КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

04 октября 2018 г.
г. Красноярск

#CODEIB

СОВРЕМЕННЫЙ ПОДХОД К УПРАВЛЕНИЮ ИБ

КОТ ИБ corporation

КОТ ИБ

ПЕТР ФЕДОСЕЕВ,
КОМПАНИЯ ООО «РОТЕКС-С»

EMAIL: PEFEDOSEEV@SIIT.RU

СОВРЕМЕННАЯ IT - ИНФРАСТРУКТУРА

#CODEIB

2. Офисные приложения

5. Мобильные устройства

7. Устройства контролируемые через интернет

4. Internet

1. Бизнес-процессы

3. Внешние сети передачи данных

6. Облачные ресурсы

Модель: Alexey Lukatsky статья.

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС

1 **БИЗНЕС-ПРОЦЕССЫ**
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА ОБЕСПЕЧИВАЮЩИЕ ОСНОВНЫЕ, КРИТИЧНЫЕ ПРОЦЕССЫ.

2 **ОФИСНЫЕ ПРИЛОЖЕНИЯ**
ОСНОВНАЯ МАССА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И СТАНДАРТНОЕ ОФИСНОЕ ПО.

3 **ВНЕШНИЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ**
НЕ КОРПОРАТИВНЫЕ СЕТИ, ИНТЕРНЕТ

4 **ИНТЕРНЕТ**
ПРОВАЙДЕР, ОПЕРАТОР, САЙТЫ

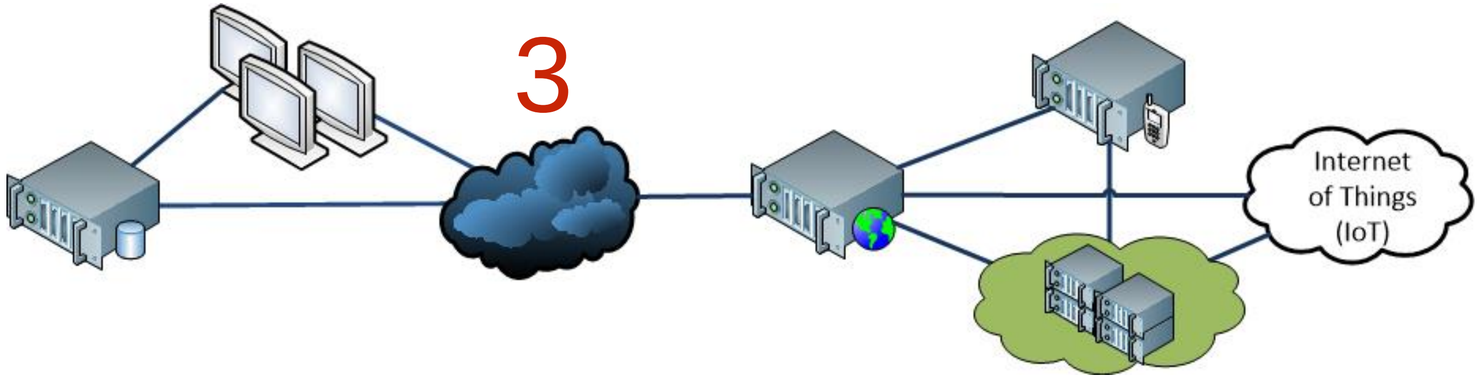
5 **МОБИЛЬНЫЕ УСТРОЙСТВА**
ВАЖНЫЕ И КРИТИЧЕСКИЕ ДАННЫЕ ХРАНЯЩИЕСЯ НА МОБИЛЬНЫХ УСТРОЙСТВАХ.

6 **ОБЛАЧНЫЕ РЕСУРСЫ**
ХРАНЕНИЕ ДАННЫХ. РАЗМЕЩЕНИЕ СЕРВЕРОВ И Т.Д.

7 **IOT**
УСТРОЙСТВА КОНТРОЛИРУЕМЫЕ ЧЕРЕЗ ИНТЕРНЕТ

Модель: Alexey Lukatsky статья.

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС



3 **ВНЕШНИЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ**
НЕ КОРПОРАТИВНЫЕ СЕТИ, ИНТЕРНЕТ

Средства защиты:

FW – межсетевые экраны

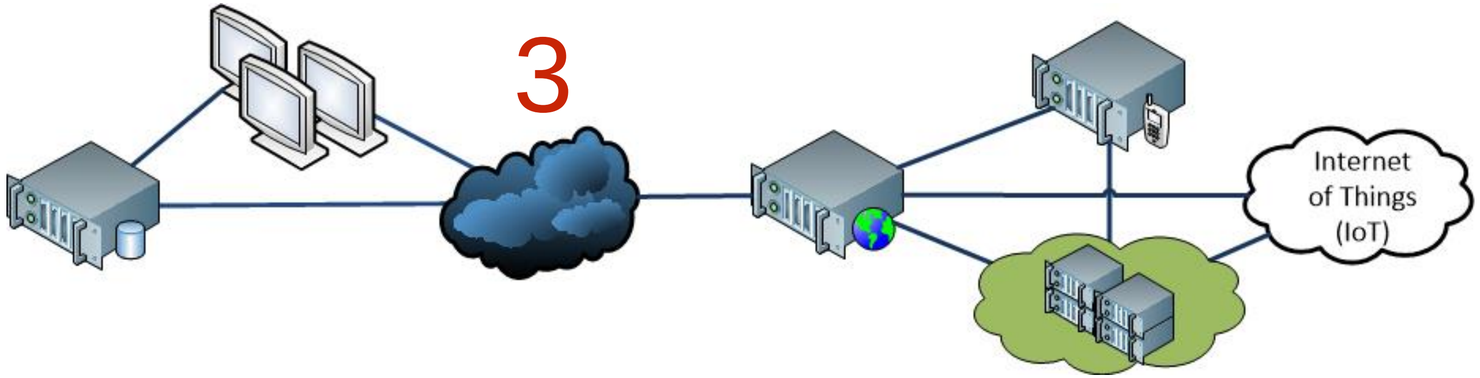
Фильтрация трафика

IDS/IPS – система обнаружения

Распознавание с использованием сигнатур.
Предотвращение атак.

Модель: Alexey Lukatsky статья.

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС



3 **ВНЕШНИЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ**
НЕ КОРПОРАТИВНЫЕ СЕТИ, ИНТЕРНЕТ

Средства защиты:

NGFW – межсетевые экраны

Фильтрация приложений.
Работа на прикладном уровне

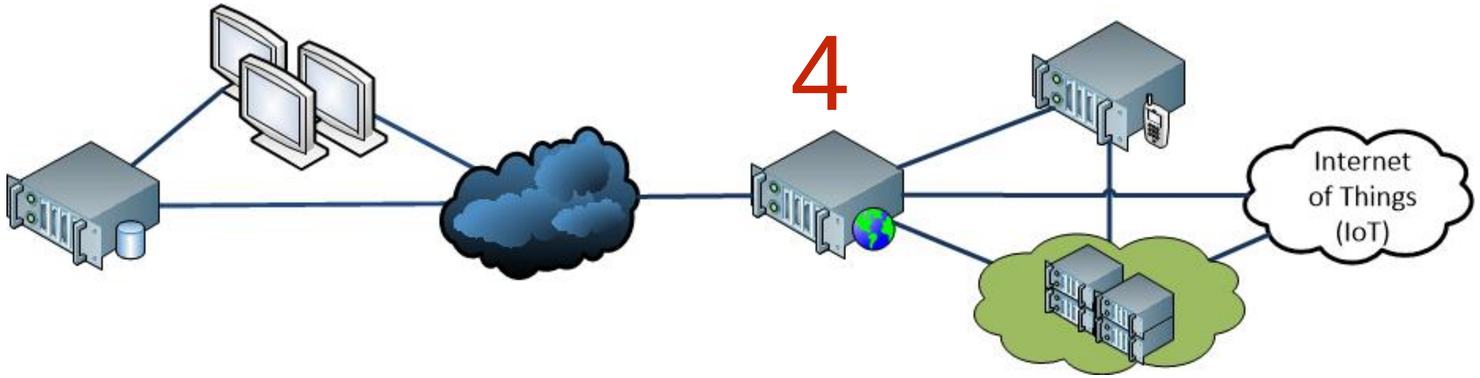
NGIDS/IPS – система обнаружения

Распознавание атакующих.
Методы обнаружений аномалий

Распознавание шифрованного трафика

Модель: Alexey Lukatsky статья.

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС

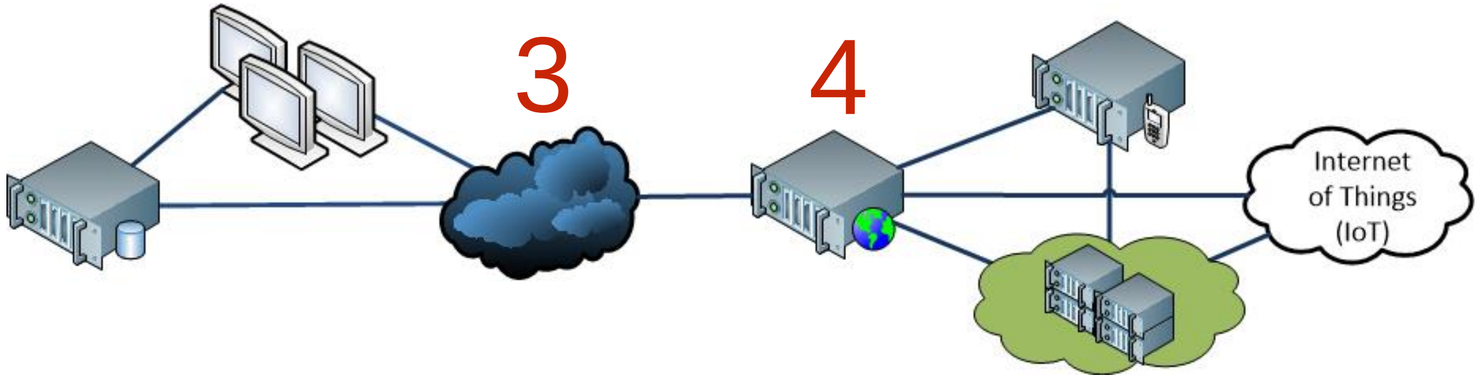


4 **ИНТЕРНЕТ**
ПРОВАЙДЕР, ОПЕРАТОР, САЙТЫ

DDoS атаки

Модель: Alexey Lukatsky статья.

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС



ИНТЕРНЕТ
ПРОВАЙДЕР, ОПЕРАТОР, САЙТЫ

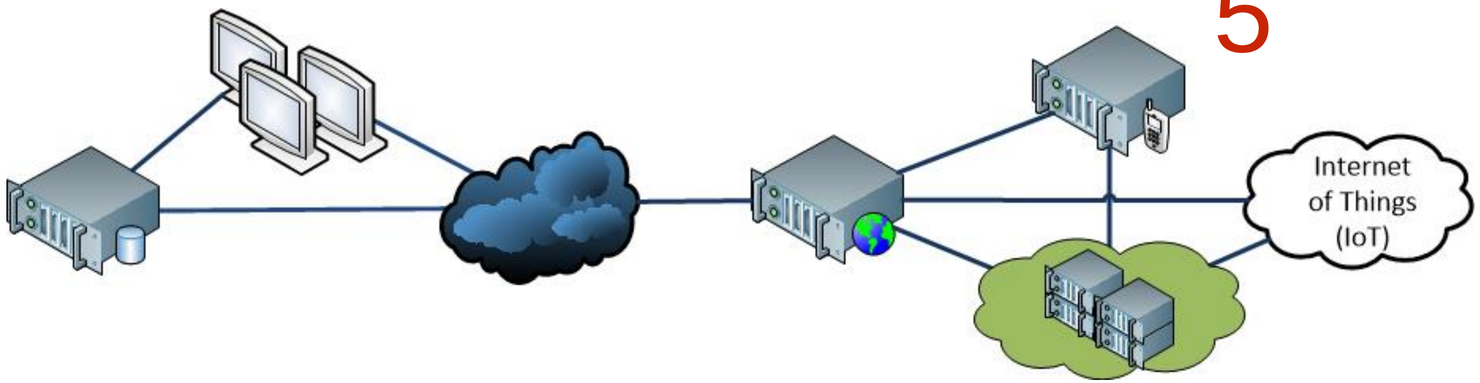
Web Application Firewall (WAF)

Secure Internet Gateway (SIG)

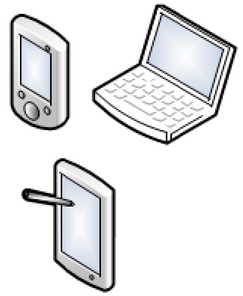
Защита электронной почты

Модель: Alexey Lukatsky статья.

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС



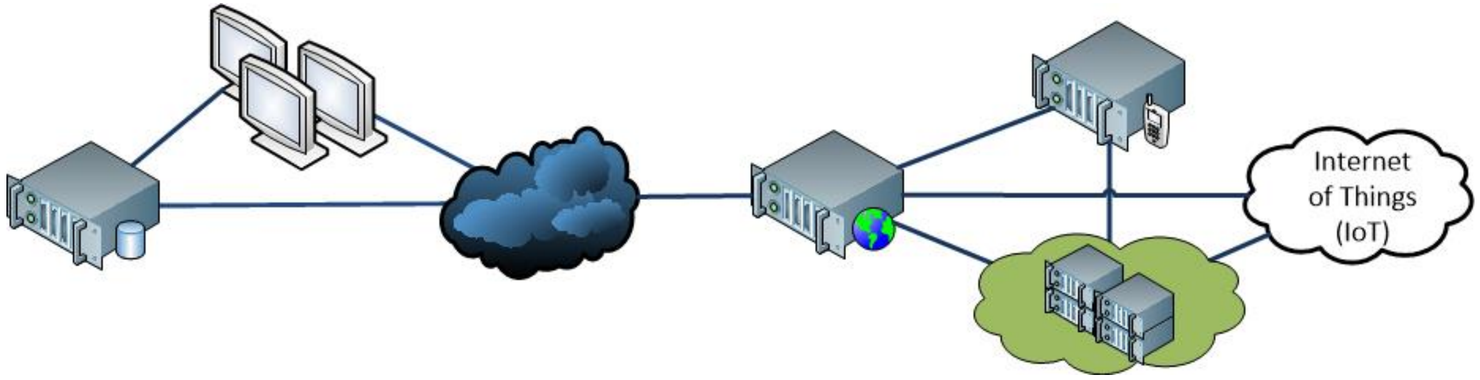
5 **МОБИЛЬНЫЕ УСТРОЙСТВА**
ВАЖНЫЕ И КРИТИЧЕСКИЕ ДАННЫЕ ХРАНЯЩИЕСЯ НА МОБИЛЬНЫХ УСТРОЙСТВАХ



Многофакторная аутентификация
Шифрование данных
Применение технологии VDI

Модель: Alexey Lukatsky статья.

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС



6

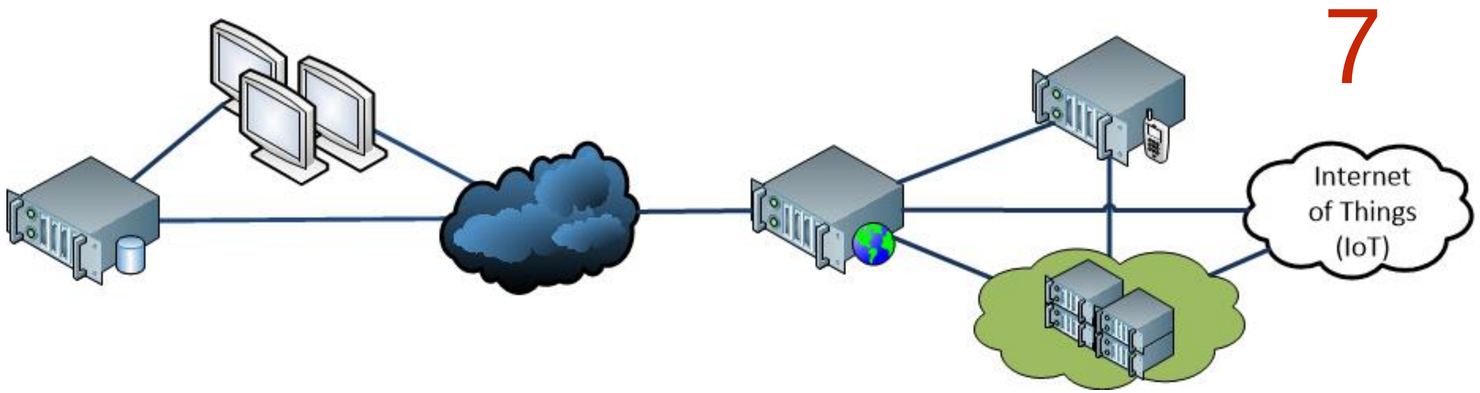
6 ОБЛАЧНЫЕ РЕСУРСЫ
ХРАНЕНИЕ ДАННЫХ. РАЗМЕЩЕНИЕ СЕРВЕРОВ И Т.Д

Контроль действий сотрудников, нарушителей политик ИБ.
Размещение и хранение служебной информации на внешних ресурсах.
Yandex Disk, MS Azure и т.д.

Cloud Access Security Broker (CASB)

Модель: Alexey Lukatsky статья.

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС



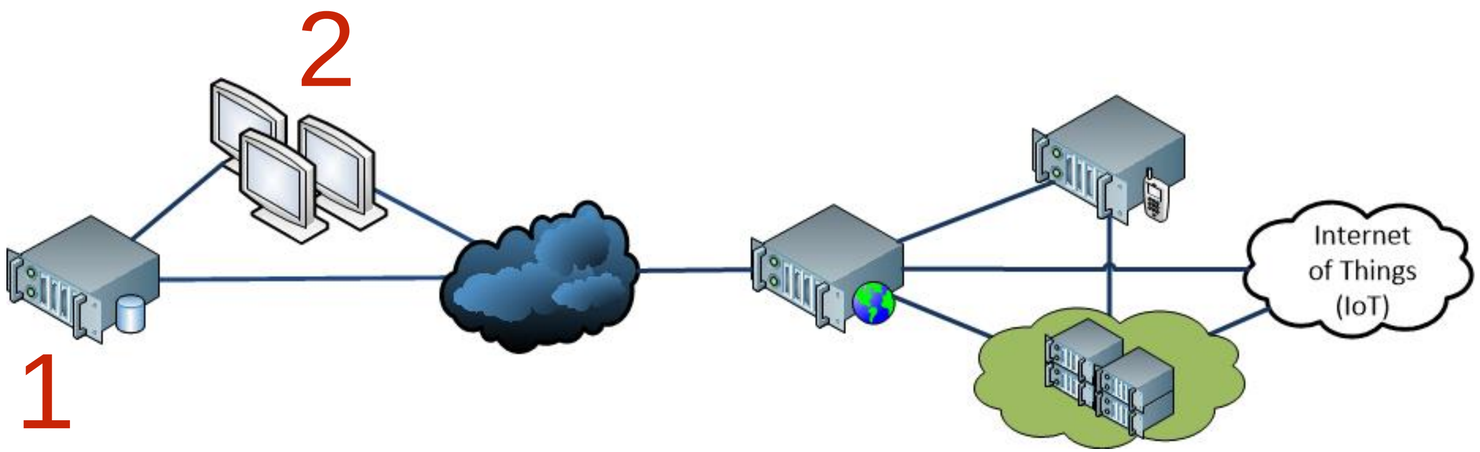
7 **IOT**
УСТРОЙСТВА КОНТРОЛИРУЕМЫЕ
ЧЕРЕЗ ИНТЕРНЕТ

Любые устройства, на которые организован доступ через Интернет:
Видеокамеры, оборудование измерения температуры,
электрооборудование и т.д.

Средства инспекции DNS-трафика

Модель: Alexey Lukatsky статья.

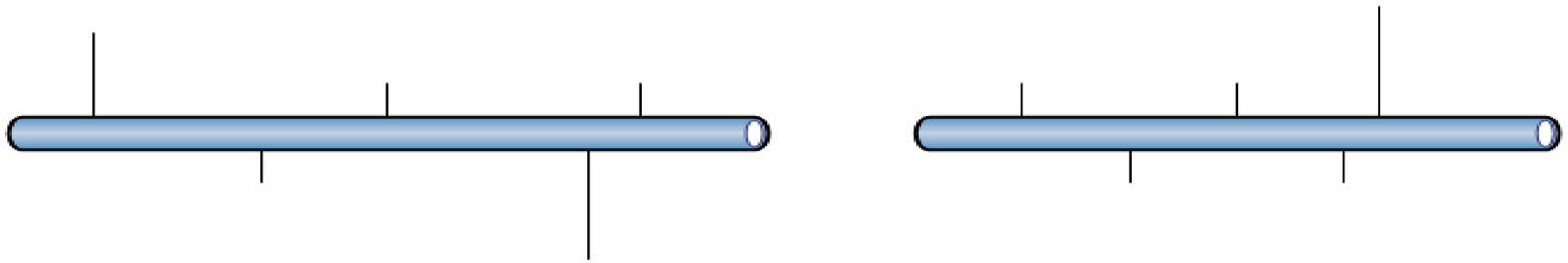
ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС



1 **БИЗНЕС-ПРОЦЕССЫ**
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА ОБЕСПЕЧИВАЮЩИЕ ОСНОВНЫЕ, КРИТИЧНЫЕ ПРОЦЕССЫ.

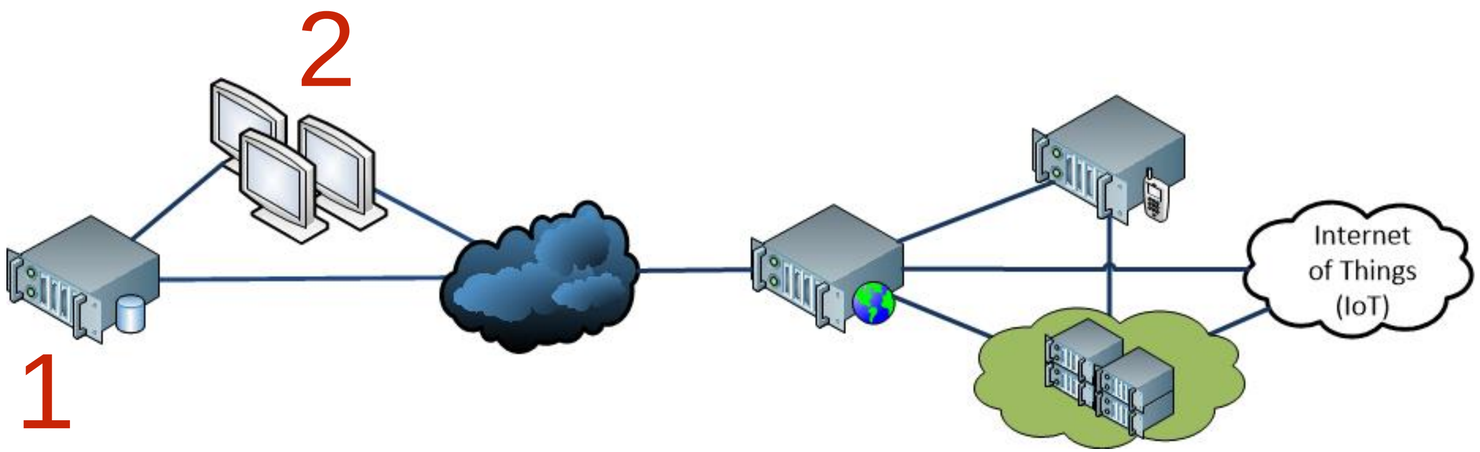
2 **ОФИСНЫЕ ПРИЛОЖЕНИЯ**
ОСНОВНАЯ МАССА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И СТАНДАРТНОЕ ОФИСНОЕ ПО.

Сегментация сетей



Модель: Alexey Lukatsky статья.

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС



1

БИЗНЕС-ПРОЦЕССЫ
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА ОБЕСПЕЧИВАЮЩИЕ ОСНОВНЫЕ, КРИТИЧНЫЕ ПРОЦЕССЫ.

2

ОФИСНЫЕ ПРИЛОЖЕНИЯ
ОСНОВНАЯ МАССА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И СТАНДАРТНОЕ ОФИСНОЕ ПО.

Распределенные межсетевые экраны внутри сети

Network Access Control, NAC

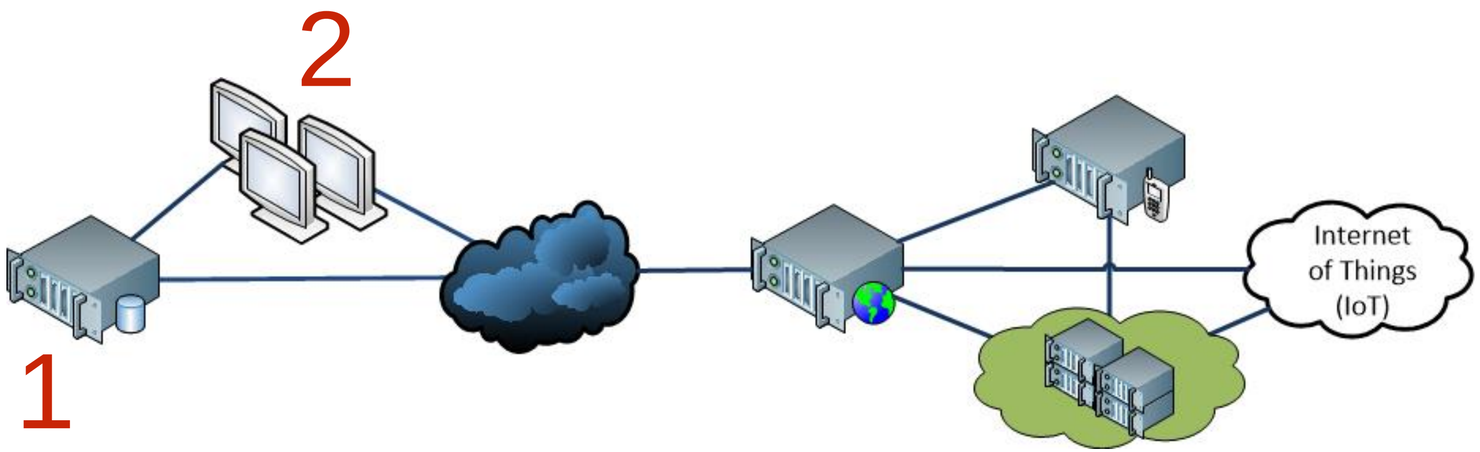
Система обнаружения атак внутри сети

Network Traffic analysis (NTA)

Модель: Alexey Lukatsky статья.

#CODEIB

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС



1 **БИЗНЕС-ПРОЦЕССЫ**
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА ОБЕСПЕЧИВАЮЩИЕ ОСНОВНЫЕ, КРИТИЧНЫЕ ПРОЦЕССЫ.

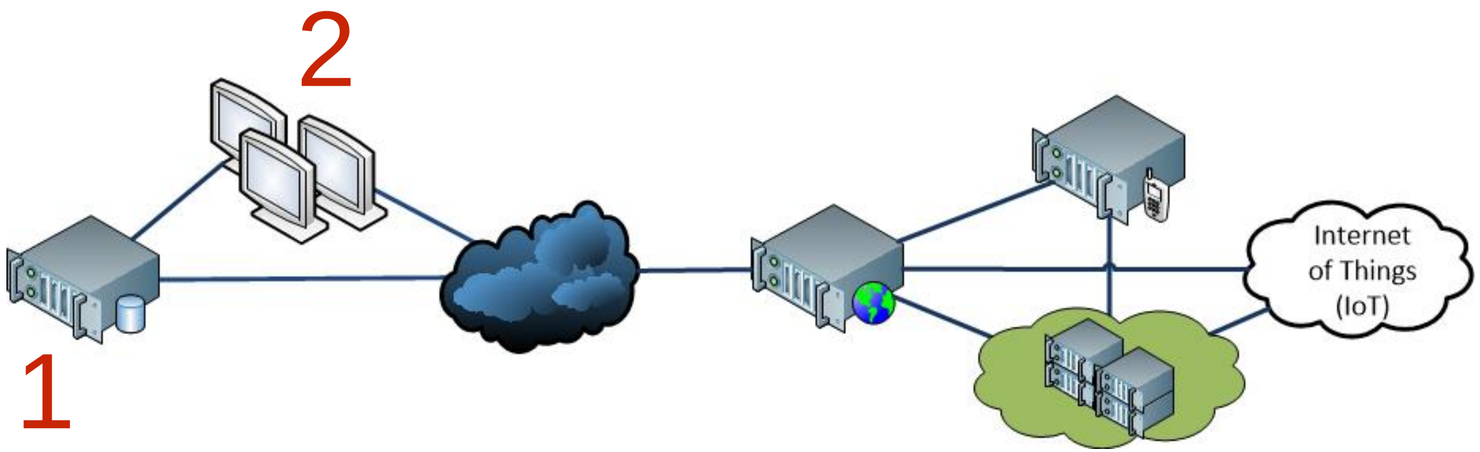
2 **ОФИСНЫЕ ПРИЛОЖЕНИЯ**
ОСНОВНАЯ МАССА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И СТАНДАРТНОЕ ОФИСНОЕ ПО.

1 Защита БД Аудит БД
Шифрование БД

2 Антивирусное ПО?
Malware? SandBox

Модель: Alexey Lukatsky статья.

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС



1 **БИЗНЕС-ПРОЦЕССЫ**
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА ОБЕСПЕЧИВАЮЩИЕ ОСНОВНЫЕ, КРИТИЧНЫЕ ПРОЦЕССЫ.

2 **ОФИСНЫЕ ПРИЛОЖЕНИЯ**
ОСНОВНАЯ МАССА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И СТАНДАРТНОЕ ОФИСНОЕ ПО.

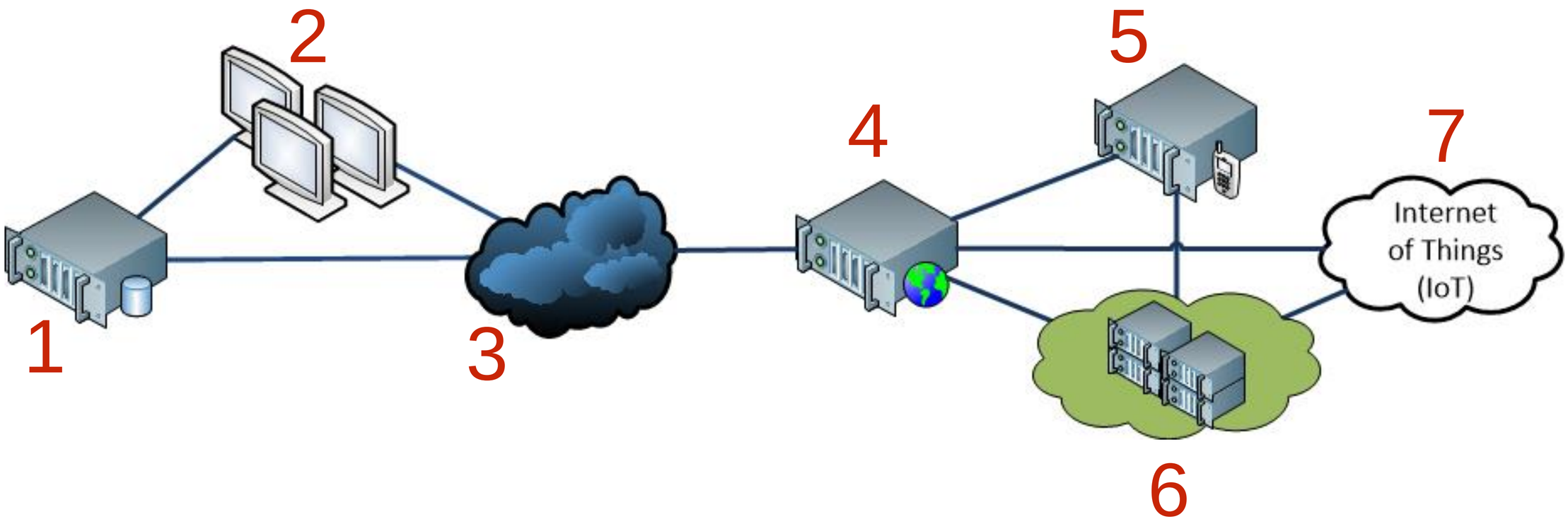
1 Резервное копирование
Хранение копий в ДМЗ

2 Резервное копирование
Хранение копий в ДМЗ

Модель: Alexey Lukatsky статья.

#CODEIB

ОСНОВНЫЕ ЭЛЕМЕНТЫ ИС



UNIFIED THREAT MANAGEMENT (UTM)
SECURITY INFORMATION EVENT MANAGEMENT
+ THREAT INTELLIGENCE PLATFORM

Модель: Alexey Lukatsky статья.

СОВРЕМЕННАЯ IT - ИНФРАСТРУКТУРА

#CODEIB

СОВРЕМЕННАЯ IT - ИНФРАСТРУКТУРА

#CODEIB

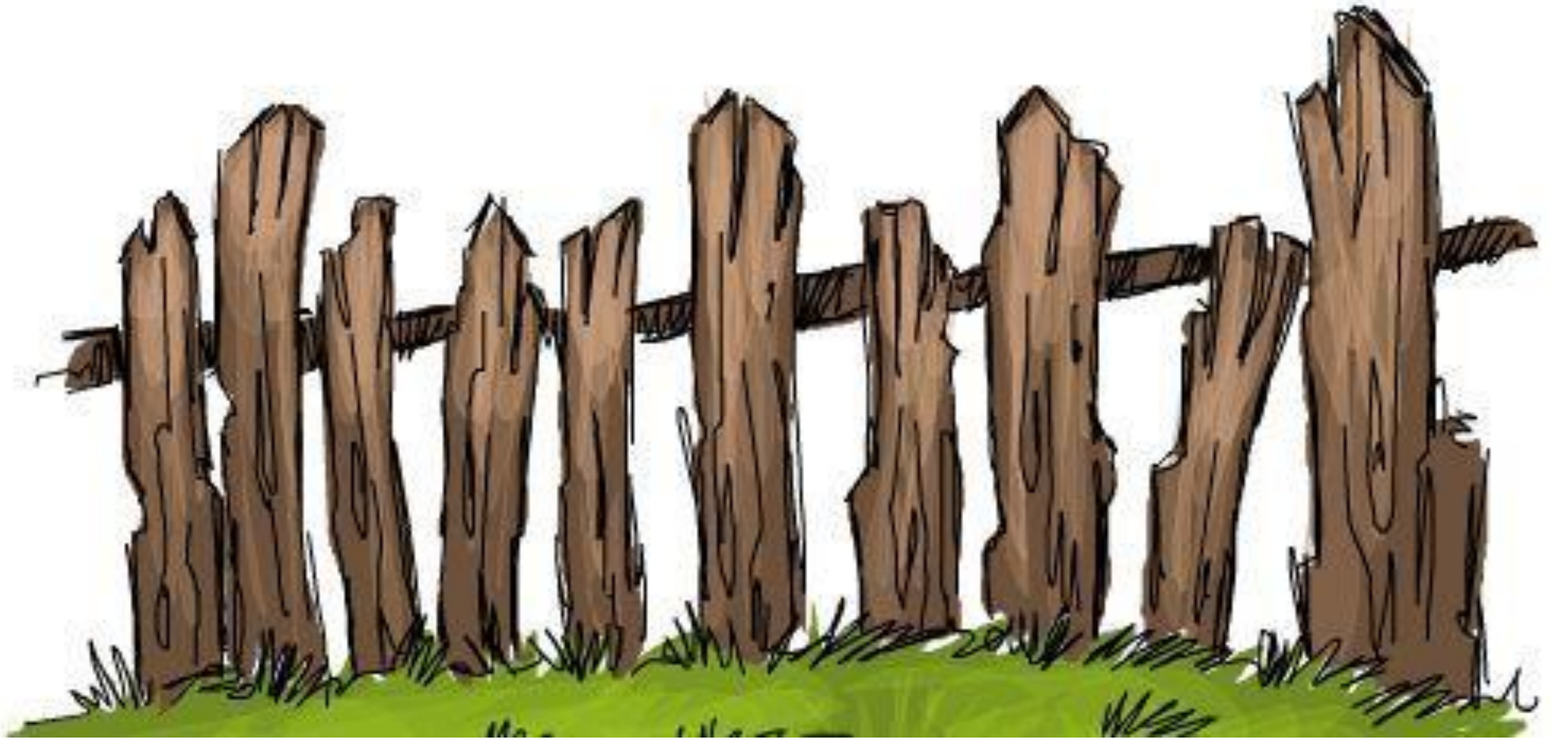
СОВРЕМЕННАЯ IT - ИНФРАСТРУКТУРА

#CODEIB

Главный актив.

Ослабление контроля.

Защита.



Политика ИБ.

Двойной контроль.

Обучение.

СПАСИБО ЗА ВНИМАНИЕ!

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

04 октября 2018 г.
г. Красноярск

#CODEIB

КОТ ИБ
corporation

КОТ ИБ

Петр Федосеев,
ООО «Ротекс-с»

EMAIL: peter@its-24x7.ru