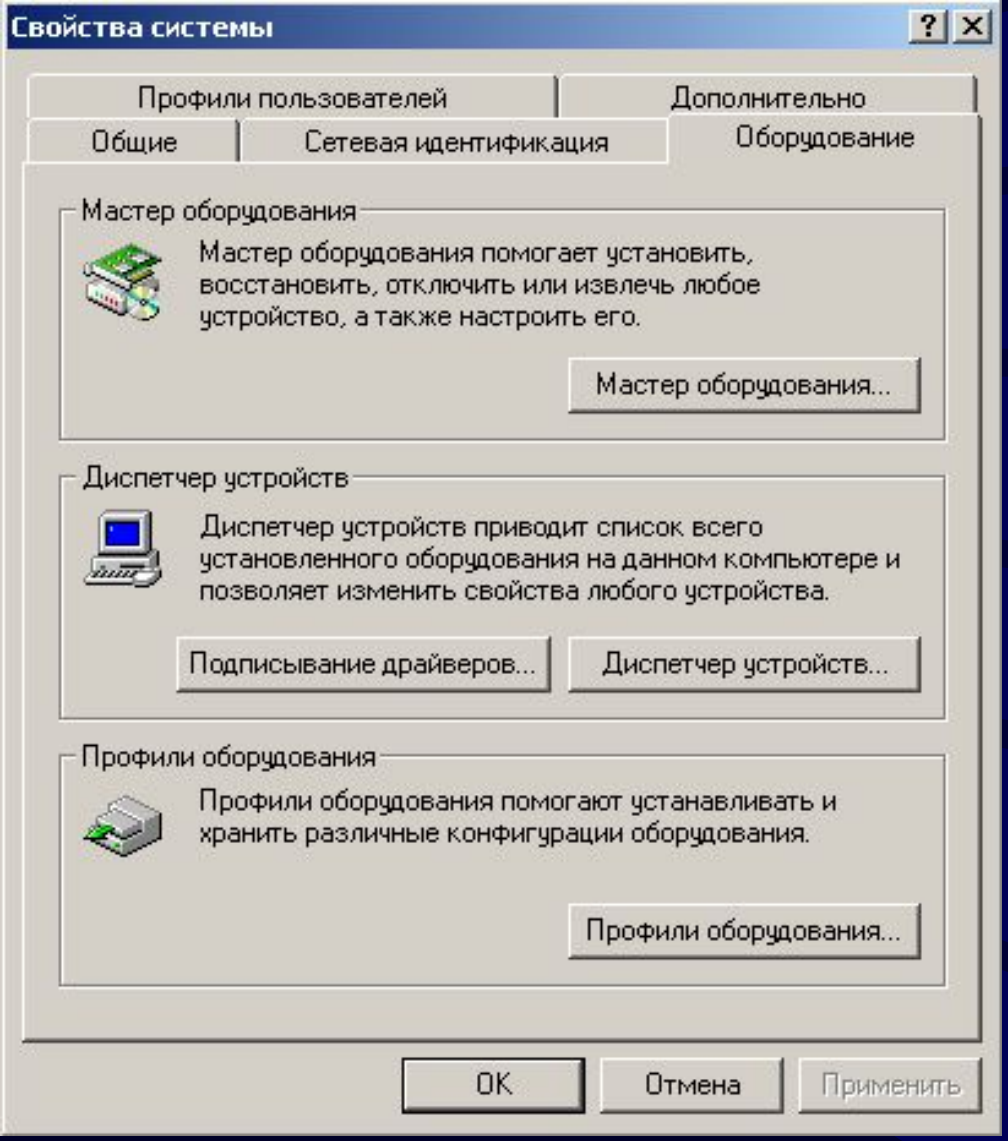
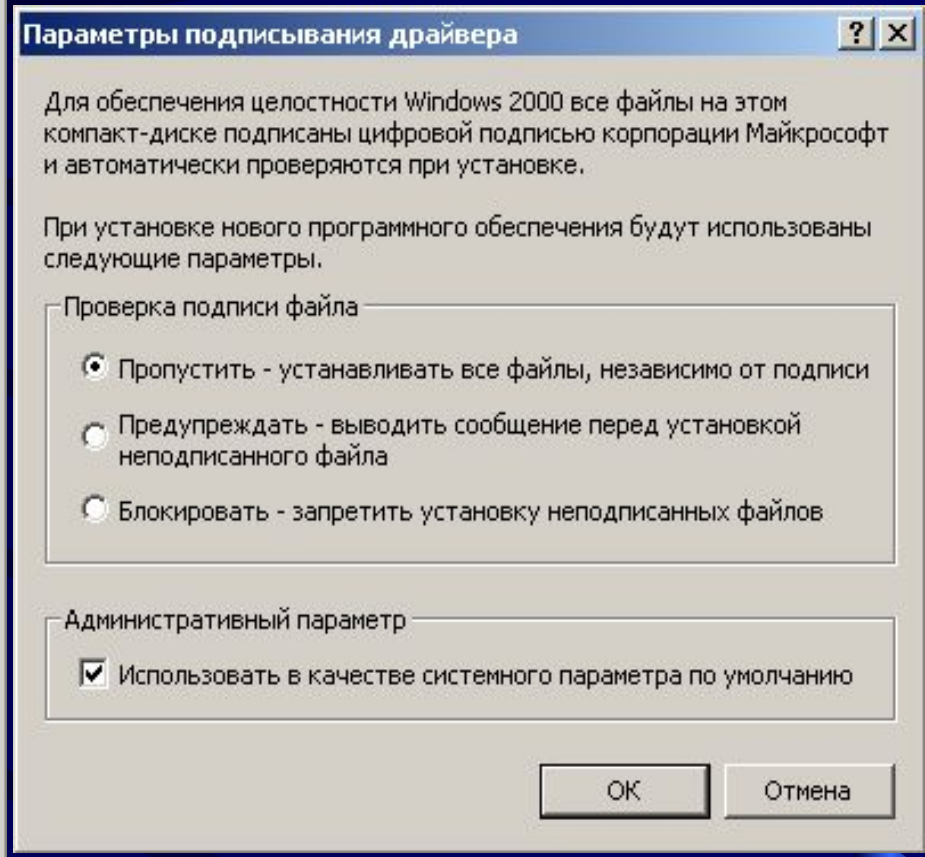
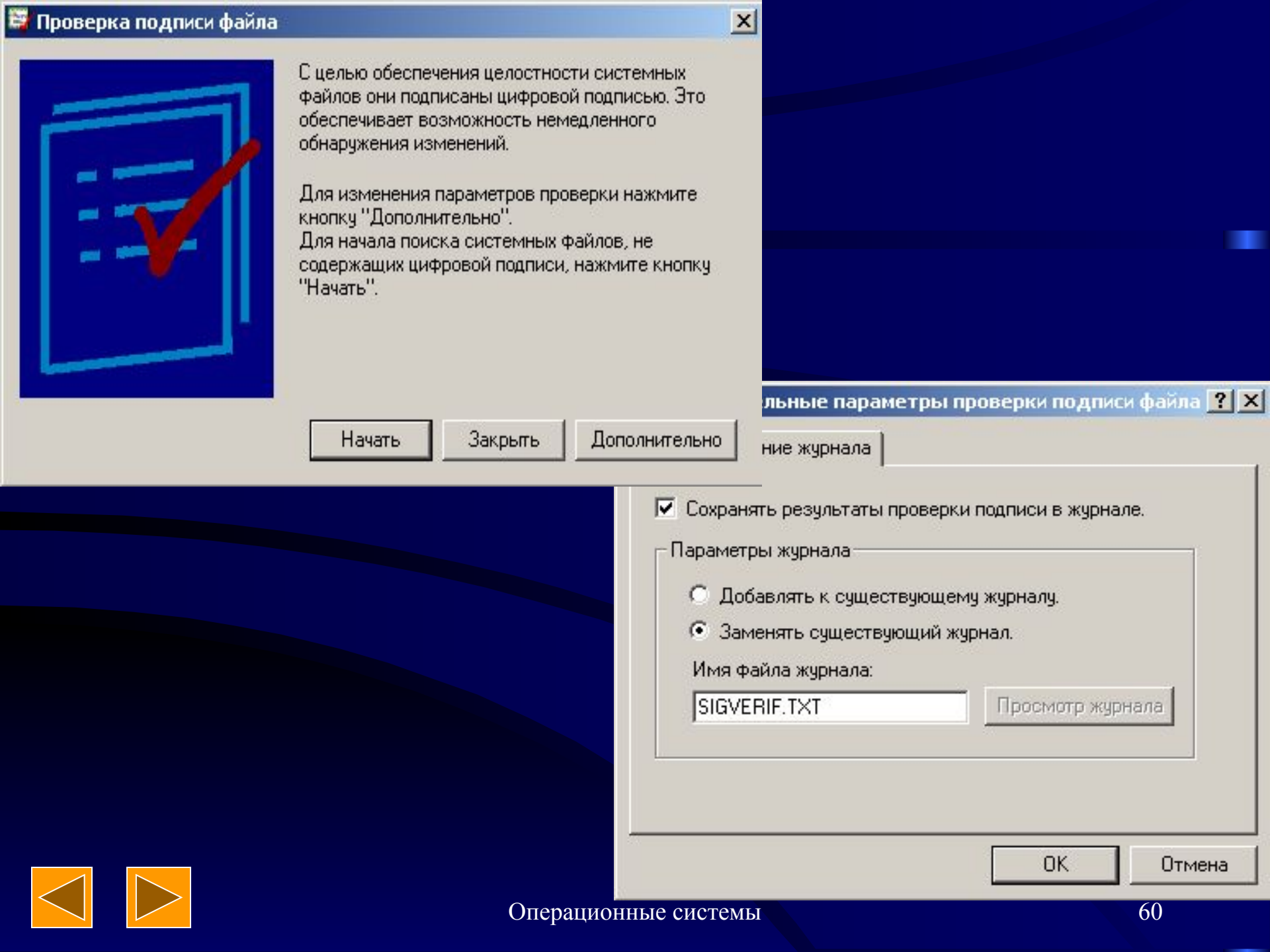

Исходный текст T
(D,n)
Шифрование закрытым ключом $S = T^D \bmod n$
Исходный текст T
Цифровая подпись S
(D,n)
Шифрование закрытым ключом $Y = X^D \bmod n$
Зашифрованное сообщение Y
Передача по сети
Зашифрованное сообщение Y
Дешифрование на открытом ключе (E,n)
Исходный текст T
Цифровая подпись S
Дешифрование цифровой подписи, открытый ключ (E,n)
СРАВНЕНИЕ

Схема получения аутентикода (разработана MS для доказательства аутентичности программ, распространяемых через Интернет)


Свойства системы
Профили пользователей
Дополнительно
Общие
Сетевая идентификация
Оборудование
Мастер оборудования
Мастер оборудования помогает установить, восстановить, отключить или извлечь любое устройство, а также настроить его.
Мастер оборудования...
Диспетчер устройств
Диспетчер устройств приводит список всего установленного оборудования на данном компьютере и позволяет изменить свойства любого устройства.
Подписывание драйверов...
Диспетчер устройств...
Профили оборудования
Профили оборудования помогают устанавливать и хранить различные конфигурации оборудования.
Профили оборудования...
OK
Отмена
Применить


Параметры подписывания драйвера
Для обеспечения целостности Windows 2000 все файлы на этом компакт-диске подписаны цифровой подписью корпорации Майкрософт и автоматически проверяются при установке.
При установке нового программного обеспечения будут использованы следующие параметры.
Проверка подписи файла
Пропустить - устанавливать все файлы, независимо от подписи
Предупреждать - выводить сообщение перед установкой неподписанного файла
Блокировать - запретить установку неподписанных файлов
Административный параметр
Использовать в качестве системного параметра по умолчанию
OK
Отмена


Проверка подписи файла
С целью обеспечения целостности системных файлов они подписаны цифровой подписью. Это обеспечивает возможность немедленного обнаружения изменений.
Для изменения параметров проверки нажмите кнопку "Дополнительно".
Для начала поиска системных файлов, не содержащих цифровой подписи, нажмите кнопку "Начать".
Начать
Закрыть
Дополнительно
льные параметры проверки подписи файла
ние журнала
Сохранять результаты проверки подписи в журнале.
Параметры журнала
Добавлять к существующему журналу.
Заменять существующий журнал.
Имя файла журнала:
SIGVERIF.TXT
Просмотр журнала
OK
Отмена

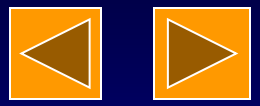
6.9. Система Kerberos

Принципы системы:

1. Все процедуры аутентификации между клиентами и серверами сети выполняются через посредника (Kerberos), которому доверяют обе стороны.
2. Клиент должен доказывать свою аутентичность для доступа к каждой нужной ему службе.
3. Все обмены по сети выполняются с использованием алгоритма шифрования DES .
4. Сетевая служба Kerberos построена по архитектуре клиент-сервер.

Доступ к ресурсу состоит из следующих этапов:

- (1) определение легальности клиента, логический вход в сеть, получение разрешения на продолжение процесса доступа к ресурсу;
- (2) получение разрешения на обращение к ресурсному серверу;
- (3) получение разрешения на доступ к ресурсу.



Kerberos-сервер

10 законов безопасности компьютеров

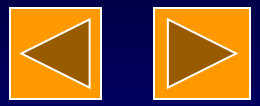
10. Если “плохой парень” может запускать свои программы на Вашем компьютере – это больше не Ваш компьютер.

9. Если “плохой парень” может изменить настройки операционной системы на Вашем компьютере – это больше не Ваш компьютер.

8. Если “плохой парень” имеет неограниченный физический доступ к Вашему компьютеру – это больше не Ваш компьютер.

7. Если Вы разрешаете “плохому парню” загружать исполняемые файлы на Ваш Веб-сайт – это больше не Ваш Веб-сайт.

6. Слабые пароли сводят на нет сильную систему защиты.



10 законов безопасности компьютеров

5. Машина защищена ровно настолько, насколько Вы уверены в своем администраторе.

4. Зашифрованные данные защищены ровно настолько, насколько защищен ключ шифрования.

3. Устаревший антивирусный сканер не намного лучше, чем отсутствие сканера вообще.

2. Абсолютной анонимности практически не бывает, ни в реальной жизни, ни в Интернете.

1. Технологии – не панацея.