Информзащита
Учебный центр

Классификация систем обнаружения атак

Лепихин Владимир
Учебный центр «Информзащита»

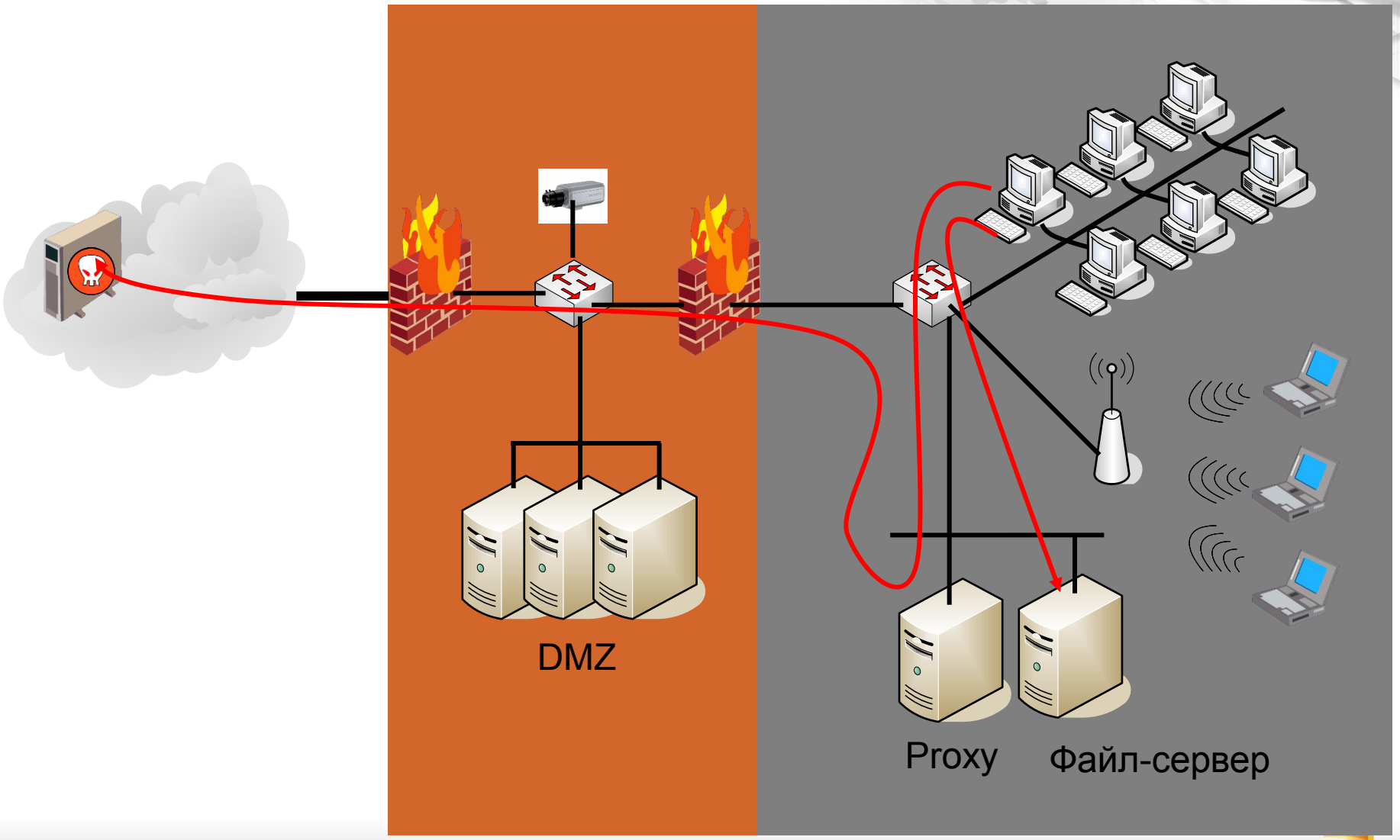
Обнаружение атак

- Обнаружение вторжений (**атак**) – это процесс мониторинга **событий**, происходящих в компьютерной системе или сети с целью поиска признаков возможных **инцидентов**

Примеры событий

- неудачная попытка входа в систему
- попытка подключения к внешнему адресу с узла DMZ
- выгрузка файла в облачное хранилище с узла пользователя

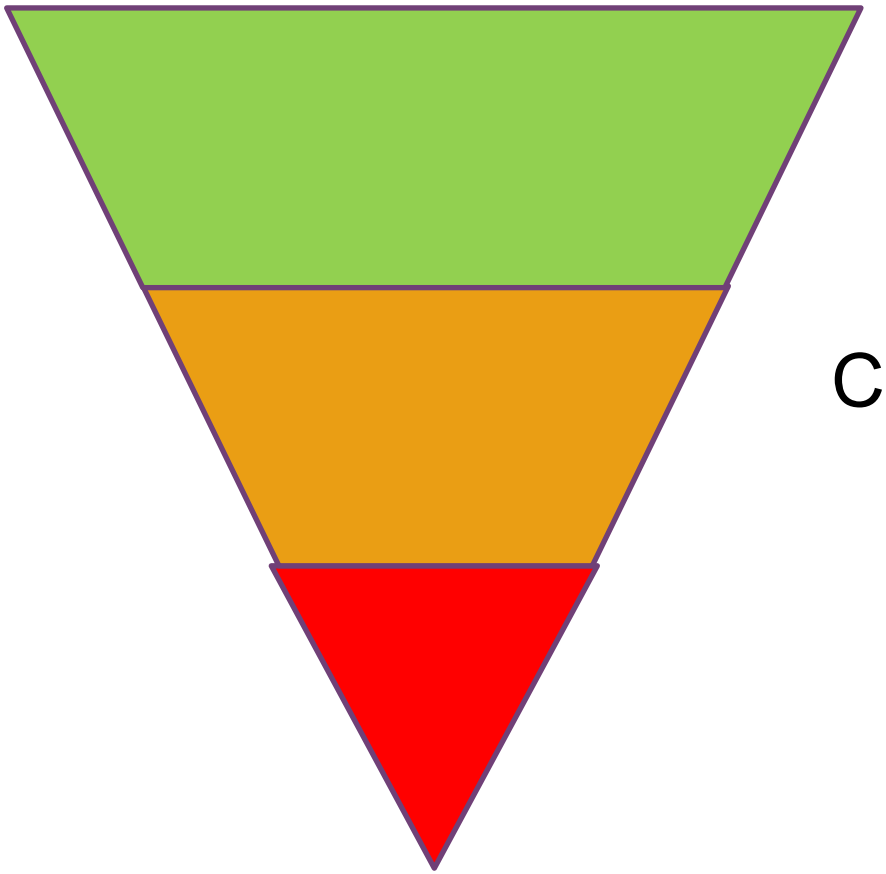
Пример инцидента



Ещё примеры

- выявление на одном из критичных узлов внутренней сети вредоносного программного обеспечения
- несанкционированный доступ к узлу DMZ со стороны внешнего нарушителя
- злоупотребления со стороны внутреннего авторизованного пользователя

Событие - > Атака -> Инцидент



События

События, влияющие на ИБ (атаки)

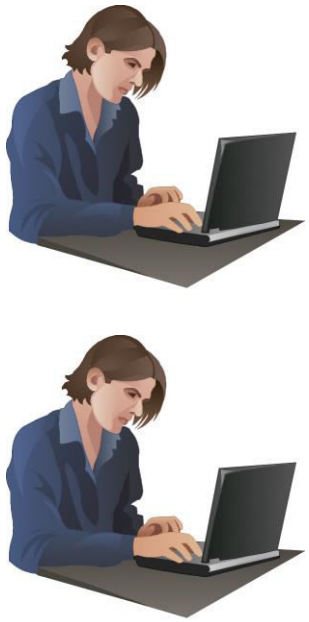
Инциденты

Система обнаружения атак

- Система обнаружения атак – это программное (или программно-аппаратное) обеспечение, автоматизирующее процесс обнаружения атак

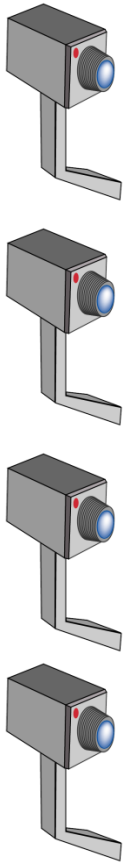
Инфраструктура обнаружения атак

Компоненты управления (клиентская часть)



Компоненты управления (серверная часть)

Модули слежения (сенсоры)



Информзащита
Учебный центр

Обнаружение атак: архитектура сенсора

Алгоритм (технология) обнаружения

Что и как обнаруживать?

Источники данных

Где обнаруживать?

Механизмы реагирования

Модуль слежения (сенсор, датчик…)

Источники данных

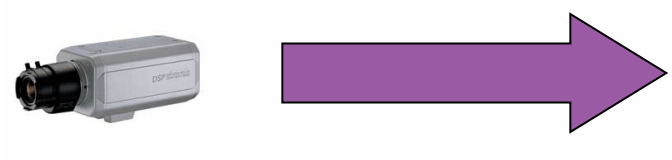
- Сетевой трафик
- Журналы событий
- Действия субъектов системы

Алгоритм (технология) обнаружения

⇩ На основе понимания ожидаемого поведения контролируемого объекта

⇩ На основе знания всех возможных атак и их модификаций

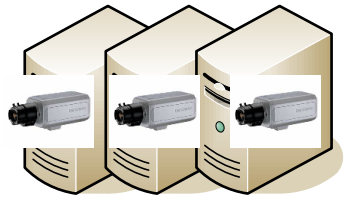
Механизмы реагирования

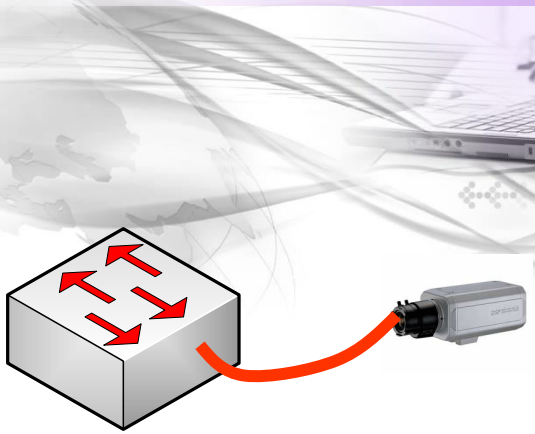


Оповещение ⇨
Блокировка ⇨
Запись данных ⇨

● ● ●

Host IDS / Network IDS





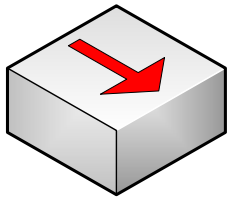
- Сетевой трафик данного узла
- Журналы ОС и приложений
- Действия субъектов системы

- Сетевой трафик
  - с концентратора
  - со SPAN-порта
  - с разветвителя
  - по протоколу Network Flow
  - из файла

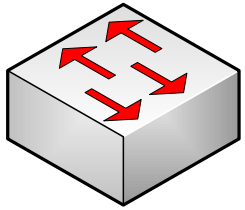
Источники данных / способ размещения

Информзащита
Учебный центр

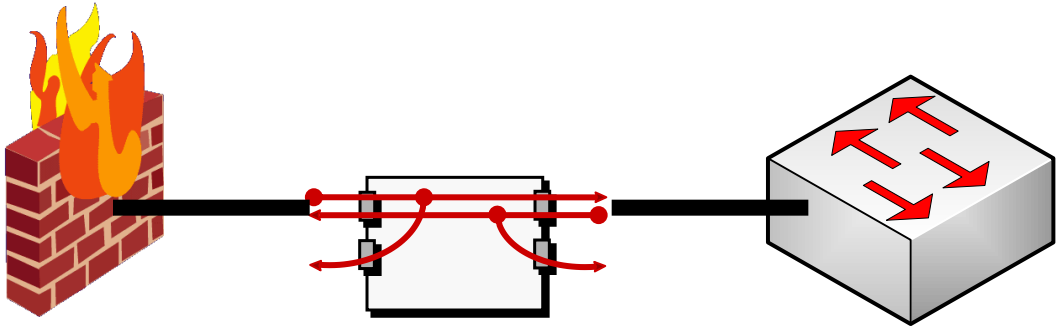
Network IDS – варианты подключения



Концентратор (Hub)

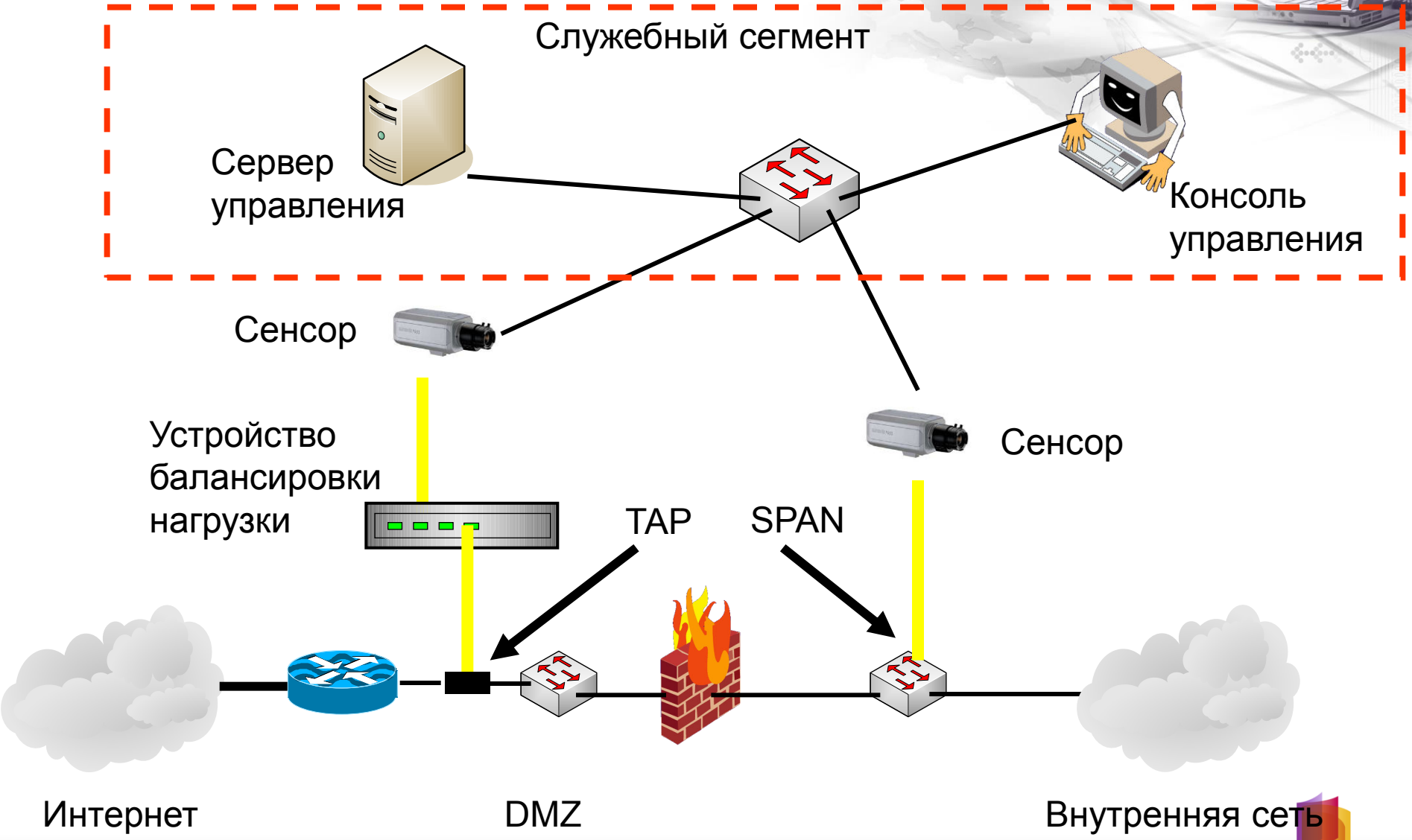


SPAN-порт коммутатора



Разветвитель (TAP)

NIDS : типовая схема размещения

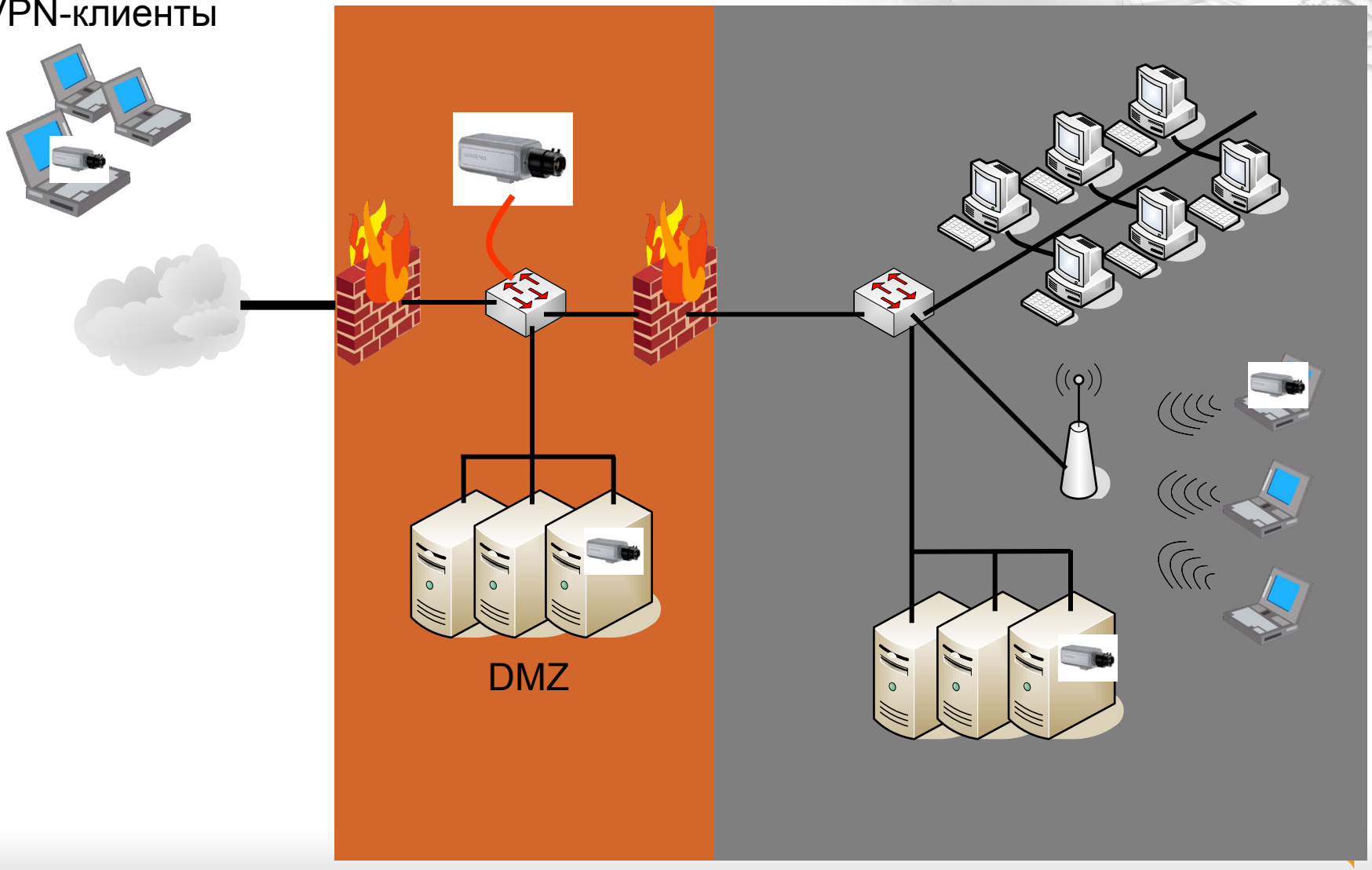


NIDS: почему её может быть недостаточно?

- Шифрование трафика
- Высокоскоростные участки
- Иные источники данных (не сетевой трафик)
- Специфика расположения объекта

Host IDS (HIDS)

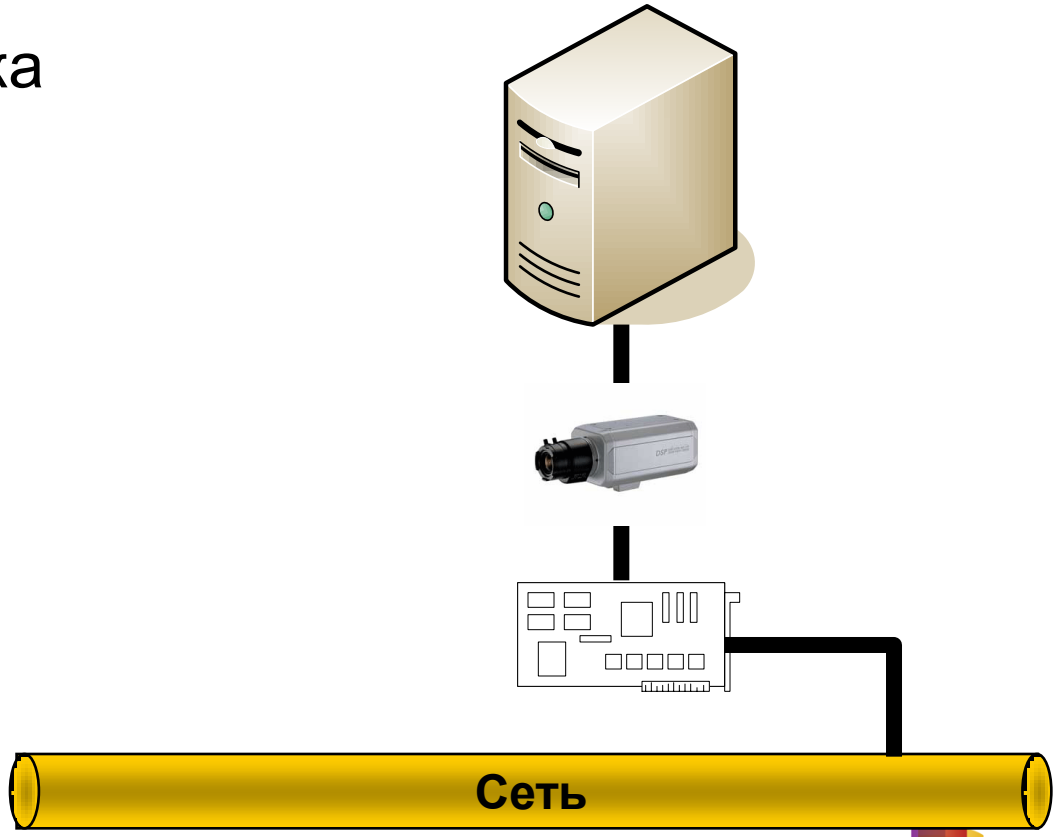
VPN-клиенты



Host IDS: мониторинг трафика

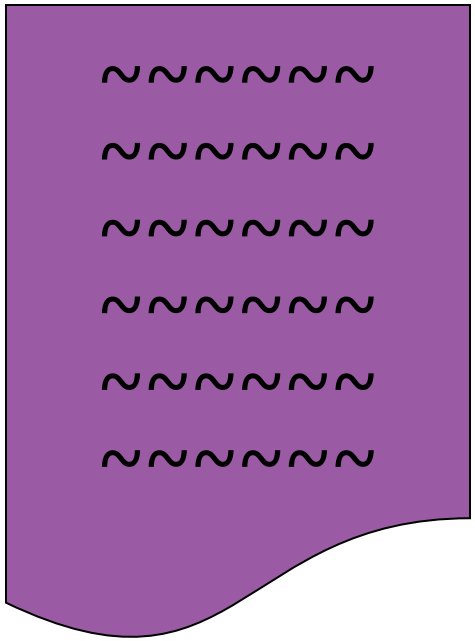
Анализ трафика на наличие признаков атак (аналогично NIDS)

Фильтрация трафика



Журнал событий

Журнал событий (лог, log) – это объект (например, файл), содержащий перечень событий, произошедших с различными активами организации (с системами или сетями).



Обычно журнал событий – это совокупность записей (entries), каждая из которых содержит информацию, относящуюся к отдельному событию с системой или сетью.

Категории журналов событий

(содержащие события безопасности)

- Журналы средств защиты
- Журналы операционных систем, приложений и СУБД

Журналы средств защиты

- Межсетевые экраны
- Средства противодействия вредоносному коду
- Системы обнаружения и предотвращения атак
- Системы управления уязвимостями
- Серверы аутентификации
- Серверы контроля доступа к сети

Журналы операционных систем

- Системные журналы
- Журналы аудита

Журналы приложений

- Почтовый сервер
- Web-сервер
- Файловый сервер
- …

Host IDS: контроль действий субъектов системы

Анализ кода

- обнаружение и предотвращение переполнения буфера
- Анализ «поведения»

Мониторинг файловой системы

- Контроль целостности
- Контроль попыток обращения к критичным объектам, включая контроль запускаемых приложений
- Антивирусный контроль

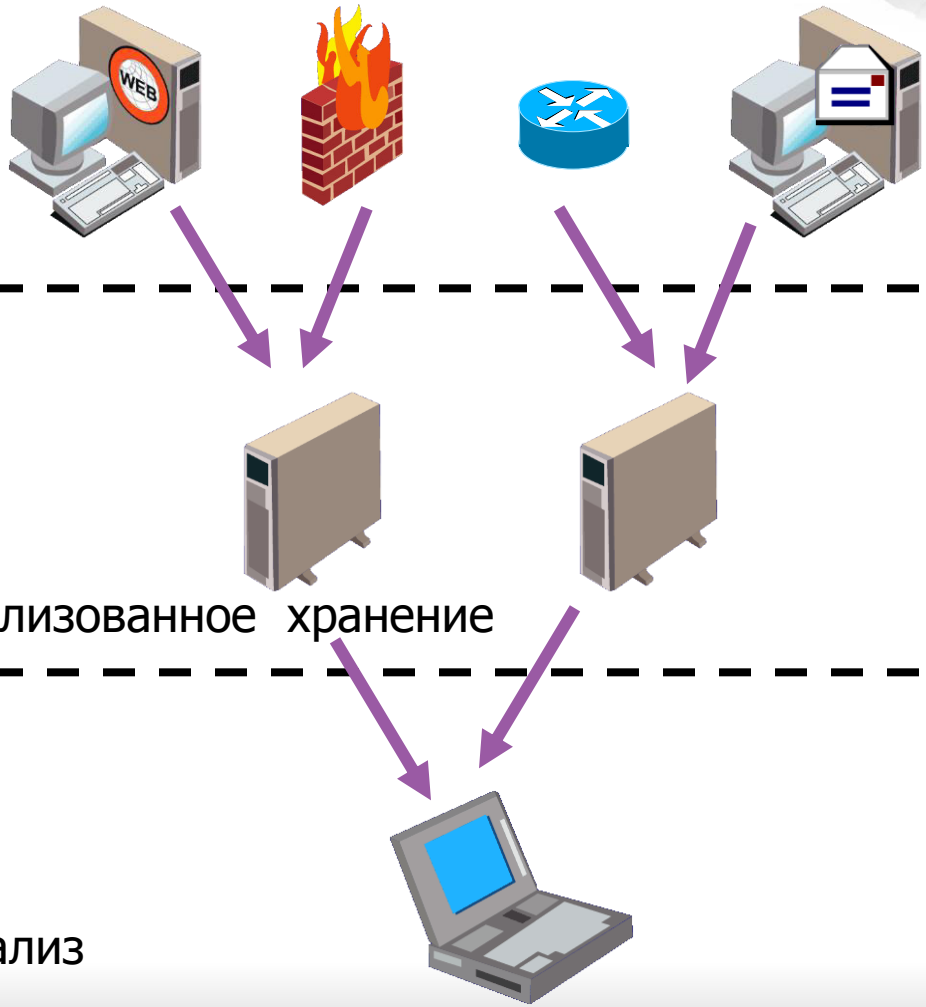
Host IDS/IPS: примеры

Endpoint security

СЗИ от НСД

…

Инфраструктура управления журналами событий



Информзащита
Учебный центр

Как обнаруживать?

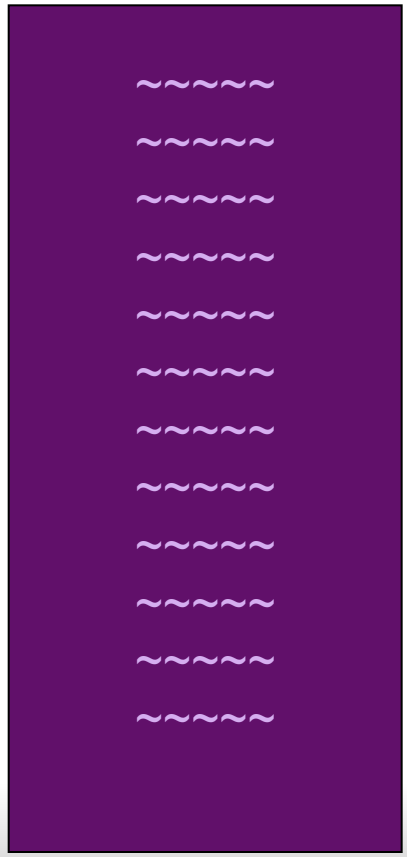
- На основе знания всех возможных атак и их модификаций
- На основе понимания ожидаемого поведения контролируемого объекта

Обнаружение «злоупотреблений»

(Misuse detection, signature-based detection)

Источники данных
(журналы, сетевой трафик)

Перечень сигнатур



Сигнатура

Сигнатура (signature) – это совокупность параметров, «отпечаток» (pattern), соответствующий известной атаке

Обнаружение «злоупотреблений» - это процесс сопоставления сигнатур и прошедших предварительную обработку данных (полученных из соответствующих источников) с целью идентификации возможных инцидентов

Примеры:

1. Попытка получения по протоколу ftp файла /etc/passwd
2. Появление в журнале аудита события с идентификатором 645
3. Попытка подключения к закрытому в данный момент TCP-порту

Простейший случай – Network IDS

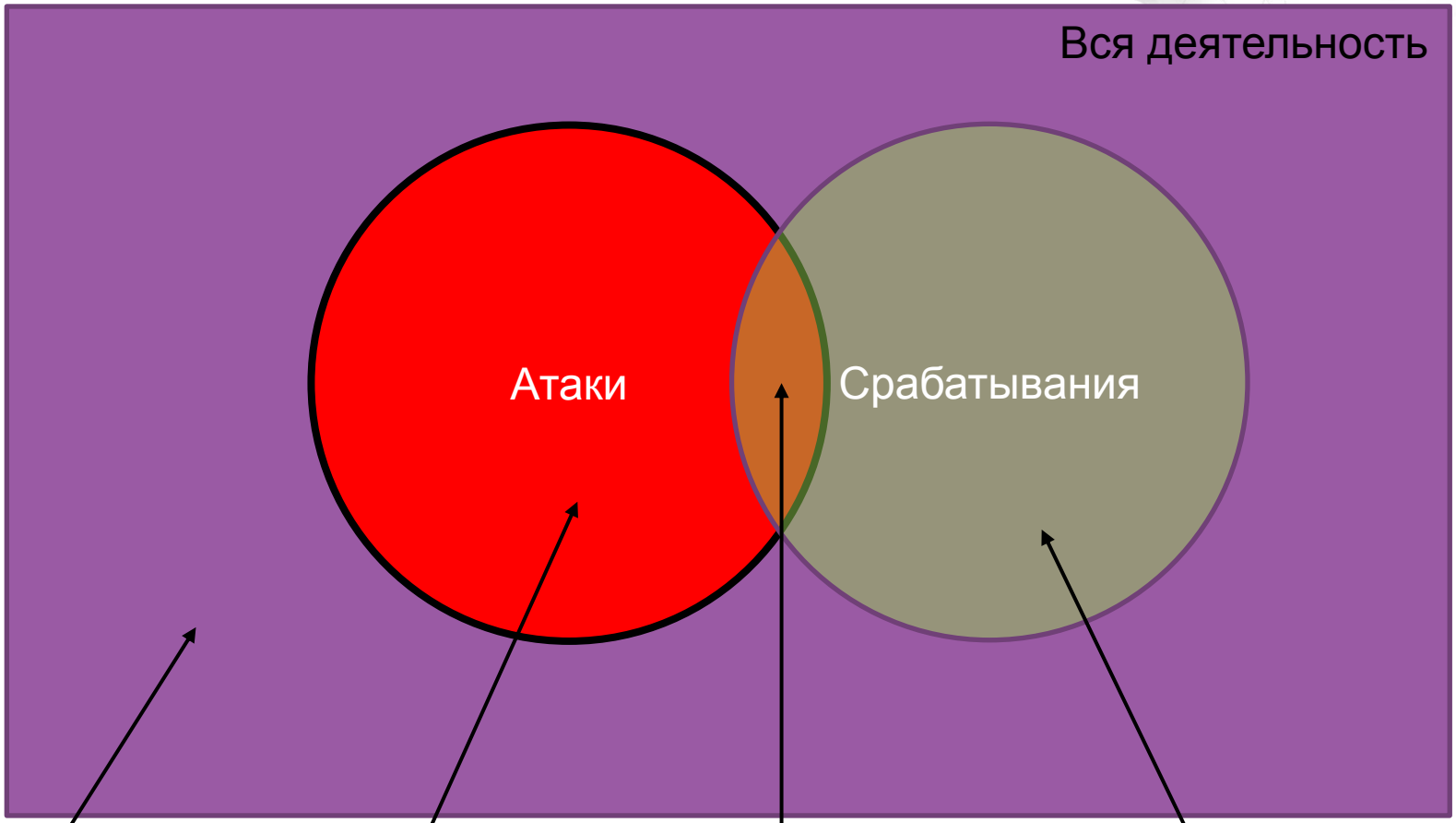
Типы сигнатур:

- Синтаксический разбор отдельных пакетов
- Анализ протоколов и другие усовершенствования
- Анализ протоколов с учётом состояния
- «Расширенный» анализ протоколов

Показатели качества модуля слежения

По результатам мониторинга	В действительности	
	Факт атаки имел место	**Факта атаки не было**
Атака обнаружена	True Positive	False Positive
Атака не обнаружена	False Negative	True Negative

Показатели качества модуля слежения



Информзащита
Учебный центр

Ложные срабатывания

False Positive

Оповещения о событиях, которых в действительно не происходило

Причины:
1. Неудачный выбор признака атаки
2. Ошибка реализации сигнатуры

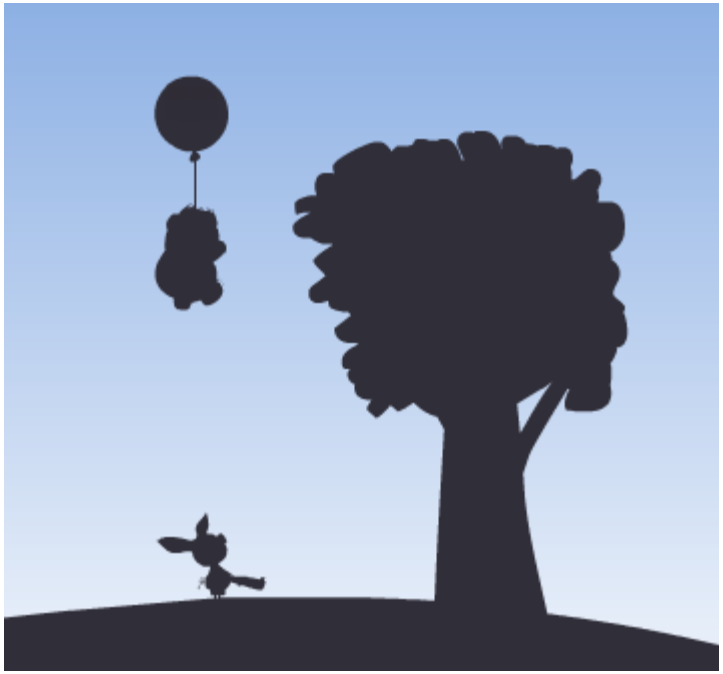
Ложные оповещения

Оповещения о событиях, которые не являются значимыми в данном конкретном случае

Причины:
1. Некорректная настройка системы
2. Особенность признака атаки

Точность обнаружения

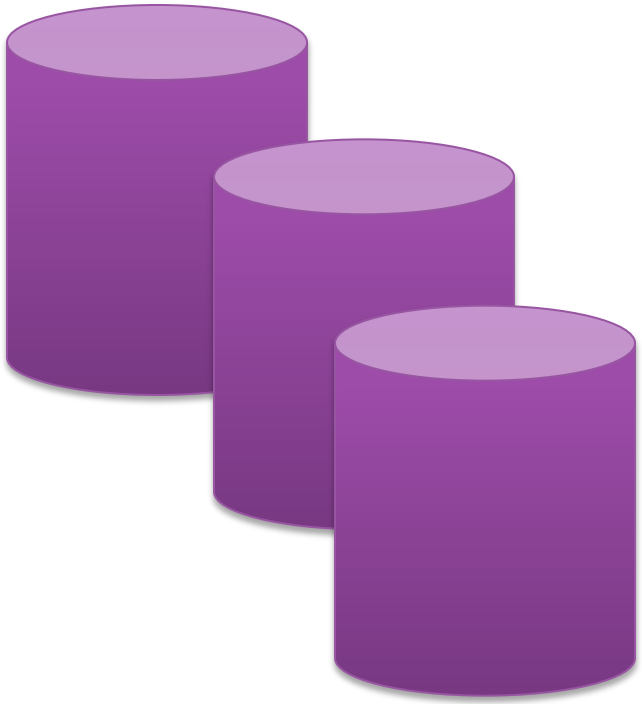
Precision= True Positive/(True Positive + False Positive)



…
— Разве я не попал? — спросил Пятачок.
— Не то чтобы совсем не попал,— сказал Пух,— но только не попал в шарик!
…

Sensitivity («чувствительность»)

Sensitivity=True Positive/(True Positive + False Negative)



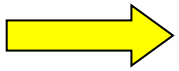
Суммарная точность работы (accuracy)

$$A=(TP+TN)/(TP+TN+FP+FN)$$

Обнаружение аномалий

(Anomaly detection model)

Источники данных
(журналы, сетевой трафик, включая NetFlow,
деятельность субъектов системы)

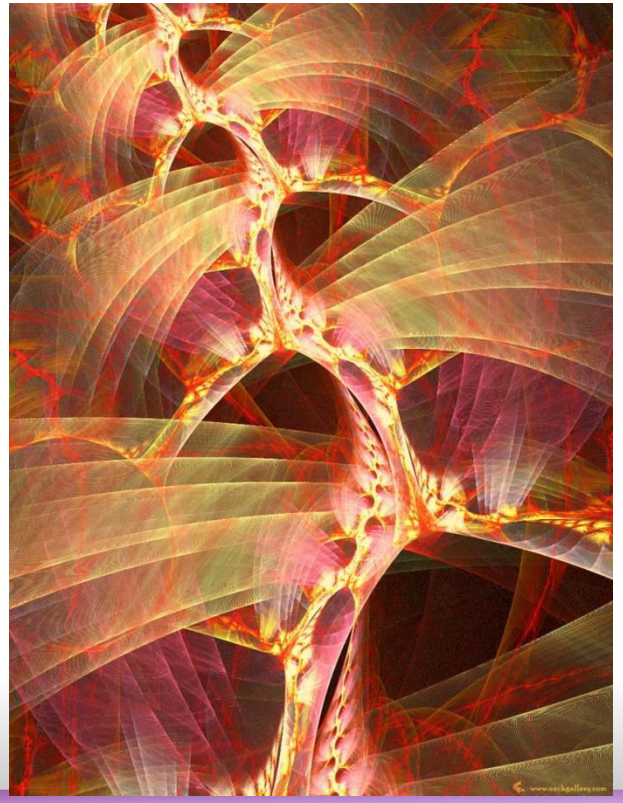


Профиль поведения

Информзащита
Учебный центр

Обнаружение аномалий

Обнаружение аномалий (Anomaly-based detection) – это процесс сопоставления прошедших предварительную обработку данных (полученных из соответствующих источников) и набора профилей поведения (соглашений о том, какая активность считается нормальной) с целью обнаружения подозрительных ситуаций



Информзащита
Учебный центр

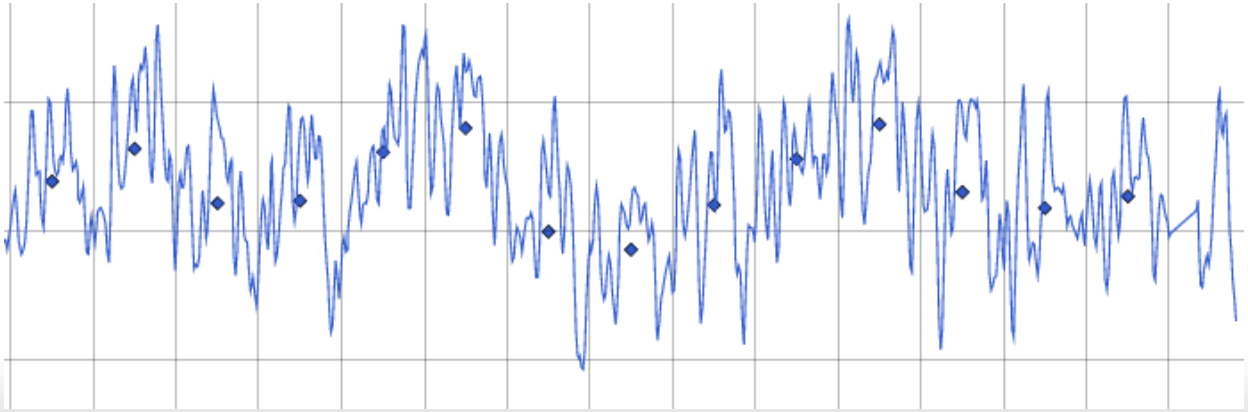
Профиль поведения

Профиль поведения определяет нормальное поведение пользователей, узлов сети, приложений и других субъектов

Профиль поведения создаётся на основе мониторинга характеристик в течение определённого периода времени

Характеристики могут быть самыми разнообразными:

- Загрузка отдельного участка сети в разное время суток
- Количество писем, отправленных пользователем в течение дня
- Модель параметра, передаваемого приложению

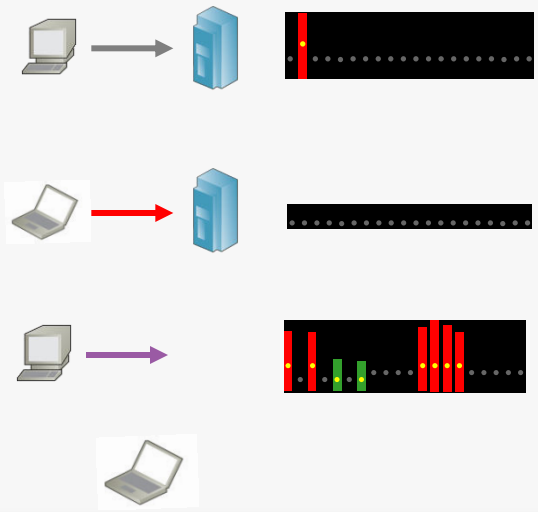


Информзащита
Учебный центр

Данные для построения профиля поведения

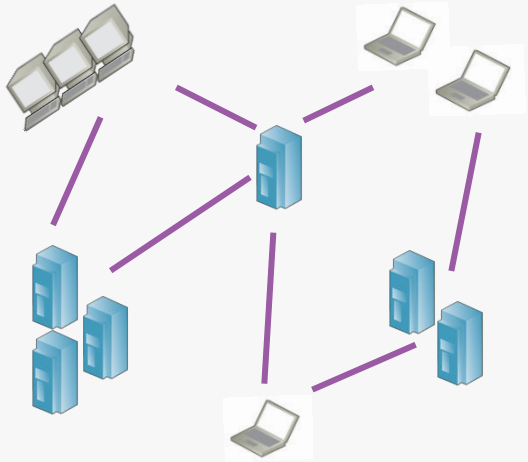
Объёмы трафика

Для каждого клиента, сервера, протокола, дня недели, времени суток измеряются минимальные, максимальные и средние значения параметров PPS (пакетов в секунду) и BPS (байт в секунду).



Отношения

«Запоминаются» отношения между узлами и группами узлов (типы взаимодействия, протоколы и т. п.)

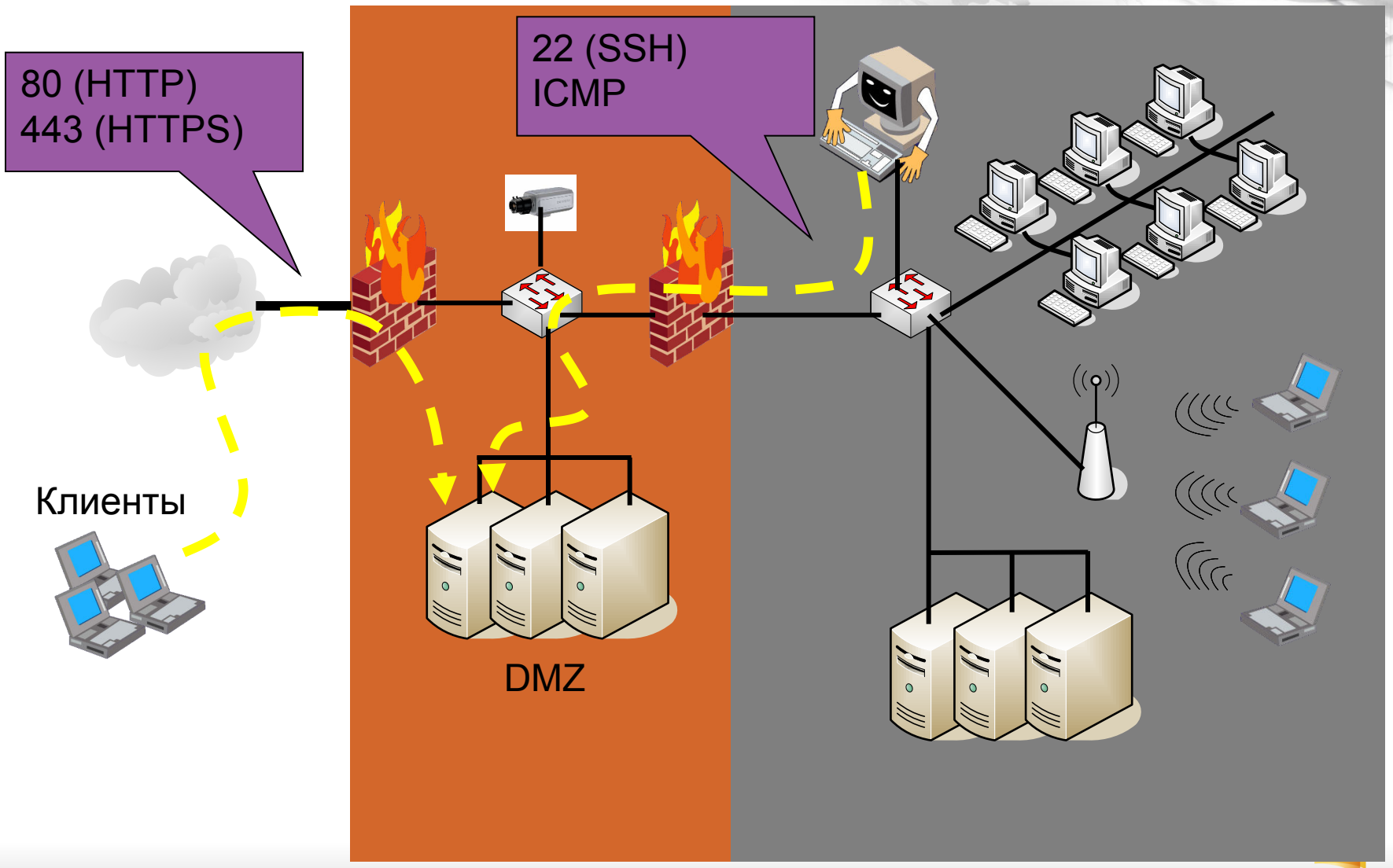


Архив потоков данных

Сохраняются низкоуровневые данные о потоках для целей расследования инцидентов

10.0.0.1	10.1.0.3	TCP 80	330 pkts
10.0.0.5	10.1.0.3	TCP 80	330 pkts
10.0.0.1	10.1.0.6	TCP 25	330 pkts
10.0.0.1	10.1.0.3	TCP 80	330 pkts
10.0.0.7	10.1.0.5	TCP 80	330 pkts
10.0.0.1	10.1.0.3	TCP 110	330 pkts
10.0.0.5	10.1.0.6	TCP 80	330 pkts
10.0.0.1	10.1.0.3	TCP 25	330 pkts
10.0.0.7	10.1.0.9	TCP 80	330 pkts
10.0.0.1	10.1.0.3	TCP 80	330 pkts

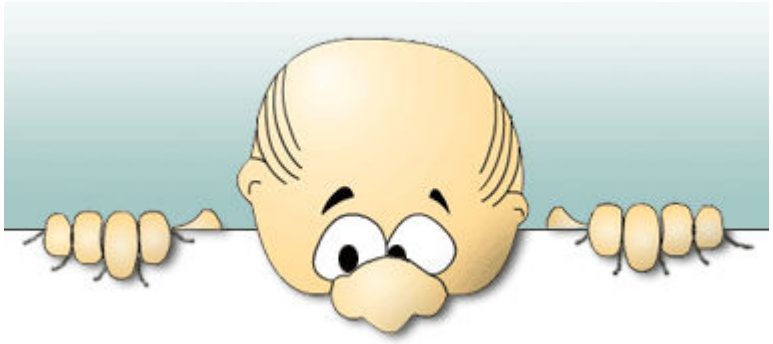
Пример модели отношений между узлами сети



Реагирование

Оповещение ⇨
Блокировка ⇨
Запуск внешней программы ⇨
• • •

Системы обнаружения атак



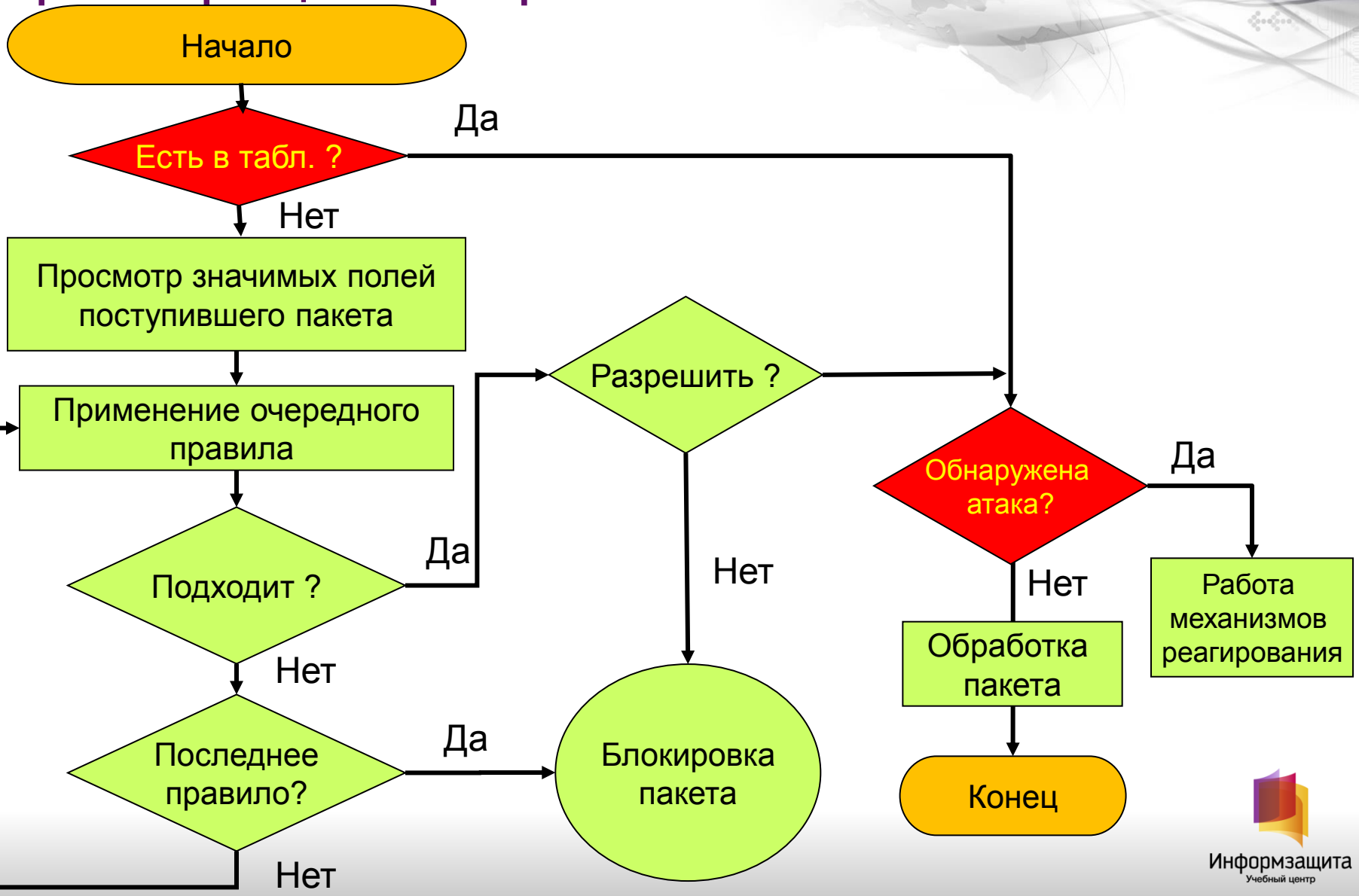
Системы противодействия атакам

Информзащита
Учебный центр

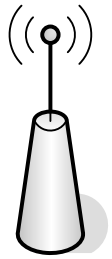
Блокировка

- Аварийное завершение TCP-соединения
- Посылка ICMP Destination Unreachable для блокировки взаимодействия по протоколу UDP
- Блокировка трафика, содержащего признаки атаки
- блокировка последующего взаимодействия (blacklists, карантин)

Интеграция предотвращения атак и фильтрации трафика



Специализация систем обнаружения атак



Беспроводные сети

Специализированный сервер

Беспроводные сети

Обнаружение атак – «не роскошь, а необходимость»

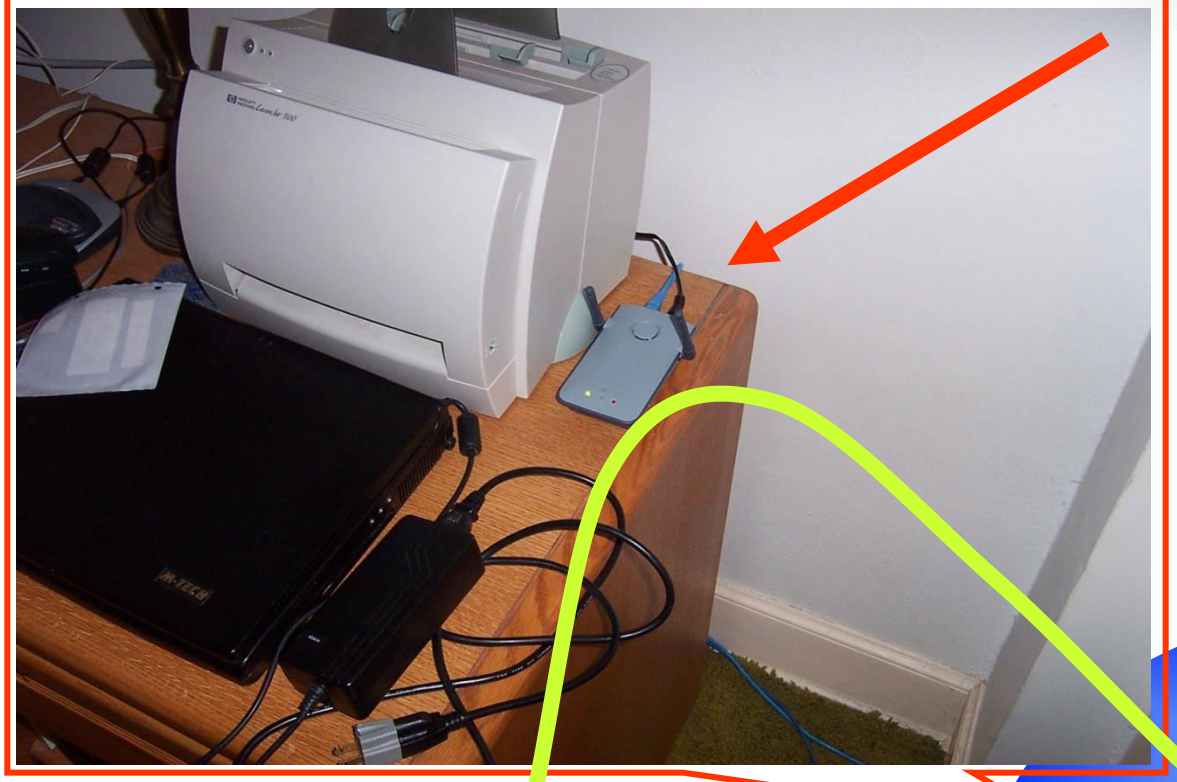
Контроль уровней 1 и 2 (физического и канального)

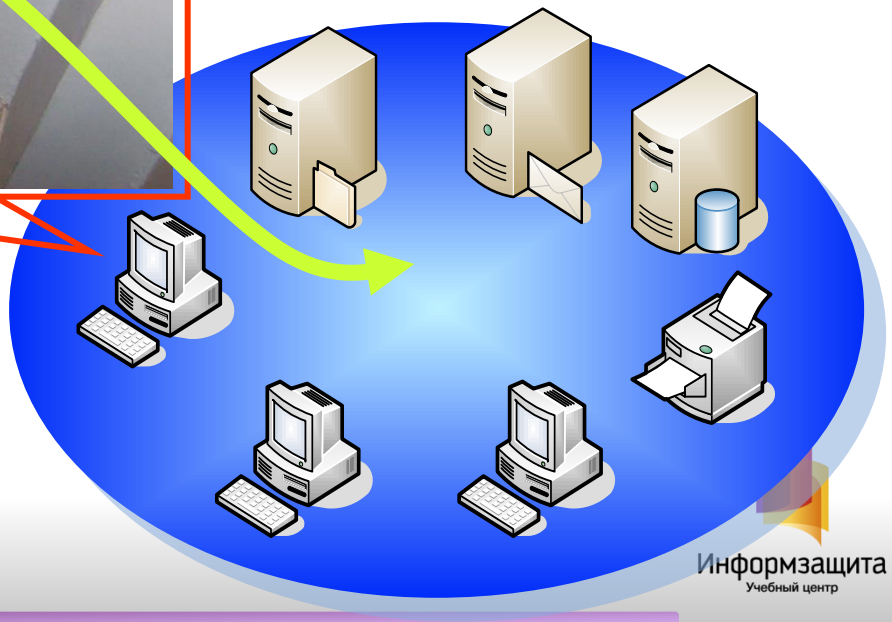
Необходимость локализации нарушителя

Обнаружение атак в беспроводных сетях

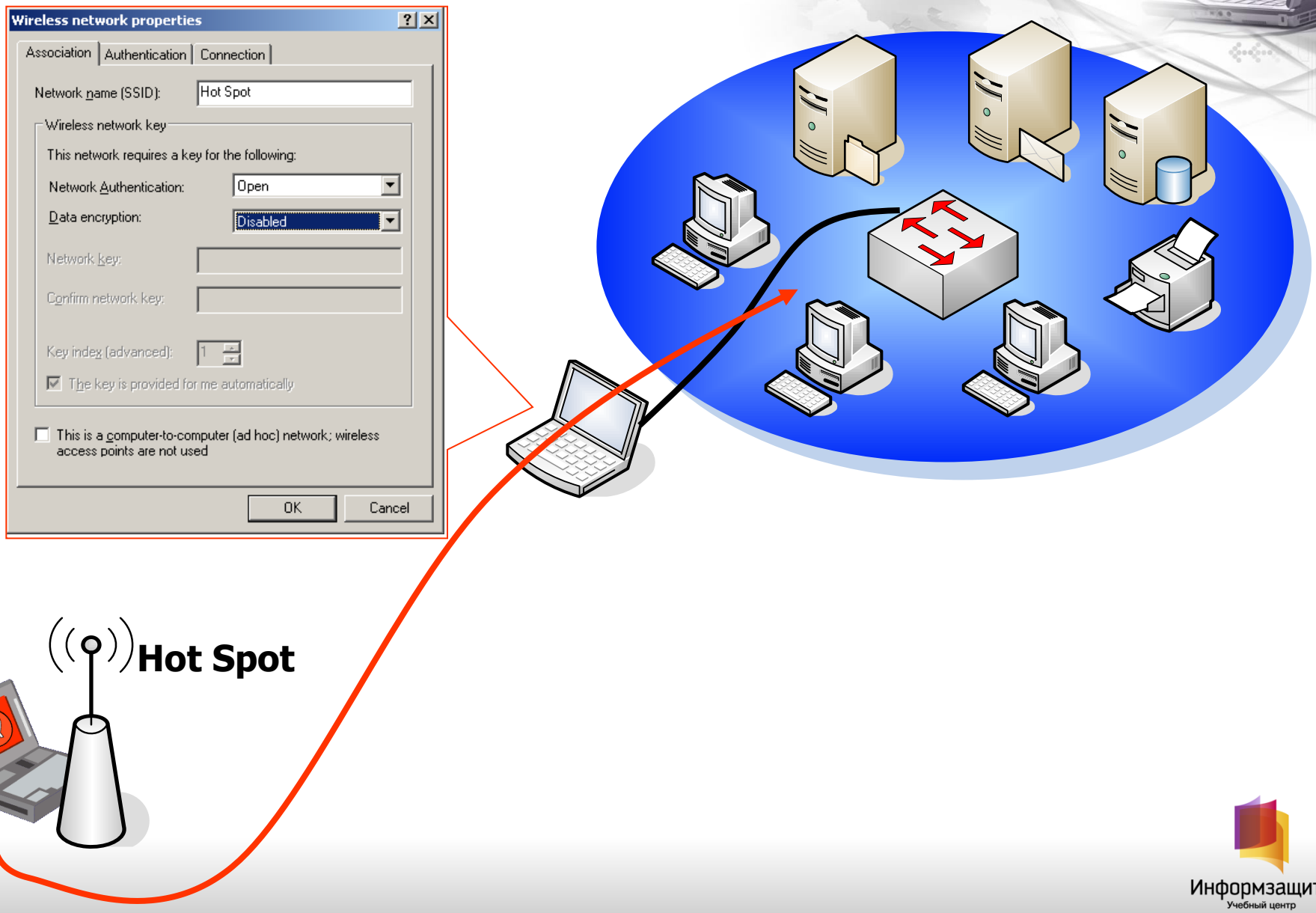
- **Несанкционированное использование беспроводных устройств**
- **Атаки на устройства и сервисы беспроводной сети, в том числе:**
  - Отказ в обслуживании
  - Сбор информации о беспроводных сетях;
  - Атаки на механизм аутентификации 802.1x;
  - Установка ложных точек доступа;
  - Атаки на клиентов беспроводных сетей

Несанкционированные беспроводные устройства



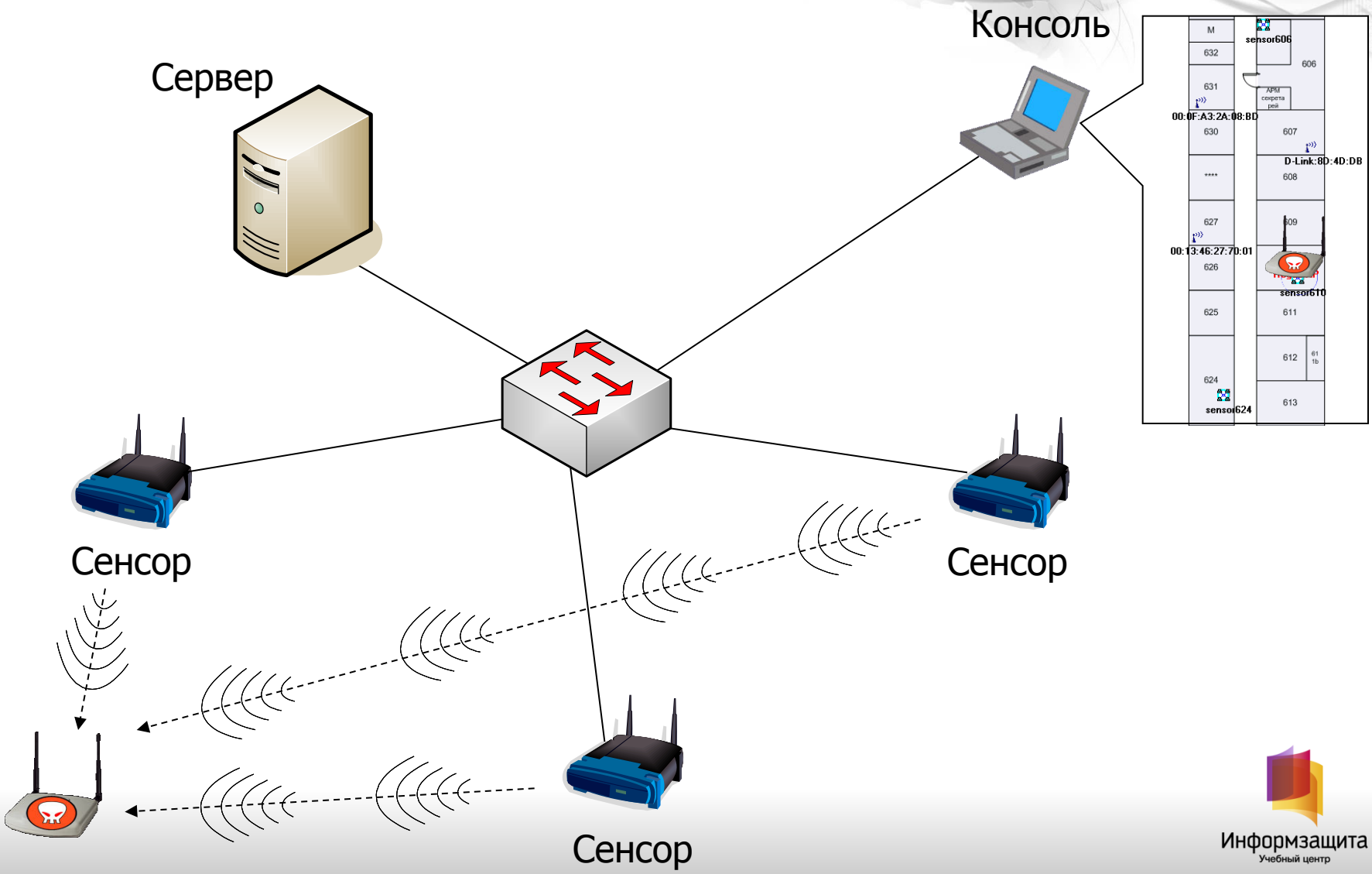


Пример: атаки на клиентов



Информзащита
Учебный центр

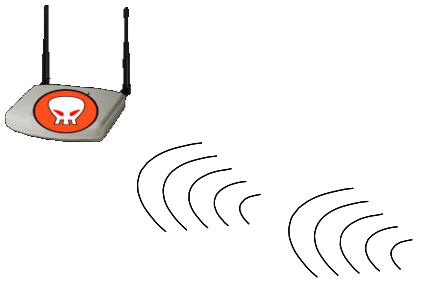
Инфраструктура обнаружения атак в беспроводной сети

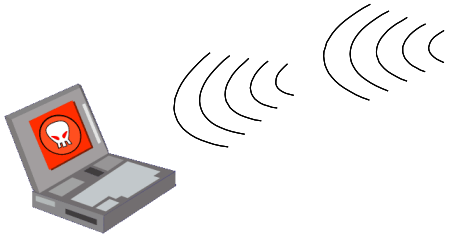


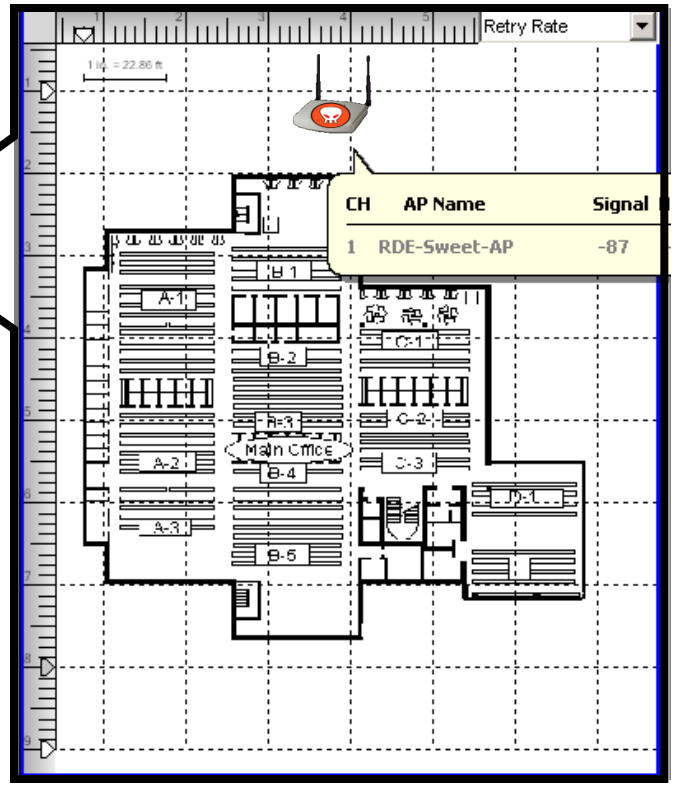
Информзащита
Учебный центр

Инфраструктура обнаружения атак в беспроводной сети

«Облегчённый» вариант

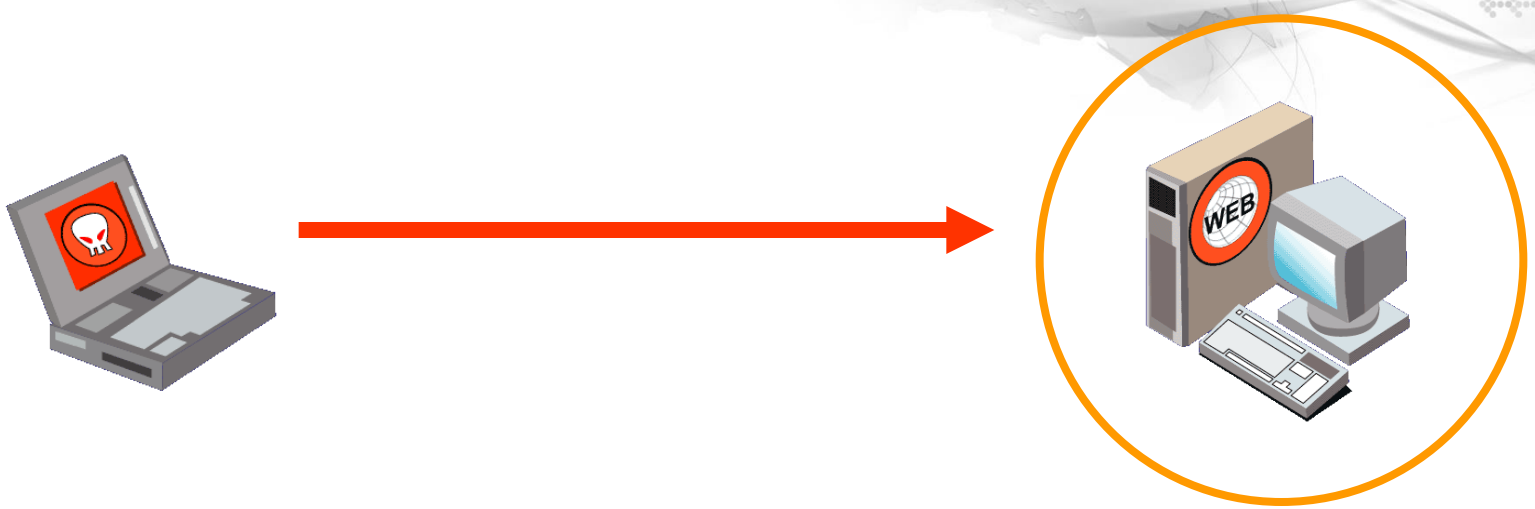






Информзащита
Учебный центр

Специализированный сервер



- **Рекомендуемый вариант – специализированная HIPS**
- **Учёт специфики сервера**
- **Возможно использование Network IDS/IPS**

Информзащита
Учебный центр

Пример – Web-приложение

Web Application Security Consortium

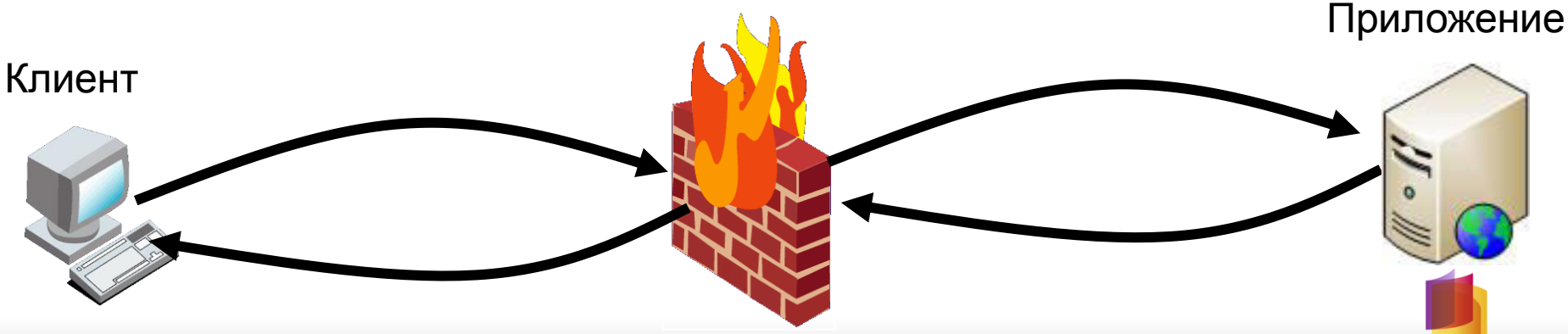
OWASP
The Open Web Application Security Project

1. Authentication
2. Authorization
3. Client-side Attacks
4. Command Execution
5. Information Disclosure
6. Logical Attacks

Информзащита
Учебный центр

Возможности

- **Фильтрация HTTP-трафика (запросов и ответов)**
- **Защита от web-атак (WASC, OWASP)**
- **Защита от роботов, поведенческий анализ**



Выводы

- Основные варианты классификации:
  - Host-based/Network-Based
  - Misuse detection/Anomaly based detection
  - Общего характера / Специализированные