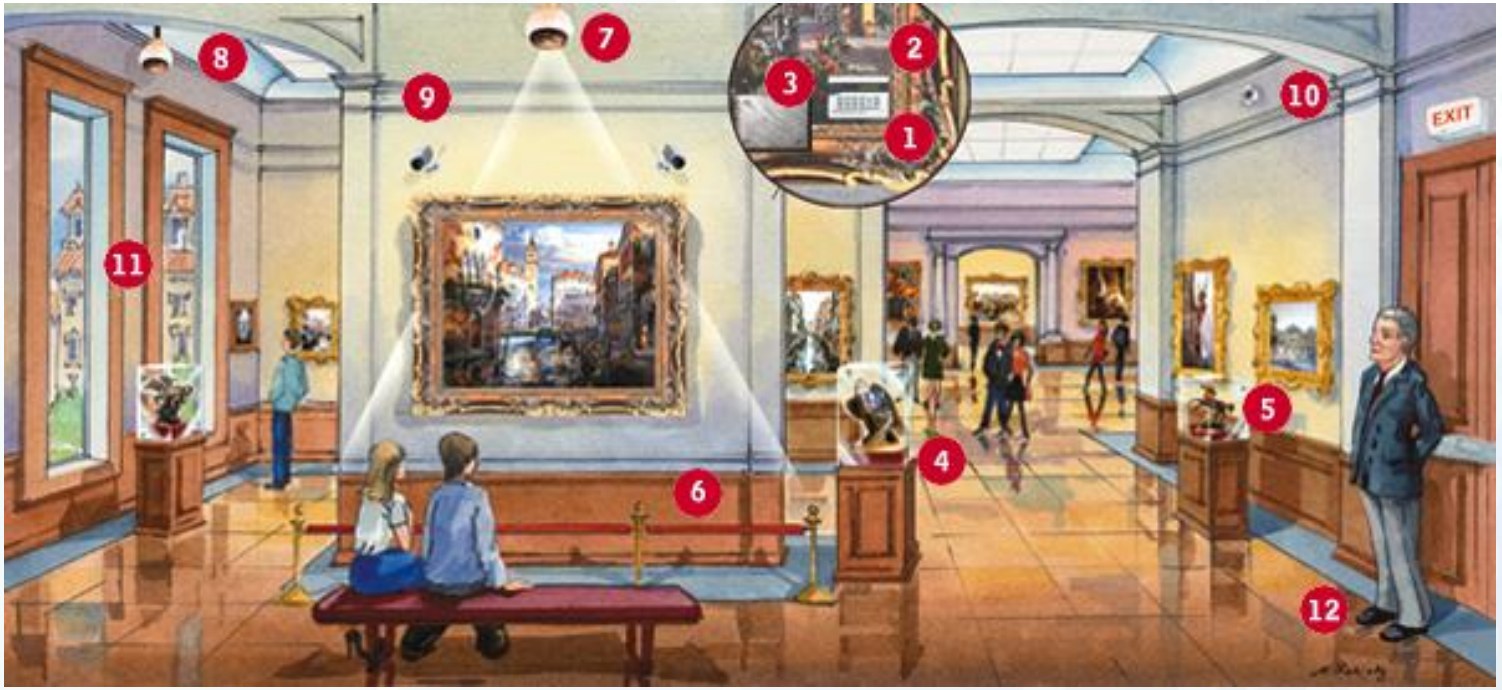
АЙТЕКО
ТЕХНОЛОГИИБЕЗПРОБЕЛОВ

Стратегия информационной безопасности. Цифровой музей 2.0

www.i-teco.ru

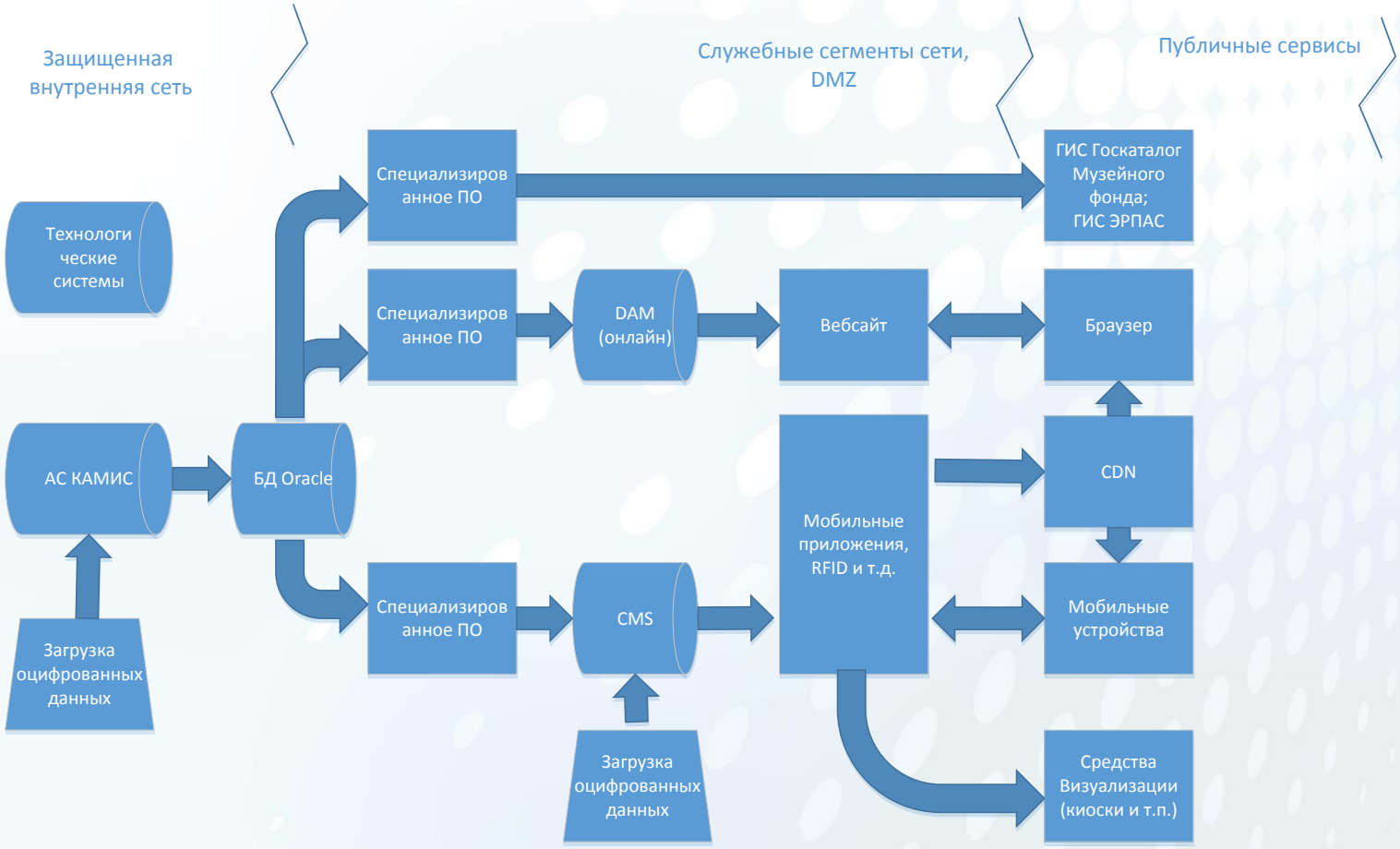
Музей версии 1.0. Безопасность.



1. Беспроводные датчики вибрации
2. Метки (RFID)
3. Специализированные крепления для предметов
4. Защитное остекление
5. Датчики мониторинга окр. среды
6. Ограждения
7. Датчики движения
8. Камеры с функцией детектирования движения
9. Система видеонаблюдения
10. Охранно-пожарная сигнализация
11. Сигнализация
12. Охранник

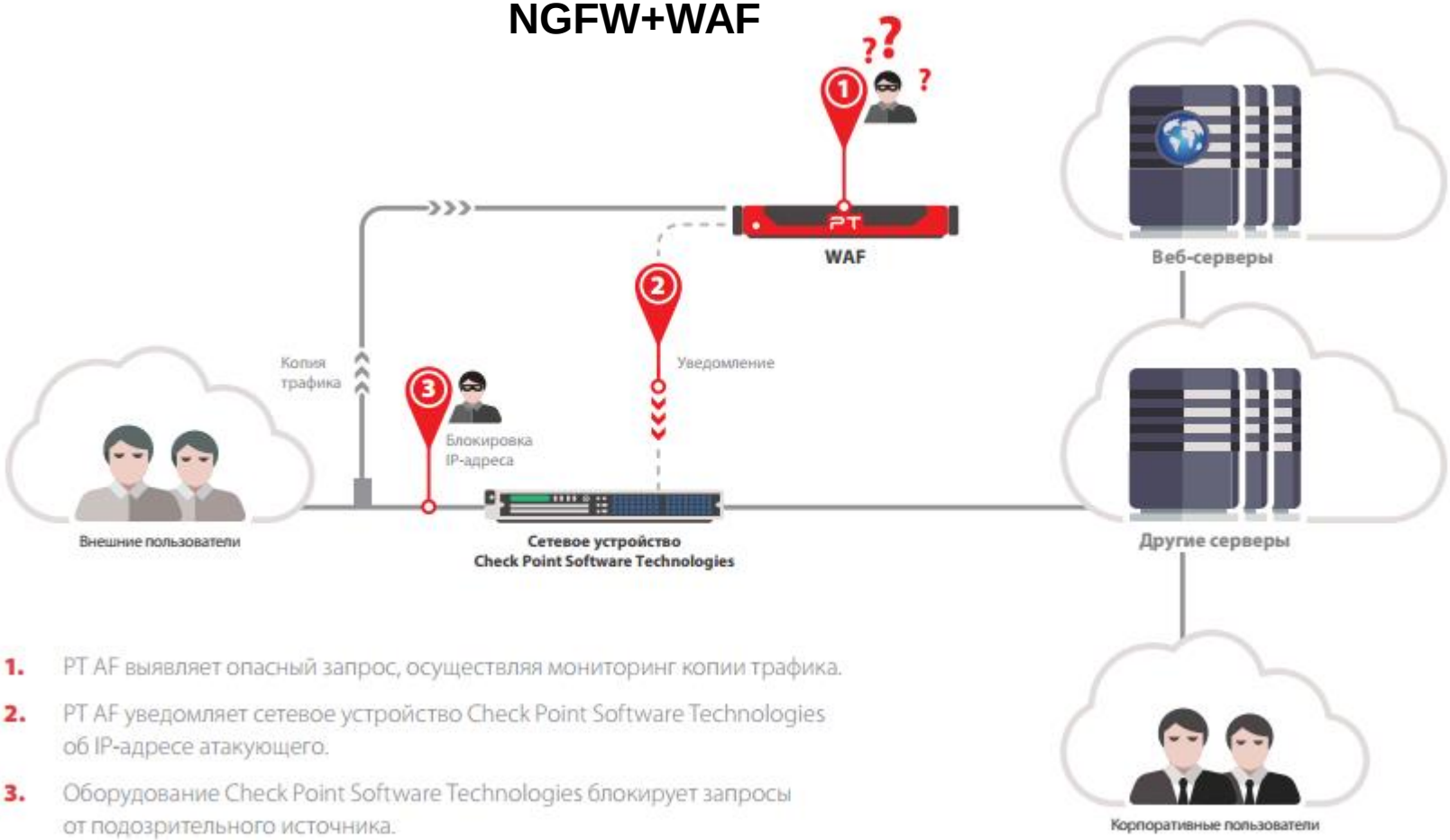
«Государственная культурная политика основывается на признании огромного воспитательного и просветительского потенциала культуры и необходимости его максимального использования в процессе формирования личности. (из проекта Основ государственной культурной политики)»

Информационные потоки




Во всех этих
фотографиях содержатся
новые модули для
вредоносного ПО

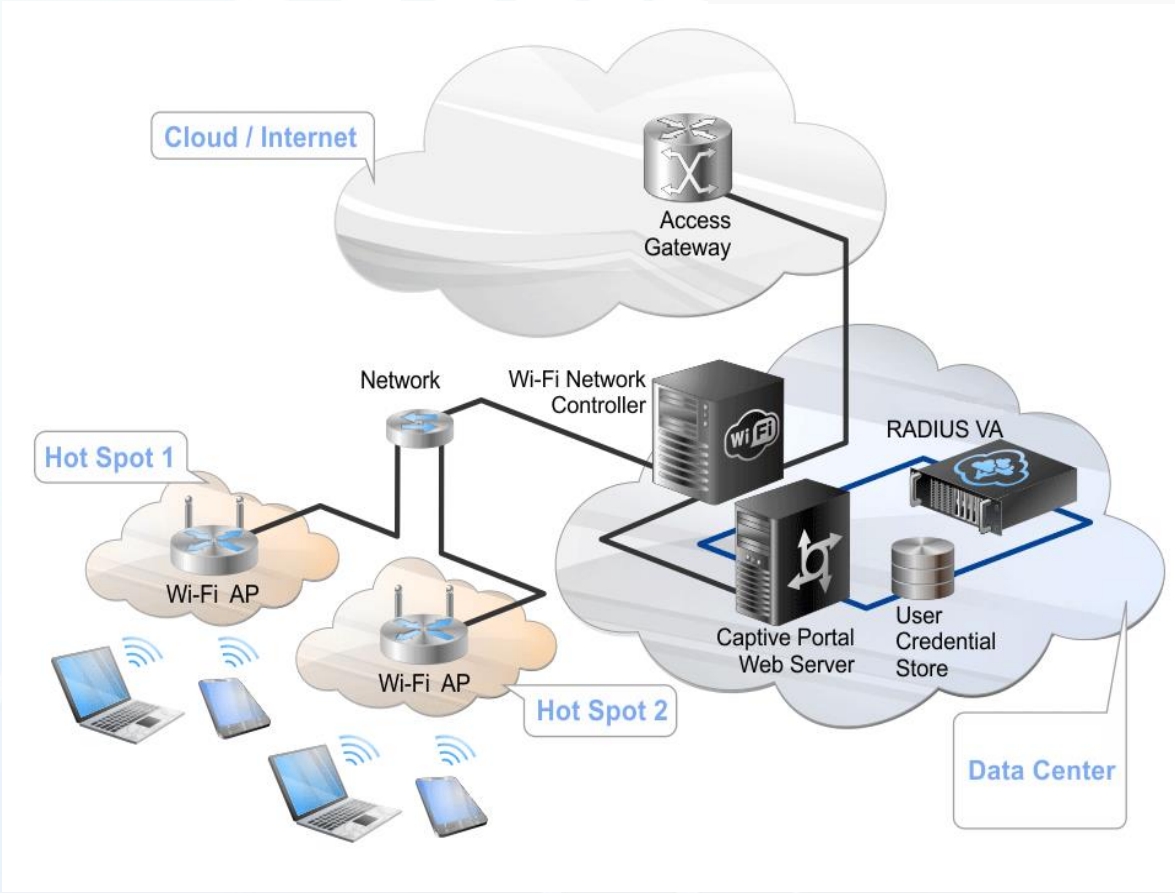
NGFW+WAF



1. PT AF выявляет опасный запрос, осуществляя мониторинг копии трафика.
2. PT AF уведомляет сетевое устройство Check Point Software Technologies об IP-адресе атакующего.
3. Оборудование Check Point Software Technologies блокирует запросы от подозрительного источника.

Беспроводной доступ

Постановление Правительства РФ от 31 июля 2014 г. N 758 "О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей"




Интерактивная визуализация
Корректно написанное ПО и/или мониторинг

Приказ ФСТЭК России от 11 февраля 2013 г. N 17 п.20

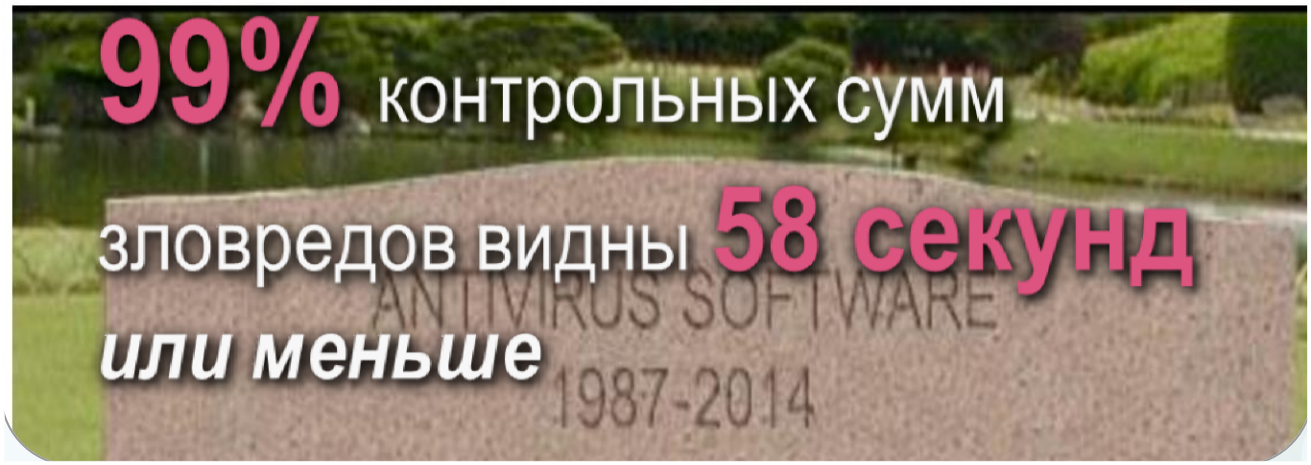
Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

1. идентификацию и аутентификацию субъектов доступа и объектов доступа;
2. управление доступом субъектов доступа к объектам доступа;
3. ограничение программной среды;
4. защиту машинных носителей информации;
5. регистрацию событий безопасности;
6. антивирусную защиту;
7. обнаружение (предотвращение) вторжений;
8. контроль (анализ) защищенности информации;
9. целостность информационной системы и информации;
10. доступность информации;
11. защиту среды виртуализации;
12. защиту технических средств;
13. защиту информационной системы, ее средств, систем связи и передачи данных.

Symantec Says Antivirus Is Dead, World Rolls Eyes

May 07, 2014 11:55 AM EST | 32 Comments

By Max Eddy



Большинство вирусов встречаются лишь раз


Сигнатурные методы защиты
Неэффективны
Что делать?
THREAT EMULATION
Среда эмуляции (Уровни ЦП и ОС), устойчивая к методикам обхо
THREAT EXTRACTION
Проактивное удаление опасного контента при доставке
ENDPOINT FORENSICS
Быстрое понимание ситуации для лучшей защиты исправления
ZERO RANSOMWARE
Идентификация и восстановление после действий программы-вымогателя
ZERO PHISHING
Защита учетных записей от кражи через фишинговые сайты

Почему важна SIEM?

полная интеграция, абсолютная видимость

Интеграция и мониторинг

Общие политики

Настраиваемый Dashboard

Защищенная внутренняя сеть

Самые опасные категории пользователей:

1. пользователи ИС, осуществляющие доступ к ресурсам ИС и, находящиеся в пределах контролируемой зоны (внутренние пользователи)
2. Технический персонал ИС (администраторы)

- Идентификация Аутентификация Авторизация
- Мониторинг действий привилегированных пользователей
- Подтверждение подлинности действий пользователя
- Противодействие навязыванию ложной информации

Министерство культуры Российской Федерации

Возможные инициативы:

1. Создание технического комитета или экспертного совета, отвечающего для стандартизацию применяемых решений по ИБ
2. Создание облачных сервисов ИБ
3. ГосСопка (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации)

АЙТЕКО
ТЕХНОЛОГИИБЕЗПРОБЕЛОВ

Департамент информационной безопасности
Компания «Ай-Теко»

Владимир Баланин
Тел. +7 (495) 777-1095, доб. 3656
Моб. +7 (909) 621-1670
E-mail: balanin@i-teco.ru

Спасибо за внимание