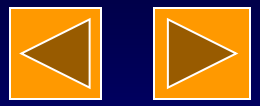
Операционные среды, системы и оболочки

Тема 6. Безопасность, диагностика и восстановление ОС после отказов

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



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.

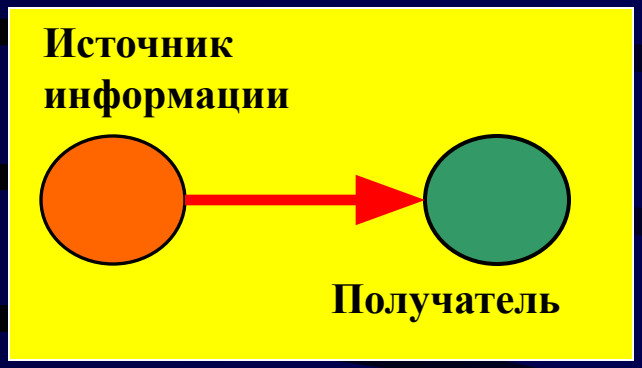
Риск – вероятностная оценка величины возможного ущерба в результате успешно проведенной атаки.

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.

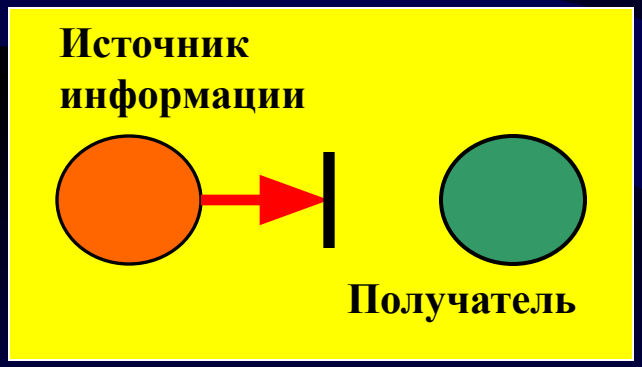
Умышленные угрозы – пассивное чтение данных, мониторинг системы, активные действия – нарушение целостности и доступности информации, приведение в нерабочее состояние приложений и устройств системы.

Типы умышленных угроз:

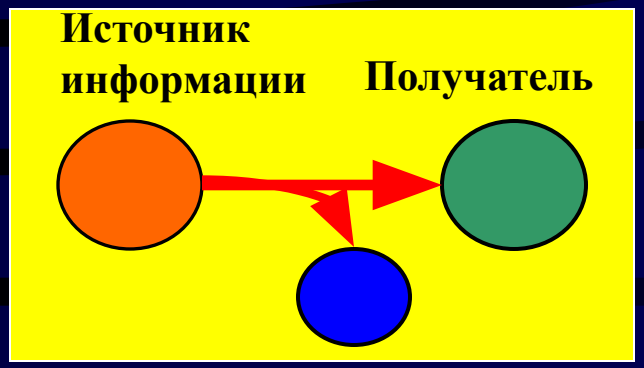
- незаконное проникновение в один из компьютеров сети под видом легального пользователя;
- разрушение системы с помощью программ-вирусов;
- нелегальные действия легального пользователя;
- подслушивание внутрисетевого трафика.



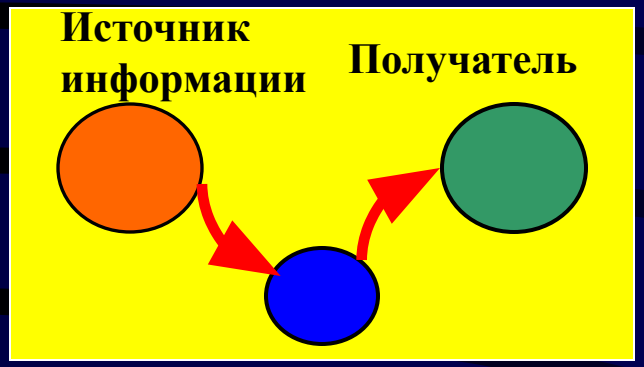
Нормальная передача. Информации от источника информации к получателю.



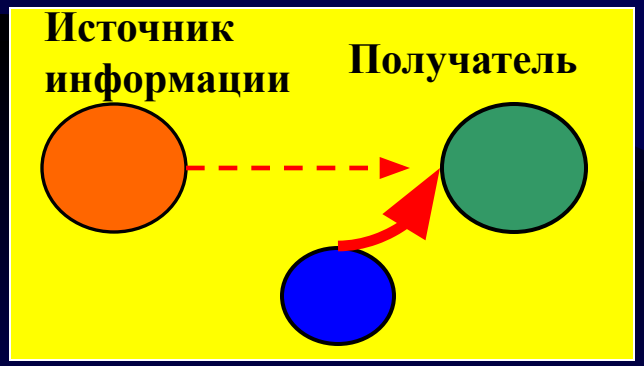
Прерывание. Компоненты системы выходят из строя, становятся недоступными или непригодными. Это атака , целью которой является **нарушение доступности.**



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.).

Почему надо заниматься безопасностью WEB приложений

Хакеры изучают уязвимости WEB приложений

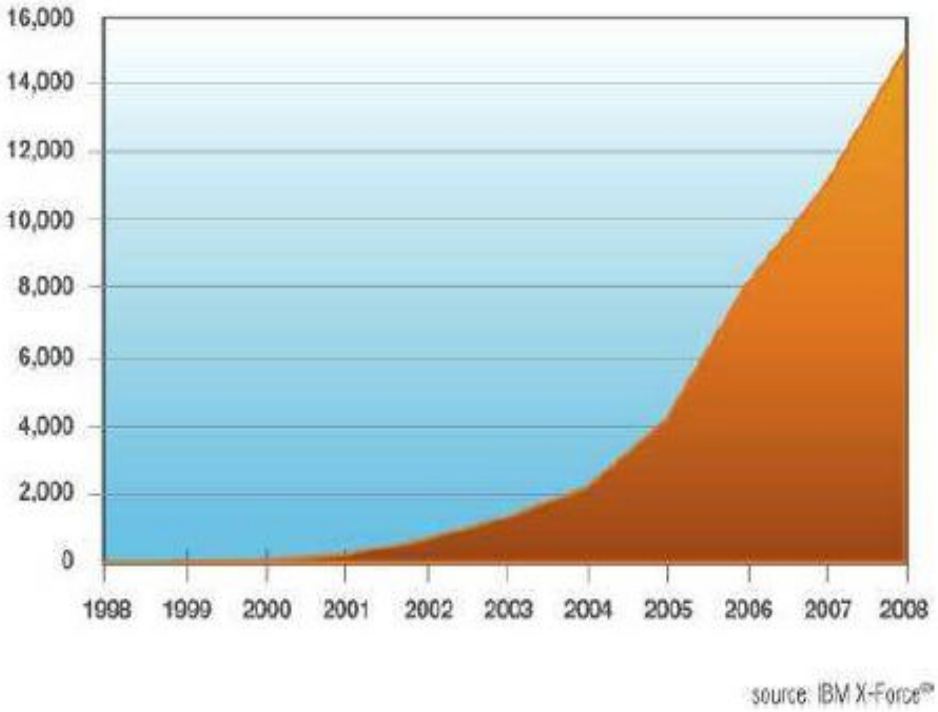
- **54.9%** от ВСЕХ найденных в 2008 уязвимостей – уязвимости WEB приложений
- **74%** от всех уязвимостей Web приложений в 2008 так и не были исправлены до конца года
- Атаки типа SQL injection выросли **в 30 раз** за последние 6 месяцев

Требование законодательства

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

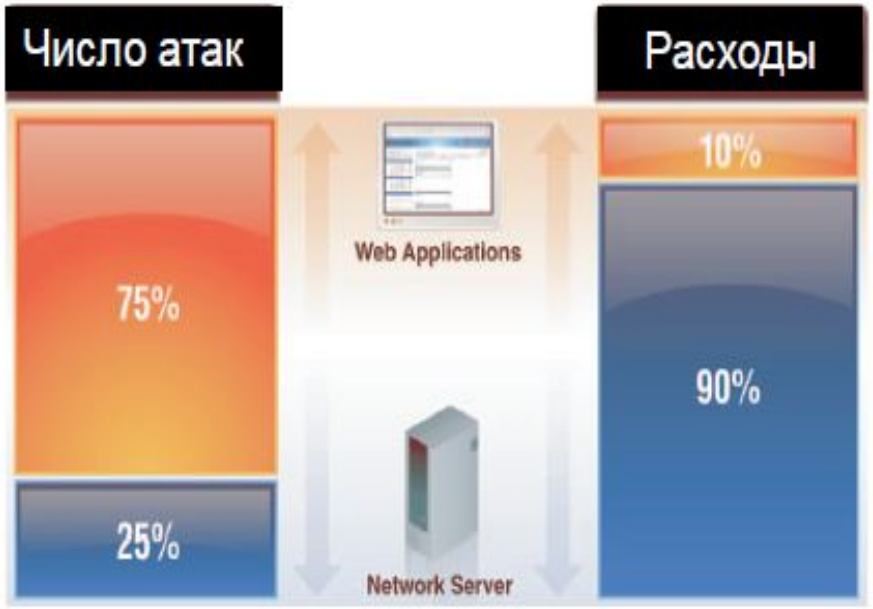
… это открытая и легкая точка для доступа и можно получить достаточно важных данных

Рост уязвимостей WEB приложений с 1998 до 2008 года



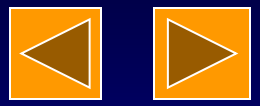
Традиционные решения упускают из вида или неэффективно защищают WEB приложения

- 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



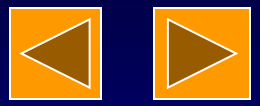
6.2.3. Случайная потеря данных

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



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.

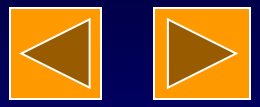


6.5. Политика безопасности

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:

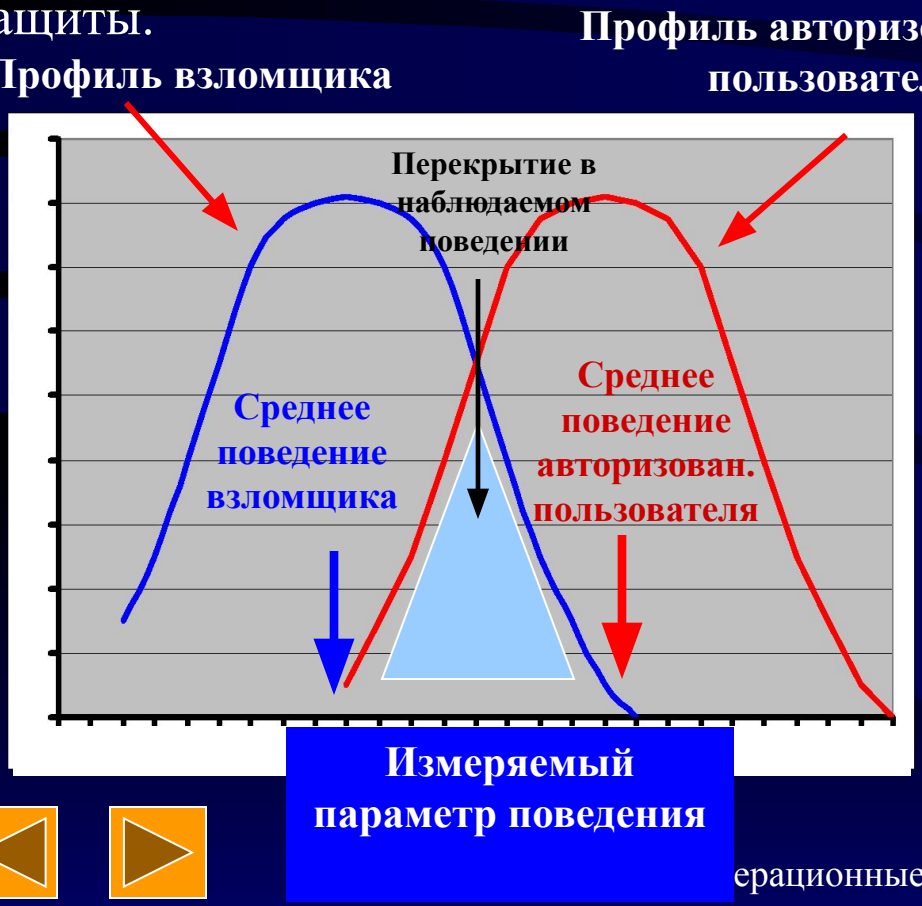
1. **Минимальный уровень привилегий на доступ к данным.**
2. **Комплексный подход к обеспечению безопасности.**
3. **Баланс надежности защиты всех уровней.**
4. **Использование средств, обеспечивающих максимальную защиту при атаке (например, полная блокировка автоматического пропускного пункта при его 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.**



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.**

6.7.2. Аутентификация, пароли, авторизация, аудит

- **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.

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.

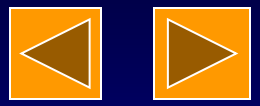
Аудит (auditing) – фиксация в системном журнале событий, происходящих в операционной системе, имеющих отношение к безопасности и связанных с доступом к защищаемым системным ресурсам.

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.**

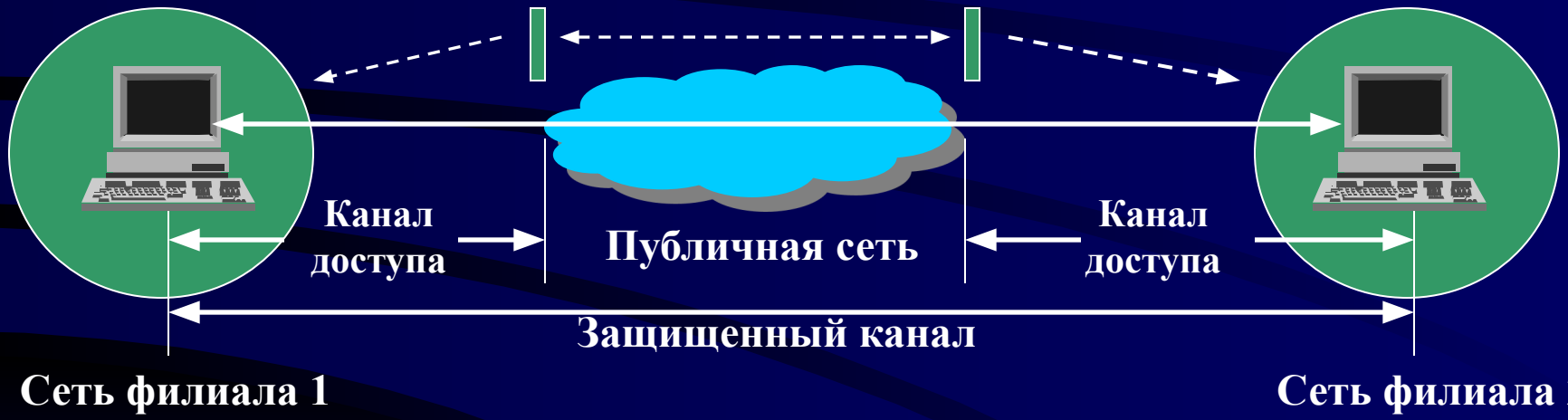
Аудит включается в локальной (групповой) политике аудита.

Журнал безопасности содержит записи, связанные с системой безопасности.



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.

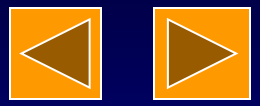
6.9. Система Kerberos

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.



10 законов безопасности компьютеров

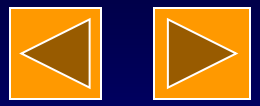
10. Если “плохой парень” может запускать свои программы на Вашем компьютере – это больше не Ваш компьютер.

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.