Проблемы обеспечения безопасности информационных систем и технологий

- **Год от года зависимость людей, обществ и государств от информационных технологий становится все более сильной и масштабной.**
- **Сегодня уже физическая реальность начинает выступать своего рода дополнением к реальности виртуальной. Все большую роль в нашей жизни начинают играть киберфизические системы.**
- **Глобальные информационные сети выступают своего рода мозгом и нервной системой для мира, в котором мы обретаемся физически.**

А что бывает с человеком, когда повреждается его мозг или нервная система?

- **Возможный ущерб от "информационного оружия" и злонамеренных действий в киберпространстве может быть сравним с оружием массового поражения**. (Не случайно создатели киберкомандования в США высказывают идею превращения кибервойск в четвертый вид вооруженных сил).

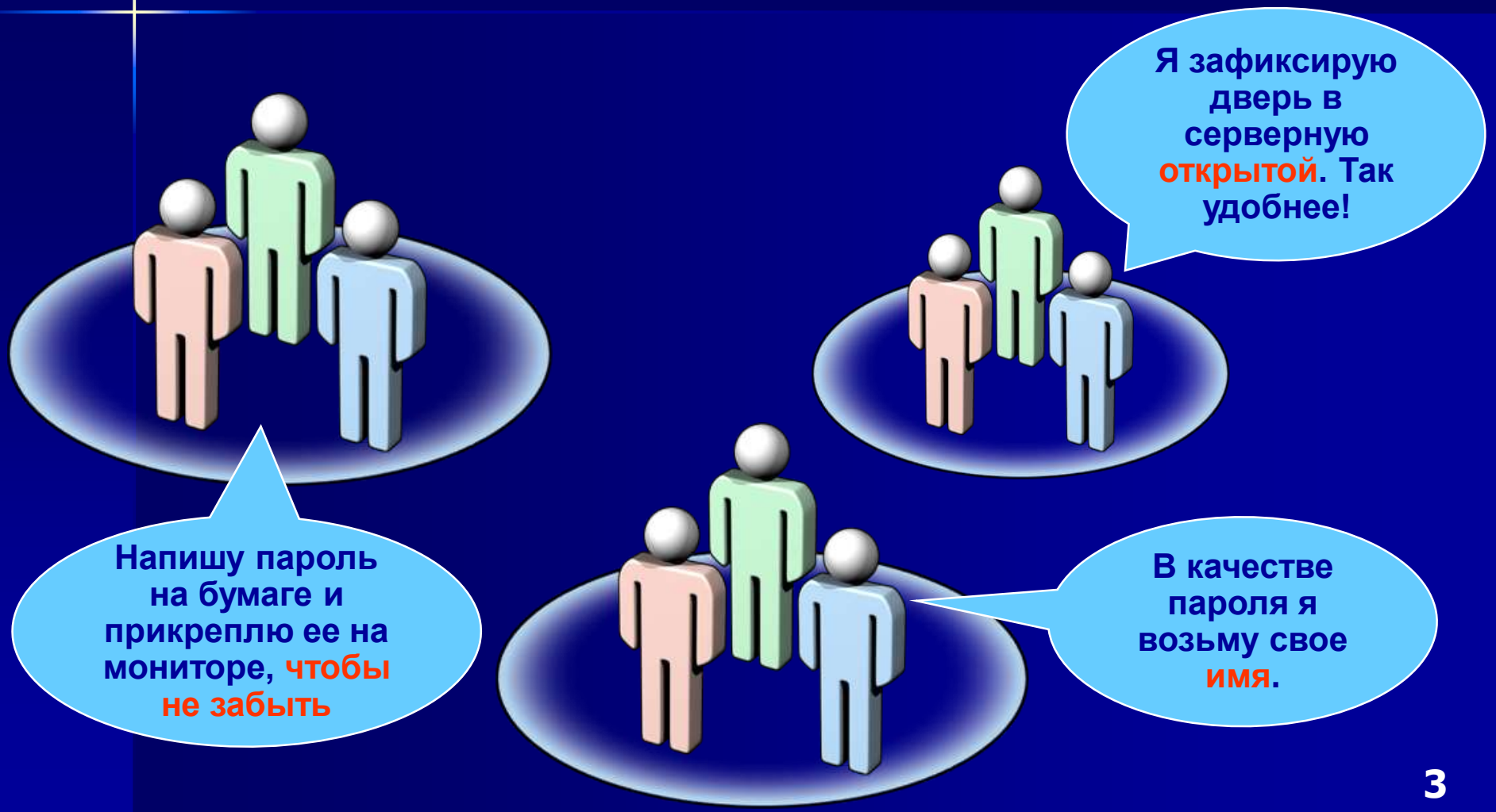
Сущность понятия «информационная **безопасность**»

- **информационная безопасность** — это *состояние* защищённости информационной среды
- **безопасность информации (при применении информационных технологий)** (англ. *IT security*) включает:

а) состояние защищенности информации (данных) от несанкционированного доступа к ней и от влияния дестабилизирующих факторов;

в) информационную безопасность автоматизированной информационной системы, в которой она реализована.

Пользователи часто забывают о безопасности



Последствия нарушения безопасности

Потери доходов

Ухудшение репутации

Снижение доверия инвесторов

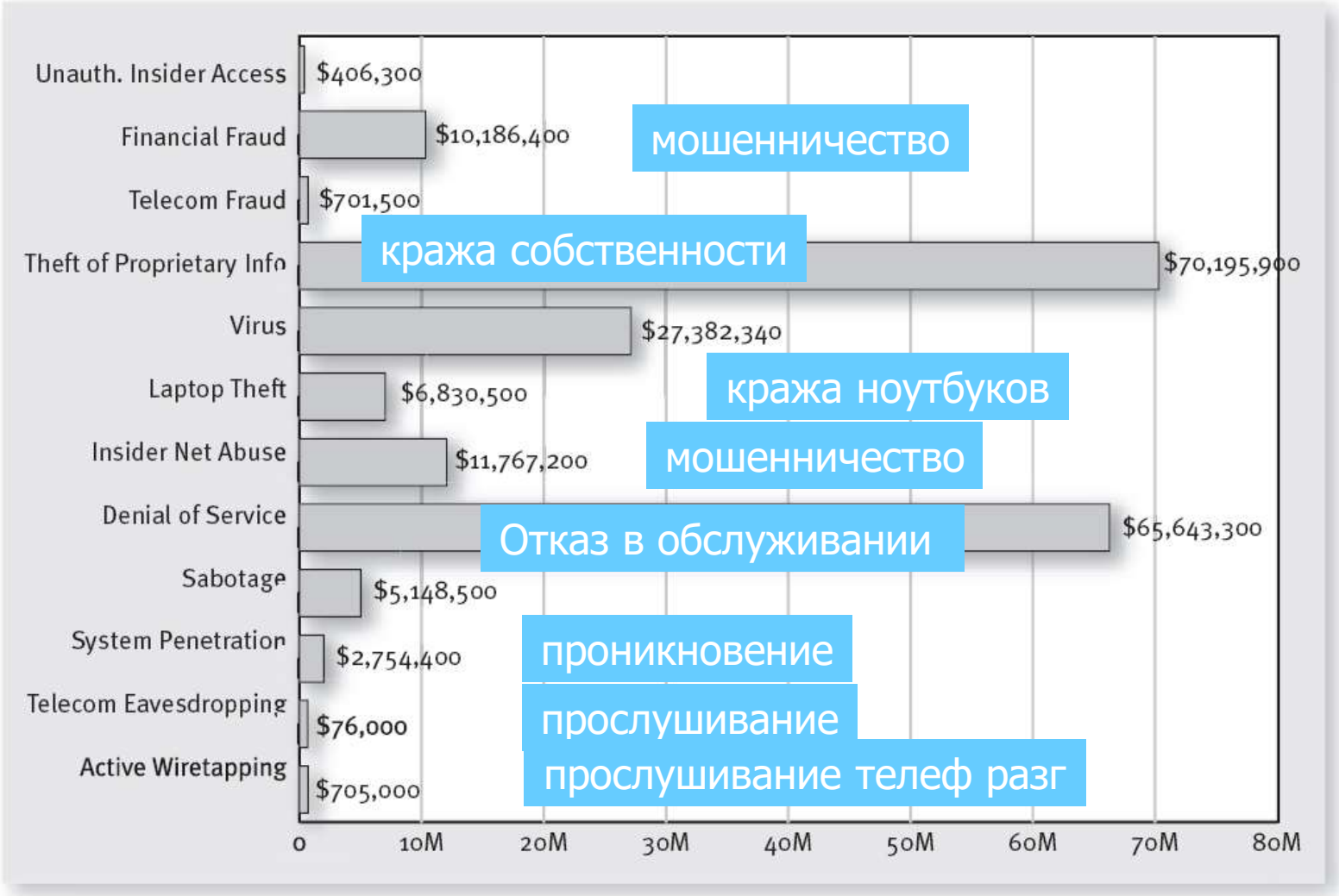
Потеря или компрометация данных

Снижение доверия клиентов

Правовые последствия

Нарушение бизнес-процесса

Финансовые потери



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 251 Respondents/47%

Исторические аспекты возникновения и развития информационной безопасности

I этап — примерно до середины 19 века — характеризуется использованием естественно возникавших средств информационных коммуникаций. Основная задача информационной безопасности - защита сведений о событиях, фактах, имуществе….

II этап — начиная с середины 19 века — связан с началом использования технических средств электро- и радиосвязи. Характеризуется применением помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

- **III этап** — начиная с 1935 года — связан с появлением радиолокационных и гидроакустических средств.
- Обеспечение информационной безопасности - сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активных и пассивных помех.
- **IV этап** — начиная с 1946 года — связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров).
- Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств сбора, переработки и передачи информации.

V этап — начиная с 1965 года — обусловлен созданием и развитием локальных информационно-коммуникационных сетей. . Задачи безопасности решались, в основном, методами и способами физической защиты средств , путём администрирования и управления доступом к сетевым ресурсам.

VI этап — начиная с 1973 года — связан с использованием мобильных коммуникационных устройств с широким спектром задач.

Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран.

- Формируется информационное право — новая отрасль международной правовой системы.

VII этап — начиная с 1985 года — связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения.

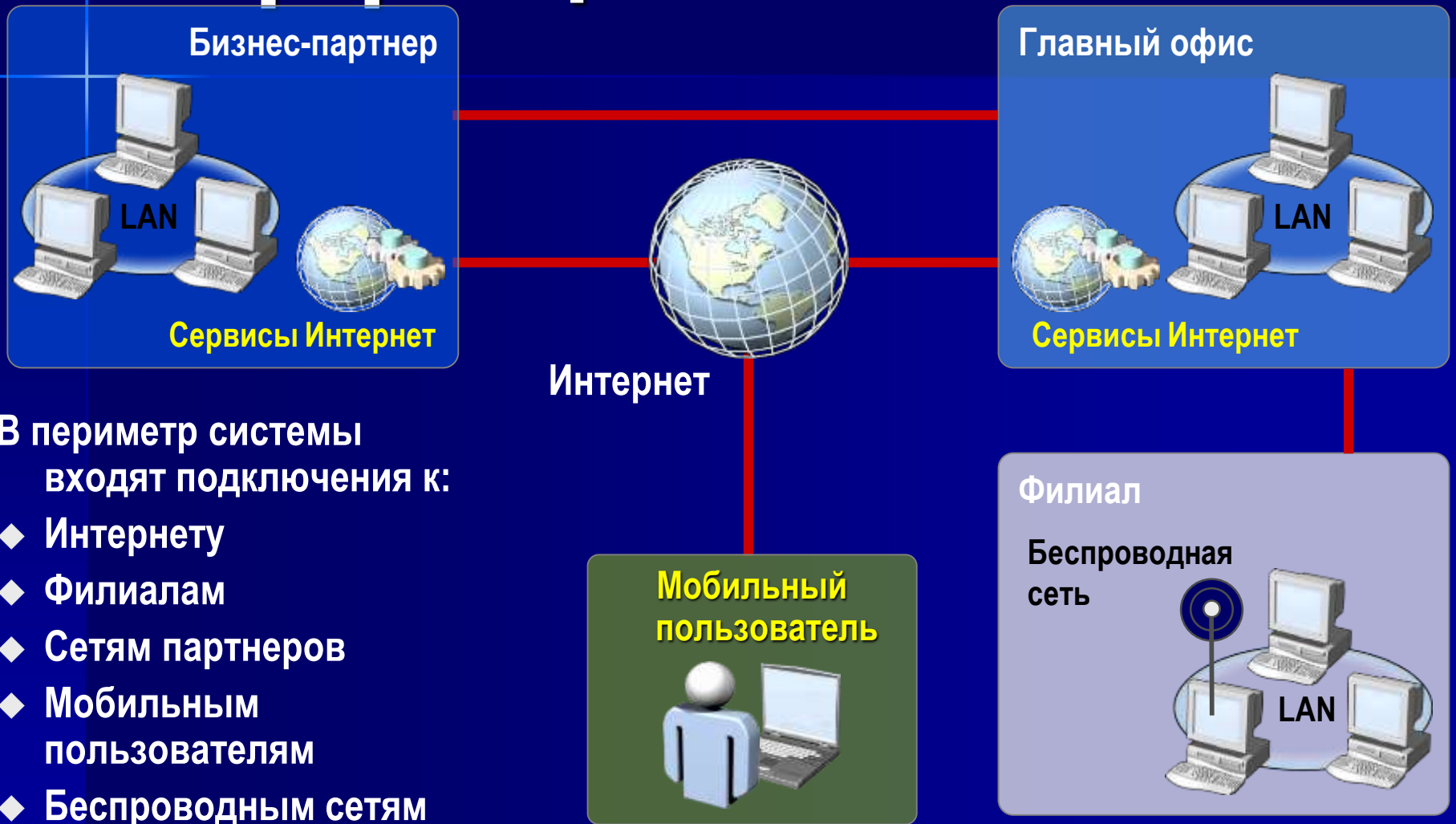
Предусматривает комплексное использование мер и средств защиты.

VIII этап — примерно с конца 20 - начала 21 вв. — связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами.

Широкий переход «на цифру».

Предусматривает комплексное использование мер и средств защиты.

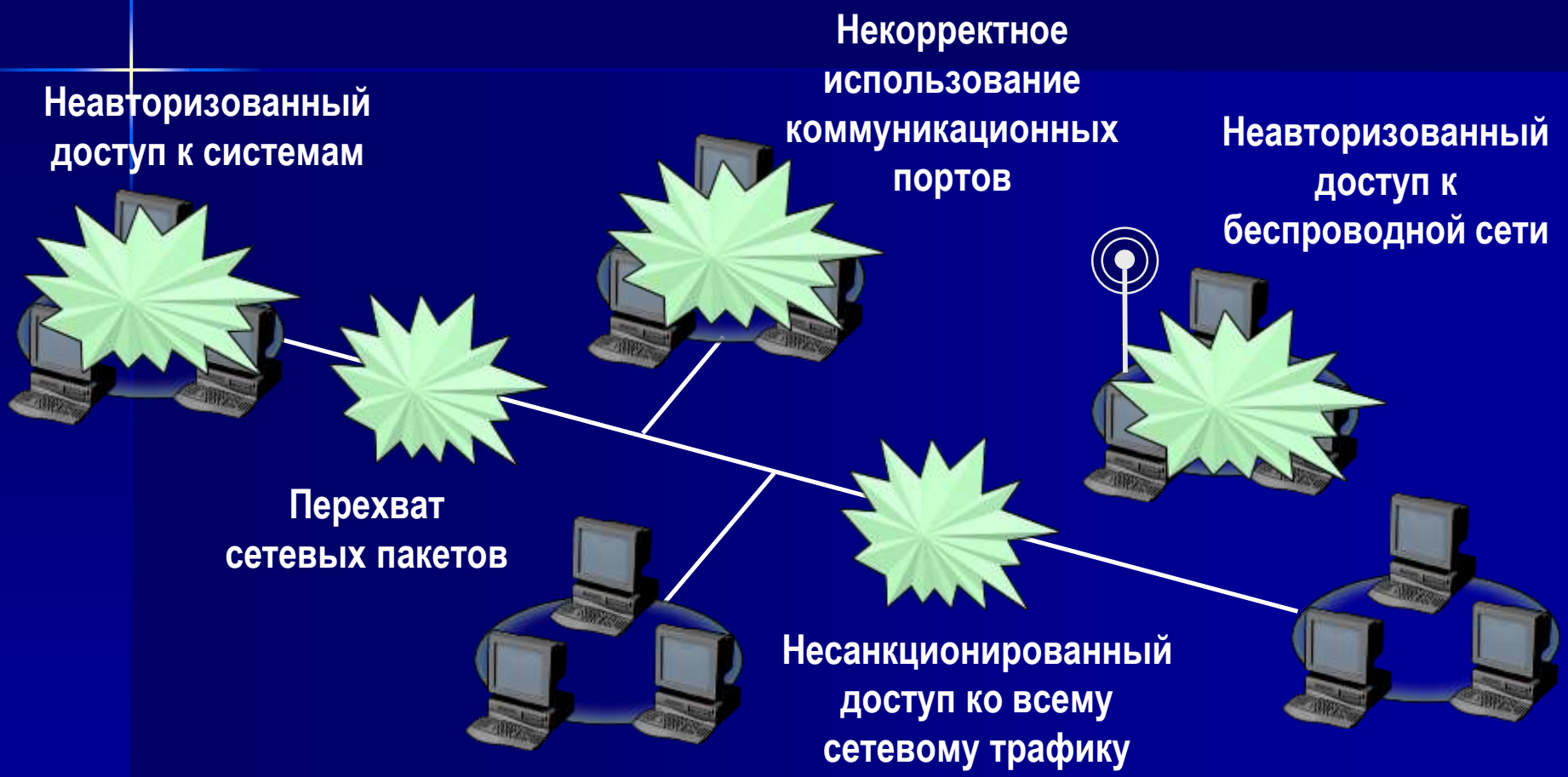
Пример периметра современной информационной системы



В периметр системы входят подключения к:

- Интернету
- Филиалам
- Сетям партнеров
- Мобильным пользователям
- Беспроводным сетям
- Интернет-приложениям

Угрозы локальной сети



Современная оценка и анализ объектов

Приоритеты объектов (шкала от 1 до 10)

1. Сервер обеспечивает базовую функциональность и не влияет на финансовую сторону бизнеса
3. Сервер содержит важную информацию, данные могут быть быстро восстановлены
5. Сервер содержит важную информацию, восстановление данных потребует времени (Дочерние серверы DNS)
8. Сервер содержит важные бизнес-данные, его потеря существенно повлияет на продуктивность всех пользователей (Серверы файлов и печати, Порталы отделов)
10. Сервер имеет критически важное значение для бизнеса, его потеря повредит конкурентоспособности компании (Интранет-портал компании)

Идентификация угроз (STRIDE)

Тип угрозы	Примеры
Имитация (Spoofing)	▪ Подделка электронных сообщений ▪ Подделка ответных пакетов при аутентификации
Фальсификация (Tampering)	▪ Модификация данных, передаваемых по сети ▪ Модификация файлов
Отречение (Repudiation)	▪ Удаление критичного файла или совершение покупки с последующим отказом признавать свои действия
Раскрытие информации (Information disclosure)	▪ Несанкционированный доступ или незаконная публикация конфиденциальной информации
Отказ в обслуживании (Denial of service) **Проблема botnet**	▪ Заполнение сети пакетами «SYN» ▪ Загрузка сетевого ресурса большим количеством поддельных пакетов ICMP
Повышение привилегий (Elevation of privilege)	▪ Получение системных привилегий через атаку с переполнением буфера ▪ Незаконное получение административных прав либо незаконная их передача с целью наживы

Почтовые черви

- Периметр
  - Сканирование всех вложений на шлюзе SMTP
- Внутренняя сеть
  - Проверить хосты, подключаемые через Службу удаленного доступа, на наличие актуальных обновлений
    и сигнатур вирусов
- Приложения
  - Office XP et Office 200x
    - Усиленная защита от почтовых вирусов включена по умолчанию
- Пользователи
  - Правила обращения с файлами в почтовых вложениях
    - «**Не открывайте файлы, если вы не уверены, что это безопасно**»

Разработка и внедрение политики безопасности

- Управление конфигурациями
- Управление обновлениями
- Мониторинг систем
- Аудит систем
- Операционные политики
- Операционные процедуры

Защита на всех уровнях

- Упрощает процесс обнаружения вторжения
- Снижает шансы атакующего на успех

Списки контроля доступа, шифрование

Защита приложений, антивирусные системы

Защита ОС, управление обновлениями, аутентификация

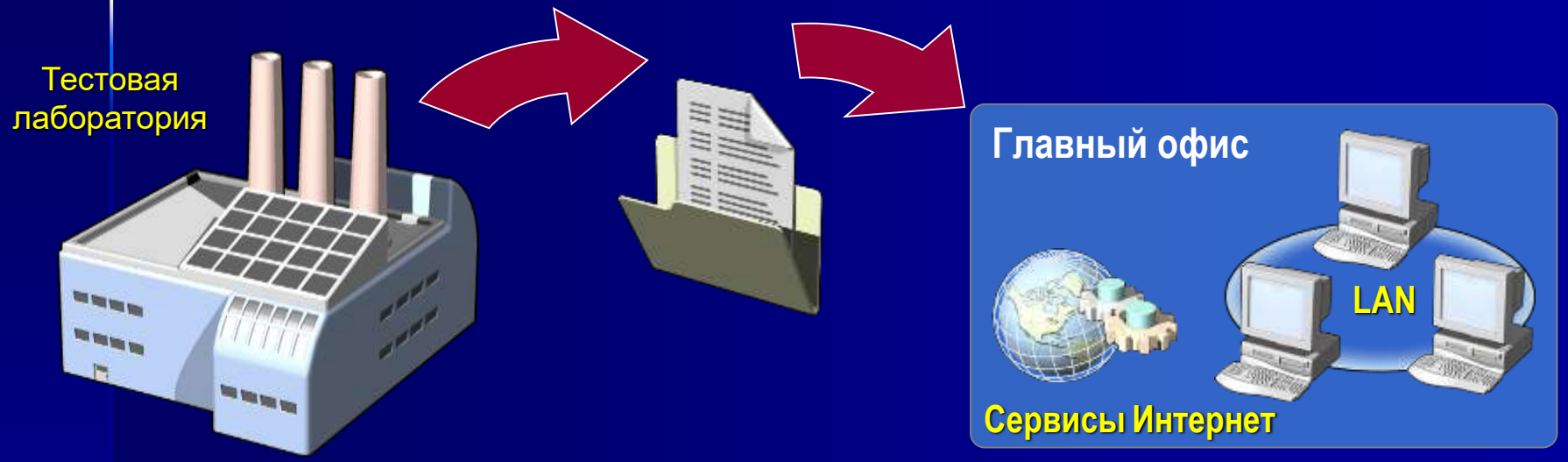
Сегментация сети, IP Security, Система обнаружения вторжений

Межсетевые экраны, Карантин VPN-соединений

Охрана, средства наблюдения

Обучение пользователей

Сохранение знаний и обучение



- Формализация процесса накопления знаний и опыта, полученных при анализе угроз и уязвимостей системы
- Последующее обучение персонала

Современные проблемно-ориентированные методы и средства защиты

Предусматривают защиту:

- от несанкционированного доступа и/или использования (проблема администраторов);
- от различных типов вирусов;
- от утечки информации по каналам электромагнитного излучения

Современные проблемно-ориентированные методы и средства защиты

Основываются на:

- Организационных методах,
- Правовых методах,
- Технических методах,
- Аппаратных, программных и аппаратно-программных методах

Программно-технические способы и средства обеспечения информационной безопасности

1. Средства защиты от несанкционированного доступа (НСД):
   - Средства авторизации ;
   - Мандатное управление доступом;
   - Избирательное управление доступом;
   - Управление доступом на основе ролей;
   - Журналирование (так же называется Аудит).
2. Системы мониторинга сетей:
   - Системы обнаружения и предотвращения вторжений (IDS/IPS);
   - Системы предотвращения утечек конфиденциальной информации (DLP-системы).

3. Анализаторы протоколов.
4. Антивирусные средства.
5. Межсетевые экраны.
6. Криптографические средства:
   - Шифрование;
   - Цифровая подпись.
7. Системы резервного копирования.
8. Системы бесперебойного питания.
9. Системы аутентификации:
   - **Пароль;**
   - Сертификат;
   - Биометрия.
10. Средства контроля доступа в помещения.

Законы информационной безопасности

1. Если (bad fellow) “плохой парень” может запускать свои программы на Вашем компьютере – это больше не Ваш компьютер.
2. Если “плохой парень” может изменить настройки операционной системы на Вашем компьютере – это больше не Ваш компьютер.
3. Если “плохой парень” имеет неограниченный физический доступ к Вашему компьютеру – это больше не Ваш компьютер.
4. Если Вы разрешаете “плохому парню” загружать исполняемые файлы на Ваш Web-сайт – это больше не Ваш Web-сайт.
5. Слабые пароли сводят на нет сильную систему защиты.

Законы информационной безопасности

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

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

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

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

10. Технологии – не панацея.

http://www.microsoft.com/technet/columns/security/essays/10imlaws.asp

Информация

- Информационный ресурс Microsoft по безопасности
  - www.microsoft.com/security
  - Для профессионалов IT: www.microsoft.com/technet/security
  - На русском языке: http://www.microsoft.com/rus/security
- Руководства Microsoft по защите информационных систем
  - www.microsoft.com/security/guidance
- Computer Security Institute
  - http://www.gocsi.com