

ОСНОВЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Значение информационной безопасности

Последствия нарушения безопасности

**Потери
доходов**

**Ухудшение
репутации**

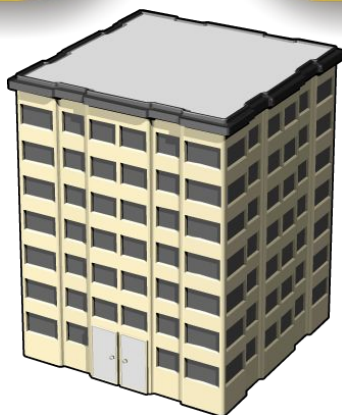
**Снижение
доверия
инвесторов**

**Потеря или
компрометация
данных**

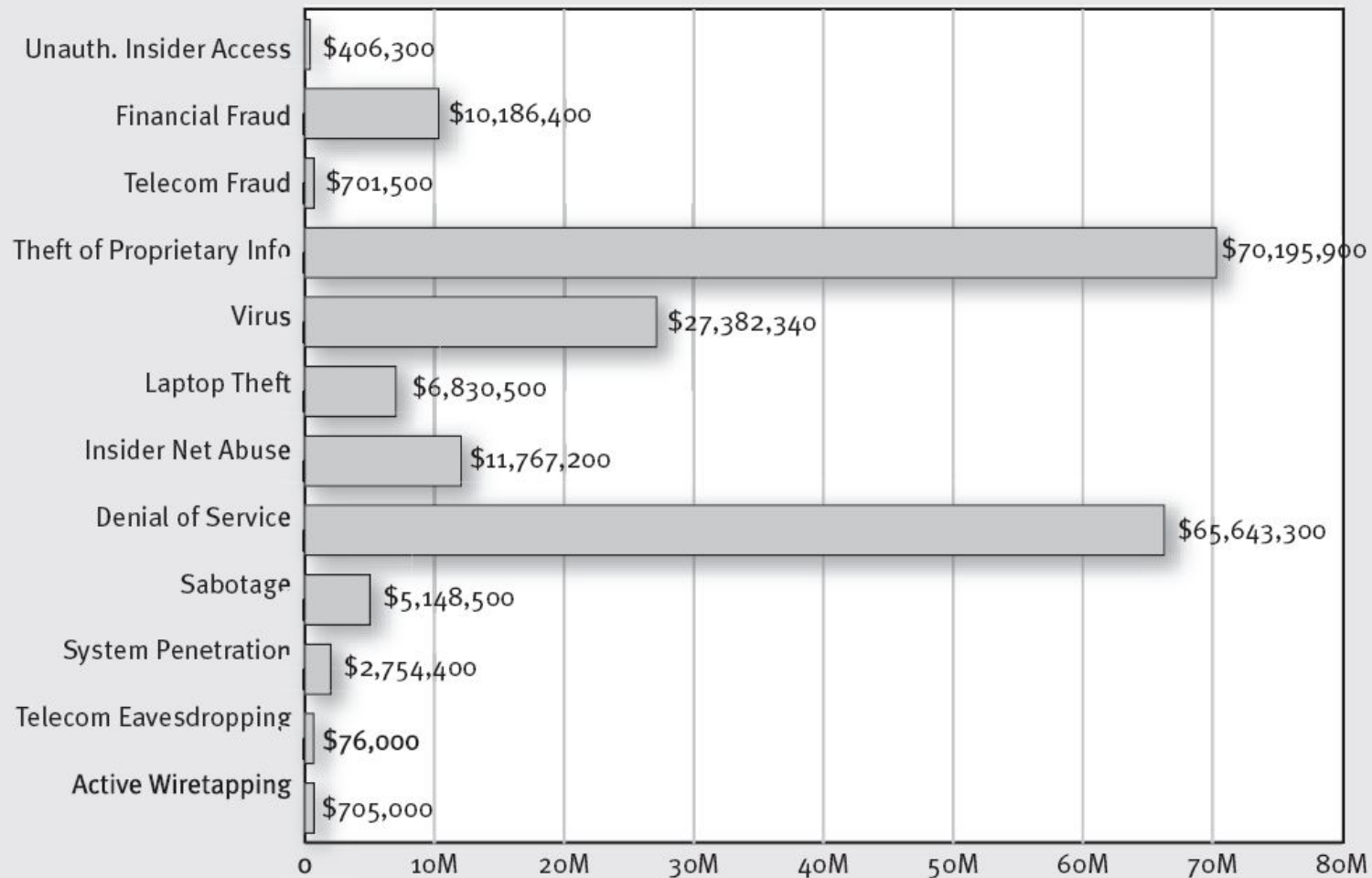
**Снижение
доверия
клиентов**

**Правовые
последствия**

**Нарушение
бизнес-
процесса**



Финансовые потери



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

2003: 251 Respondents/47%

Управление рисками

Дисциплина управления рисками

◆ Оценка



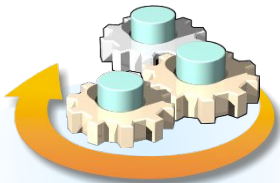
- Анализ объектов
- Идентификация угроз
- Анализ и расстановка приоритетов
- Планирование, назначение и отслеживание действий по работе с рисками

◆ Разработка и внедрение



- Разработка и тестирование процесса исправления
- Сохранение знаний

◆ Операции



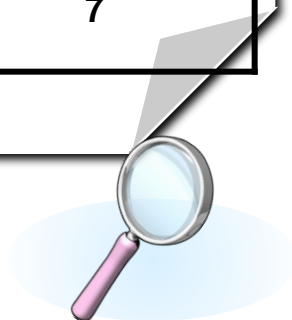
- Повторная оценка объектов и рисков
- Стабилизация и применение новых или измененных контрмер

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
8. Сервер содержит важные бизнес-данные, его потеря существенно повлияет на продуктивность всех пользователей
10. Сервер имеет критически важное значение для бизнеса, его потеря повредит конкурентоспособности компании

Классификация сервера	Приоритет
Контроллеры корневого домена	8
Контроллеры дочерних доменов	8
Корневой сервер DNS	4
Дочерние серверы DNS	5
Серверы WINS	3
Серверы DHCP	1
Серверы файлов и печати	8
Инtranet-портал компании	10
Порталы отделов	8
Web-сервер отдела кадров	7



Идентификация угроз



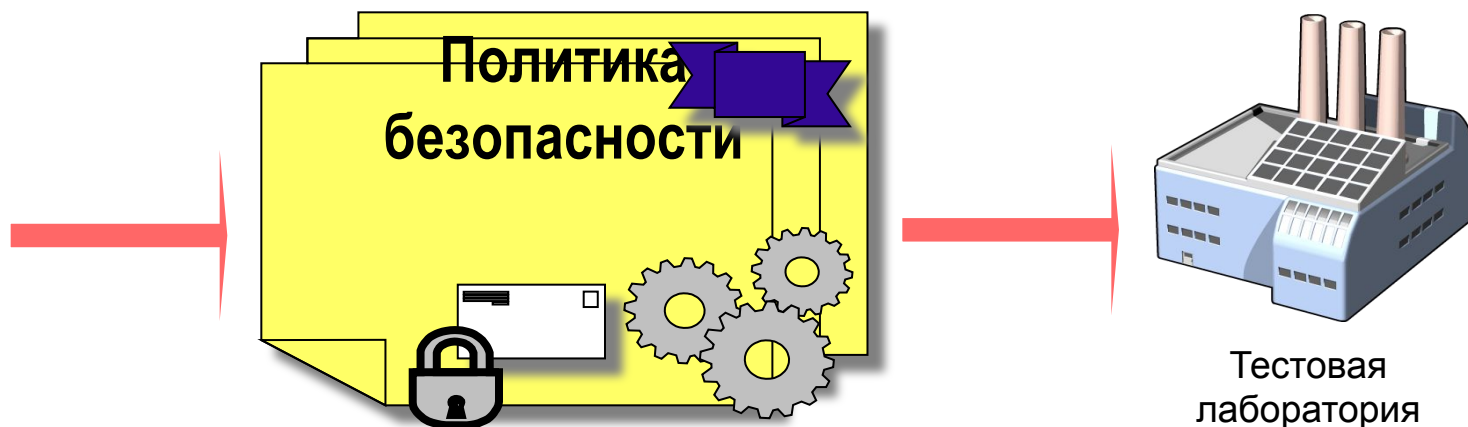
Тип угрозы	Примеры
Имитация (Spoofing)	<ul style="list-style-type: none">◆ Подделка электронных сообщений◆ Подделка ответных пакетов при аутентификации
Фальсификация (Tampering)	<ul style="list-style-type: none">◆ Модификация файлов◆ Модификация данных, передаваемых по сети
Отречение (Repudiation)	<ul style="list-style-type: none">◆ Удаление критичного файла или совершение покупки с последующим отказом признавать свои действия
Раскрытие информации (Information disclosure)	<ul style="list-style-type: none">◆ Несанкционированный доступ или незаконная публикация конфиденциальной информации
Отказ в обслуживании (Denial of service)	<ul style="list-style-type: none">◆ Заполнение сети пакетами «SYN»◆ Загрузка сетевого ресурса большим количеством поддельных пакетов ICMP
Повышение привилегий (Elevation of privilege)	<ul style="list-style-type: none">◆ Получение системных привилегий через атаку с переполнением буфера◆ Незаконное получение административных прав

Анализ рисков



- ◆ **Основные цели анализа рисков**
 - ▣ Идентификация угроз
 - ▣ Определение степени воздействия угрозы
 - ▣ Обеспечение баланса между степенью риска и стоимостью противодействия
- ◆ **Вычисление рейтингов угроз**
- ◆ **Установить рейтинг (от 1 до 10) для каждой из пяти областей и взять среднее значение**
 - ▣ Ущерб (Damage)
 - ▣ Воспроизводимость (Reproducibility)
 - ▣ Используемость (Exploitability)
 - ▣ Затрагиваемые пользователи (Affected Users)
 - ▣ Открытость (Discoverability)
- ◆ **Степень риска = Приоритет объекта * Рейтинг угрозы**

Разработка и внедрение политики безопасности



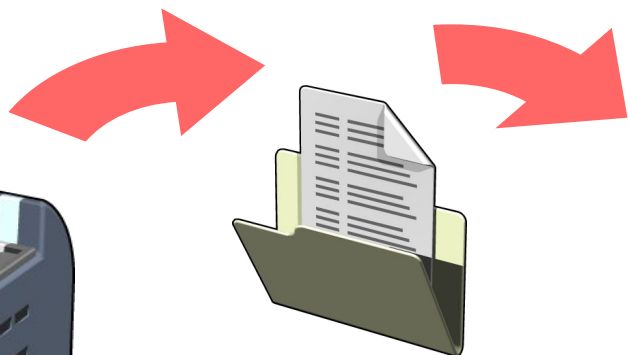
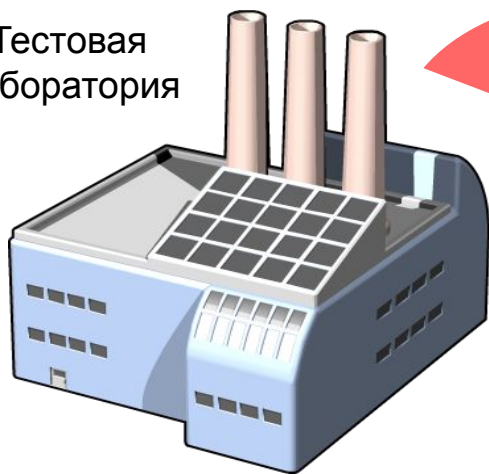
- ◆ Управление конфигурациями
- ◆ Управление обновлениями
- ◆ Мониторинг систем
- ◆ Аудит систем
- ◆ Операционные политики
- ◆ Операционные процедуры



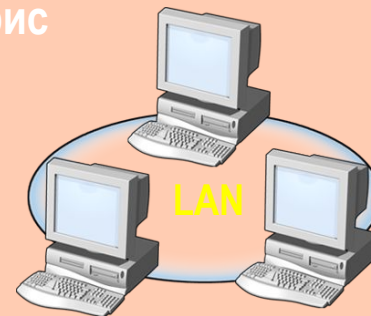
Сохранение знаний и обучение



Тестовая
лаборатория

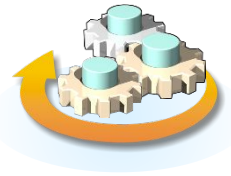


Главный офис



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

Повторная оценка и изменения



- ◆ При изменении или при появлении новых объектов необходимо проводить повторную оценку и анализ
 - Модификация политики безопасности

Общая картина операций по управлению рисками



Глубокая оборона

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

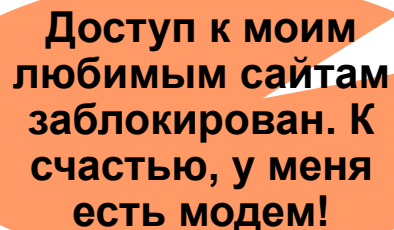
Пользователи часто забывают о безопасности



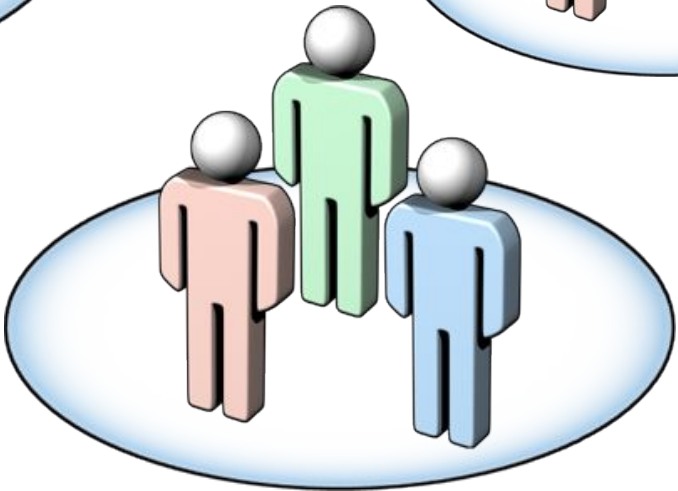
Мне нужно настроить брандмауэр. Какие порты мне заблокировать?



Я зафиксирую дверь в серверную открытой. Так удобнее!




Доступ к моим любимым сайтам заблокирован. К счастью, у меня есть модем!



В качестве пароля я возьму свое имя.

Социальный инжиниринг

The illustration depicts several groups of stylized human figures in a networked environment. Each group is contained within a light blue oval. The figures are colored in shades of green, pink, and blue. Some figures have a pink starburst effect behind them, indicating they are the target of an attack. The text bubbles are yellow and contain questions related to social engineering.

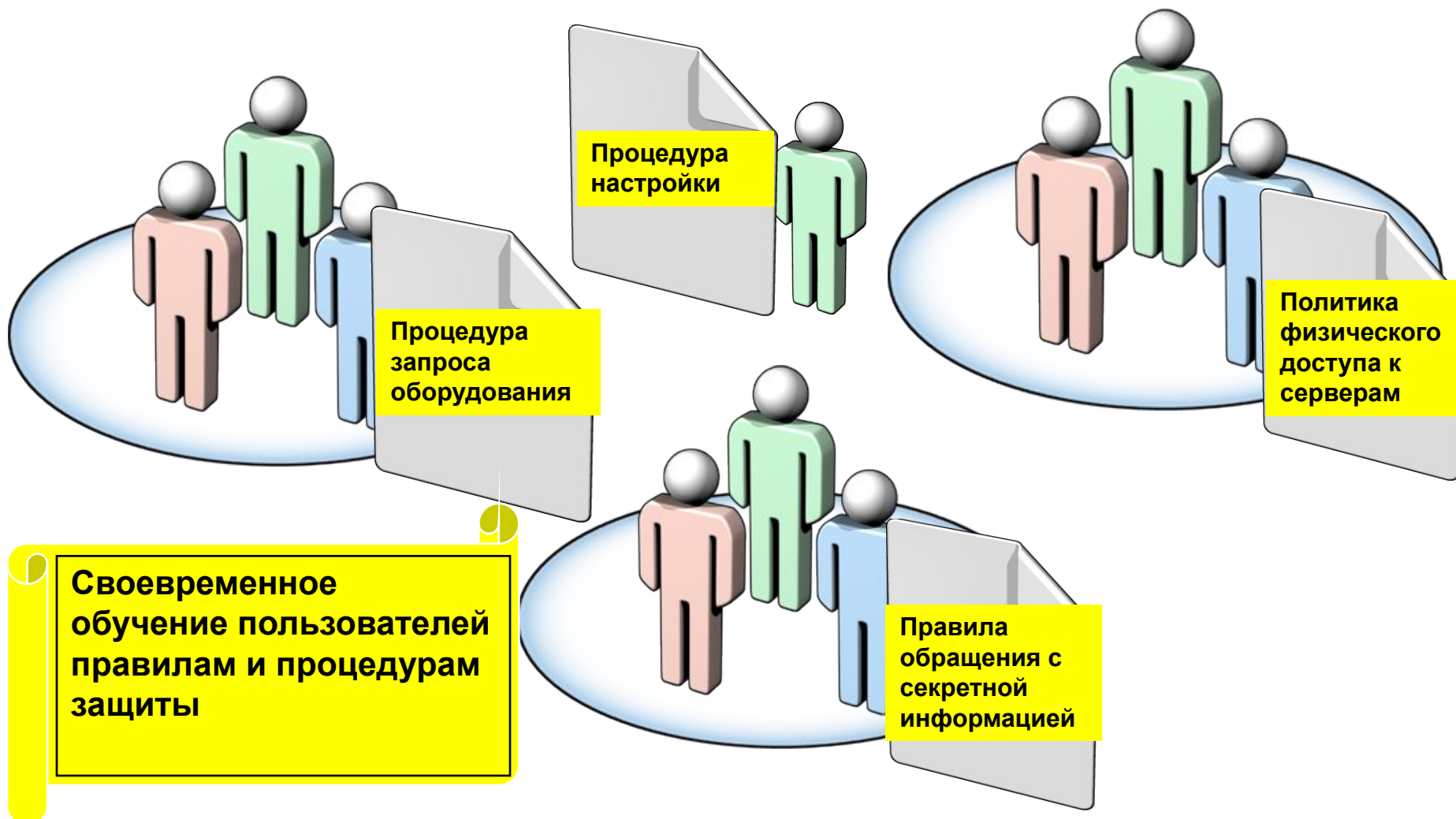
А у нас тоже есть сеть! Как вы настраиваете свои брандмауэры?

Отличный модем! А какой номер у вашей линии?

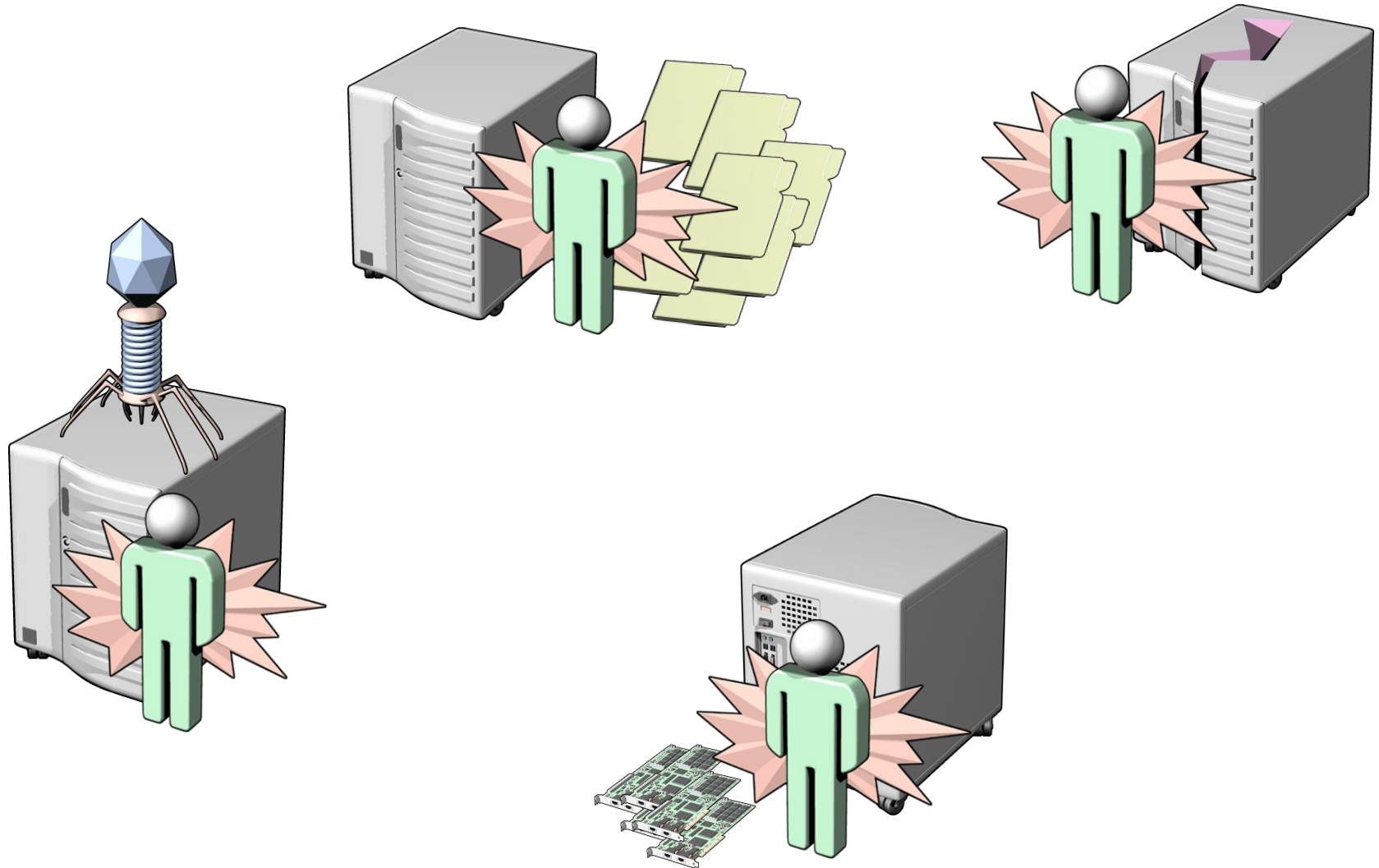
Я никак не могу придумать хороший пароль. А вы какой используете?

Вы не знаете, как пройти в серверную комнату?

Политики, процедуры и обучение



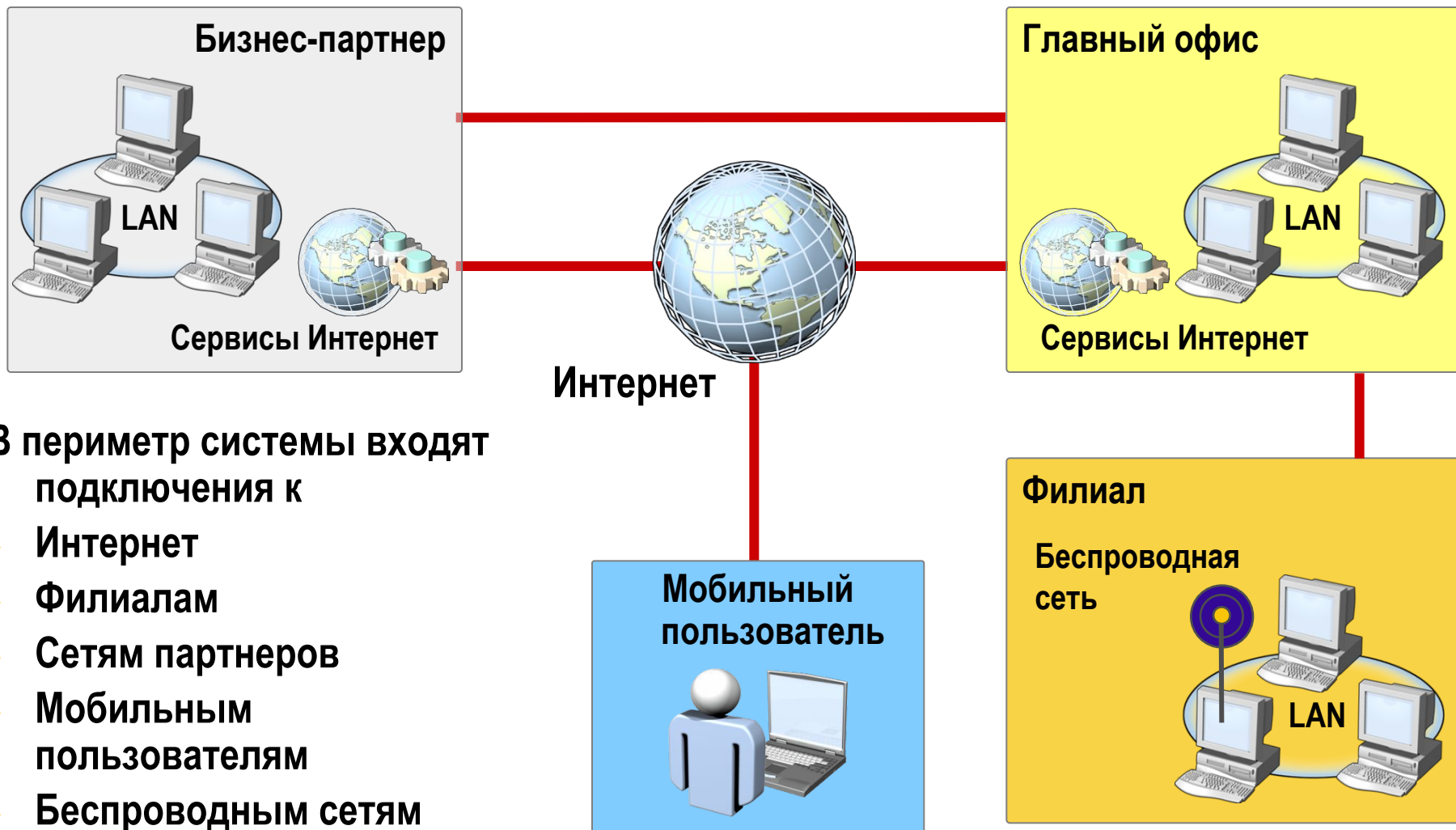
Воздействия при физическом доступе



Физическая защита

- ✓ **Блокировка дверей, средства слежения и сигнализации**
- ✓ **Выделенный персонал для охраны**
- ✓ **Жесткая регламентация процедур доступа в серверные помещения**
- ✓ **Системы видео-наблюдения**
- ✓ **Удаление лишних устройств ввода данных**
- ✓ **Средства удаленного администрирования**

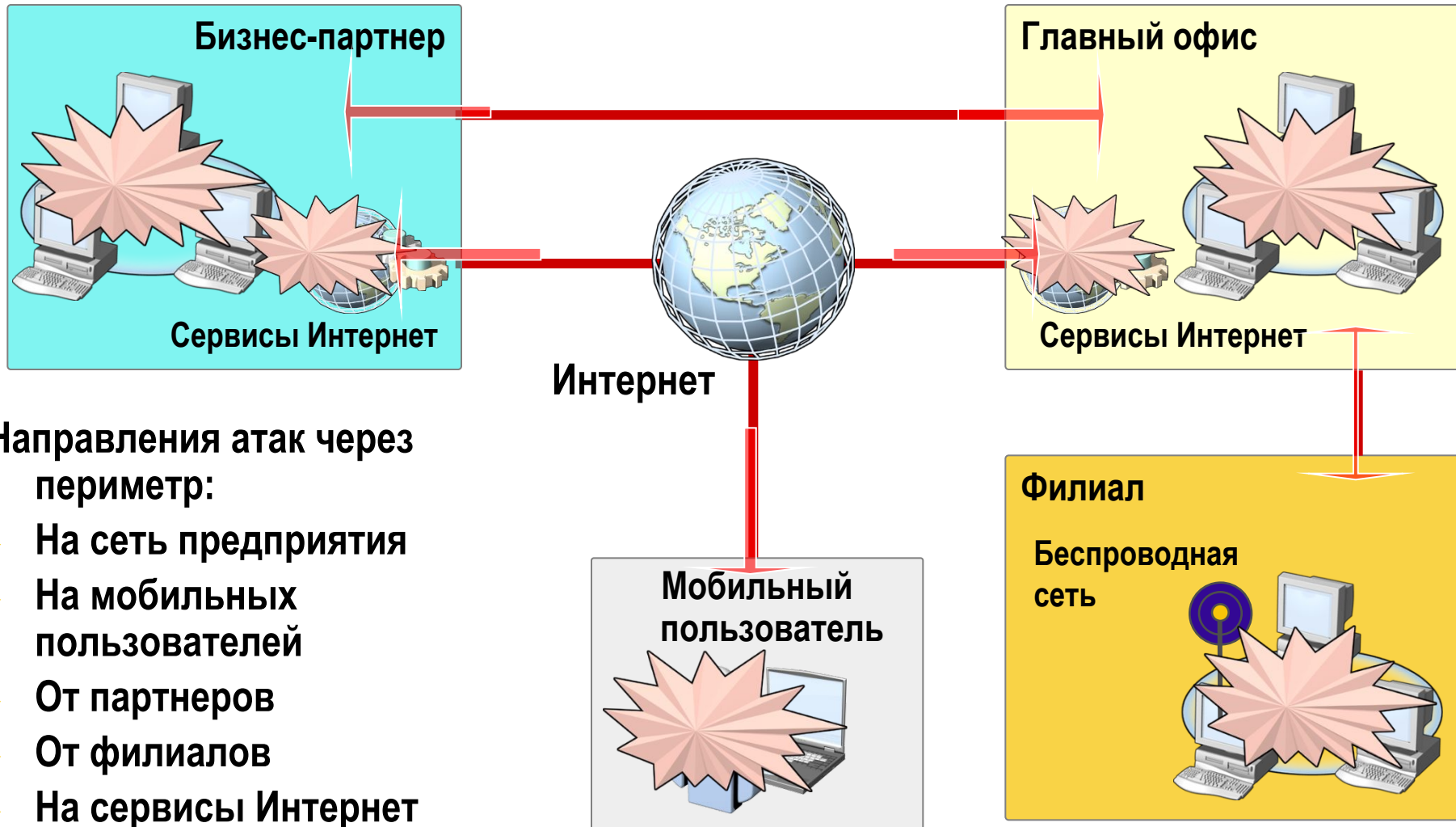
Периметр информационной системы



В периметр системы входят подключения к

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

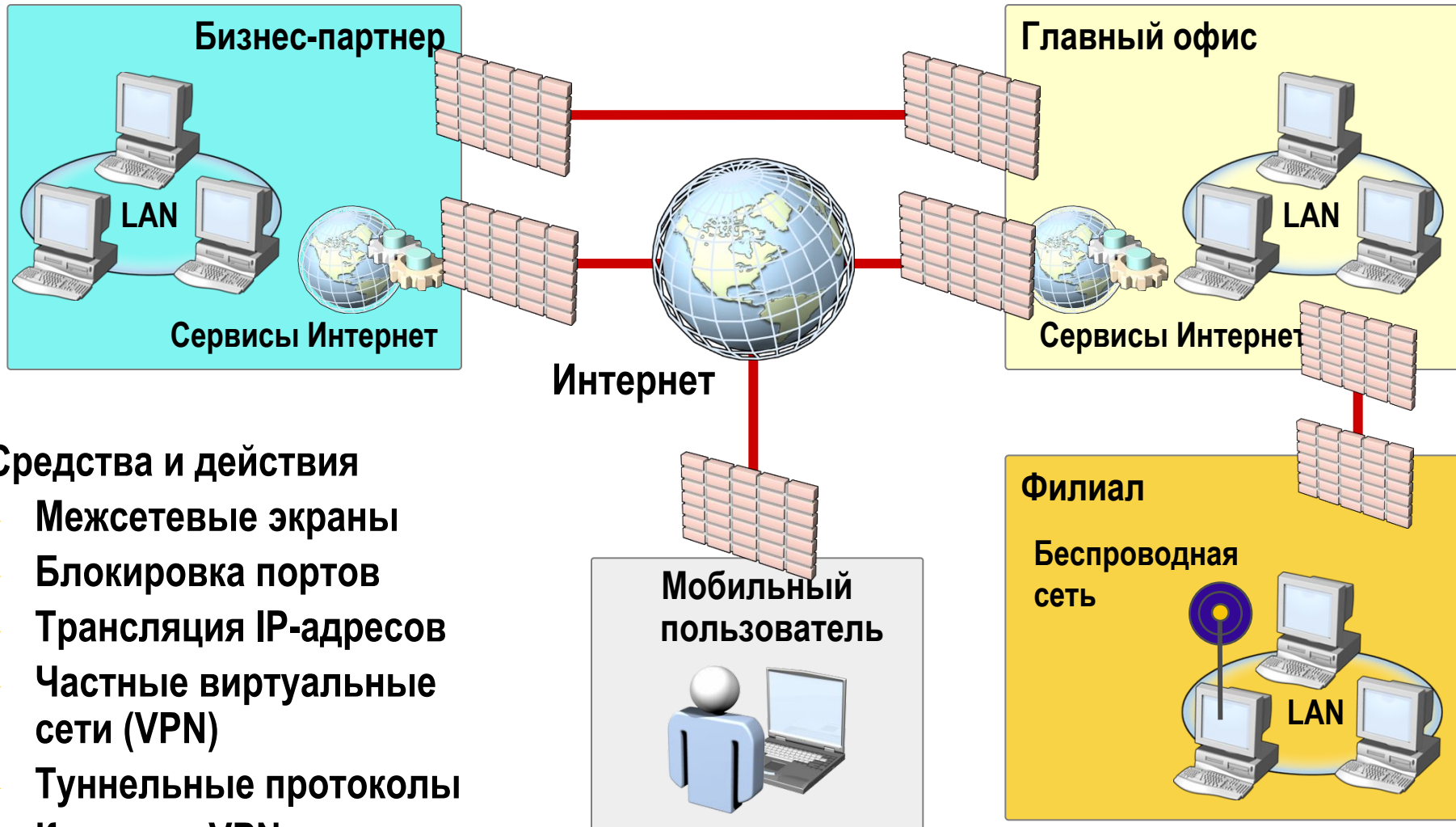
Компрометация периметра



Направления атак через периметр:

- ◆ На сеть предприятия
- ◆ На мобильных пользователей
- ◆ От партнеров
- ◆ От филиалов
- ◆ На сервисы Интернет
- ◆ Из Интернет

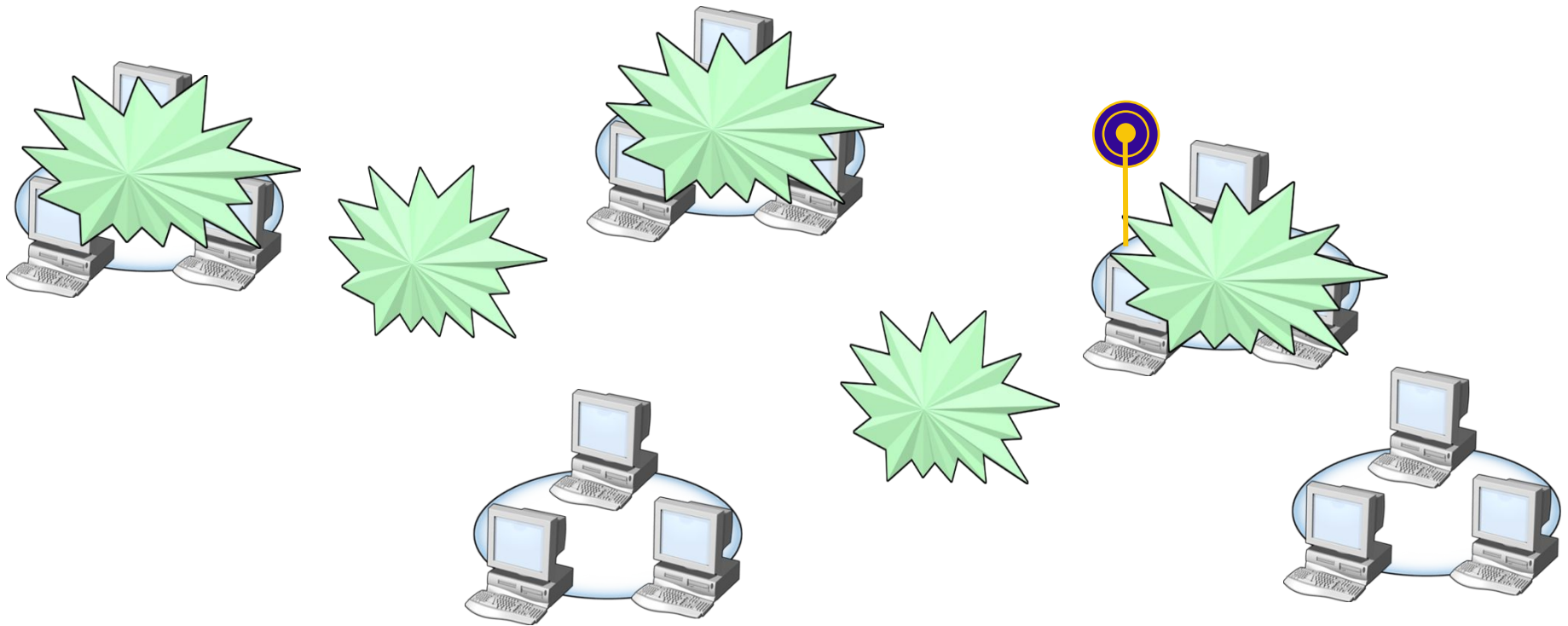
Защита периметра



Средства и действия

- ◆ Межсетевые экраны
- ◆ Блокировка портов
- ◆ Трансляция IP-адресов
- ◆ Частные виртуальные сети (VPN)
- ◆ Туннельные протоколы
- ◆ Карантин VPN

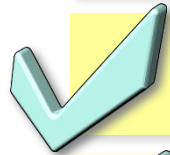
Угрозы локальной сети



Защита локальной сети



Взаимная аутентификация пользователей и сетевых ресурсов



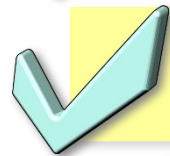
Сегментация локальной сети



Шифрование сетевого трафика



Блокировка неиспользуемых портов

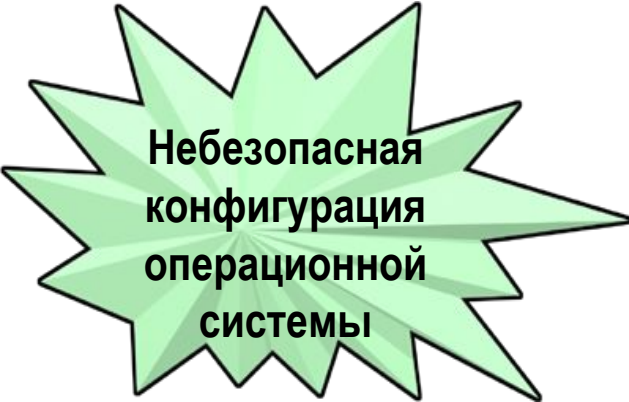


Контроль доступа к сетевым устройствам




Цифровая подпись сетевых пакетов


Компрометация компьютера



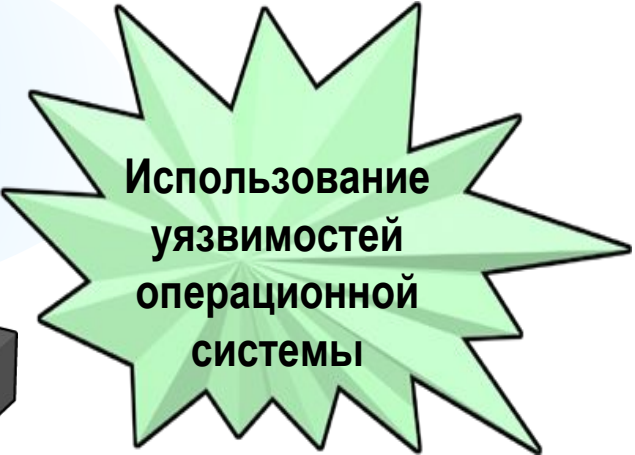
Небезопасная
конфигурация
операционной
системы



Неконтролируемый
доступ



Распространение
вирусов



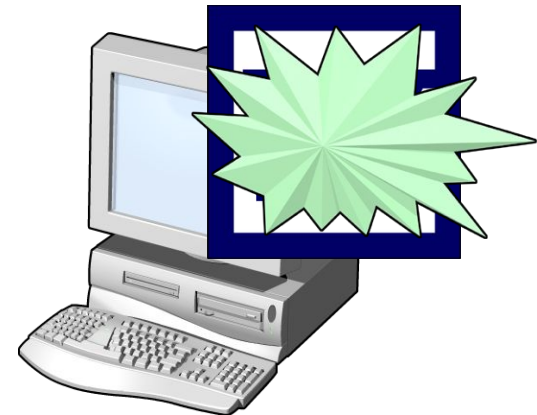
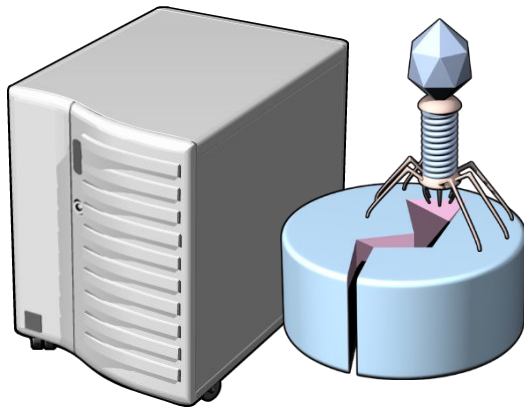
Использование
уязвимостей
операционной
системы

Защита компьютеров

- ✓ **Взаимная аутентификация пользователей, серверов и рабочих станций**
- ✓ **Защита операционной системы**
- ✓ **Установка обновлений безопасности**
- ✓ **Аудит успешных и неуспешных событий**
- ✓ **Отключение неиспользуемых сервисов**
- ✓ **Установка и обновление антивирусных систем**

Компрометация приложений

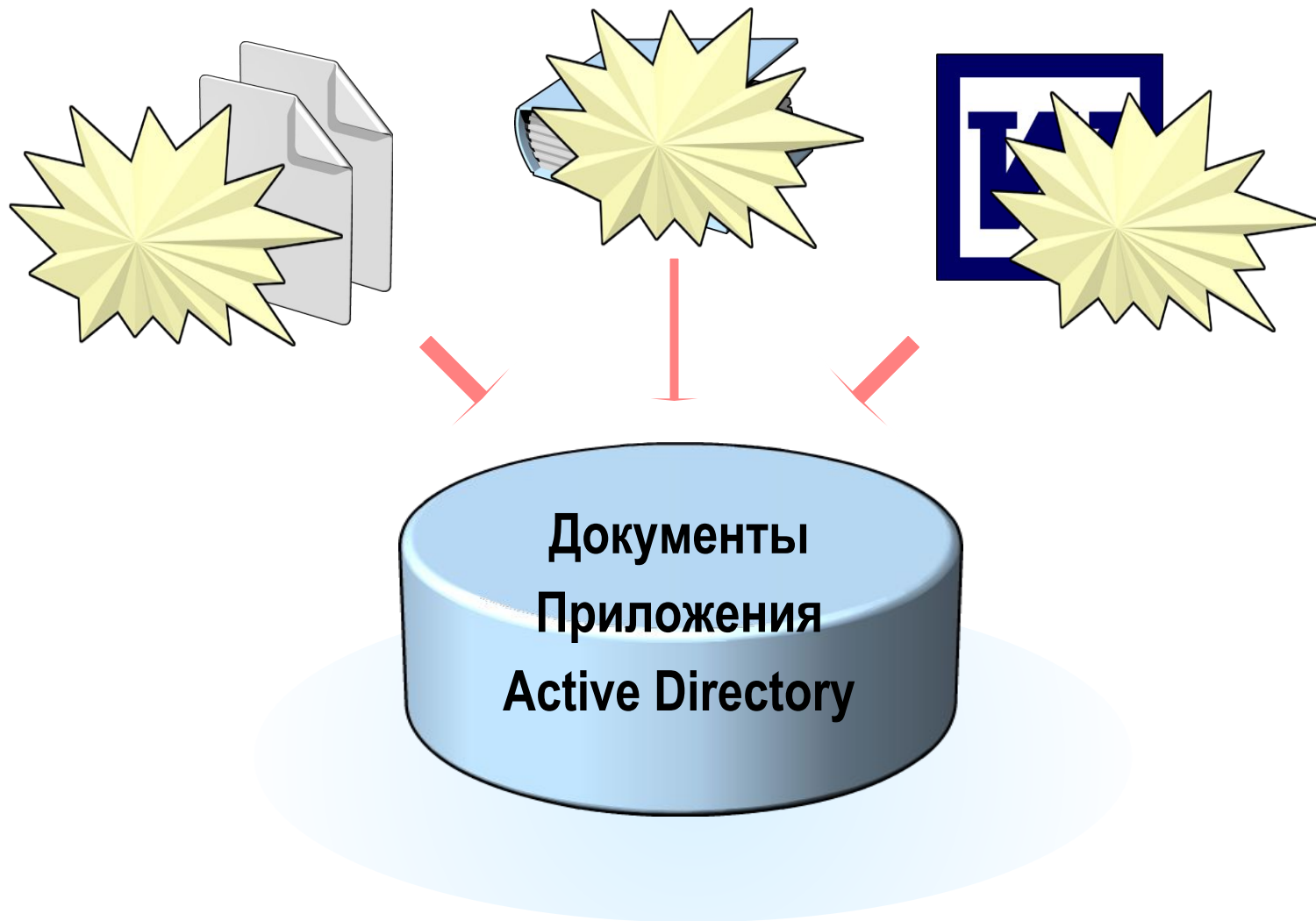
- ◆ Потеря приложения
- ◆ Исполнение вредного кода
- ◆ Экстремальная загрузка приложения (DoS)
- ◆ Несанкционированные и некорректные операции



Защита приложений

- ✓ Включать только необходимые службы и функции приложений
- ✓ Настройка параметров защиты приложений
- ✓ Установка обновлений безопасности
- ✓ Запуск приложений в контексте с минимальными привилегиями
- ✓ Установка и обновление антивирусных систем

Компрометация данных



Защита данных



Защита файлов средствами Шифрующей файловой системы (EFS)



Настройка ограничений в Списках контроля доступа



Система резервного копирования и восстановления



Защита на уровне документов с помощью Windows Right Management Services

Необходимые действия при защите от атак

Атака червя на порт

- ◆ **Периметр**
 - ▣ Межсетевой экран должен блокировать порт
- ◆ **Внутренняя сеть**
 - ▣ Просканировать сеть и обнаружить уязвимые компьютеры
 - ▣ Проверить машины, подключаемые через Службу удаленного доступа, на наличие обновлений
- ◆ **Компьютер**
 - ▣ Установить соответствующие обновления
 - ▣ Разрешить входящий трафик для порта
 - ▣ Фильтры IP Security
 - ▣ Заблокировать ненужный входящий трафик
 - ▣ Internet Connection Firewall

Почтовые черви

- ◆ **Периметр**
 - ▣ Сканирование всех вложений на шлюзе
- ◆ **Внутренняя сеть**
 - ▣ Проверить хосты, подключаемые через Службу удаленного доступа, на наличие актуальных обновлений и сигнатур вирусов
- ◆ **Приложения**
 - ▣ Установить обновления безопасности
- ◆ **Пользователи**
 - ▣ Правила обращения с файлами в почтовых вложениях
 - ▣ «Не открывайте файлы, если вы не уверены, что это безопасно»

Стандартный процесс обработки инцидента

Обнаружение атаки



Идентификация атаки



Оповещение



Защитные действия

Превентивные меры



Документирование



✓ Выключить и отсоединить пораженные компьютеры от сети

✓ Заблокировать входящий и исходящий сетевой трафик

✓ Исследовать пораженные компьютеры

✓ Зафиксировать улики вторжения

Законы информационной безопасности

- 1. Если “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.**