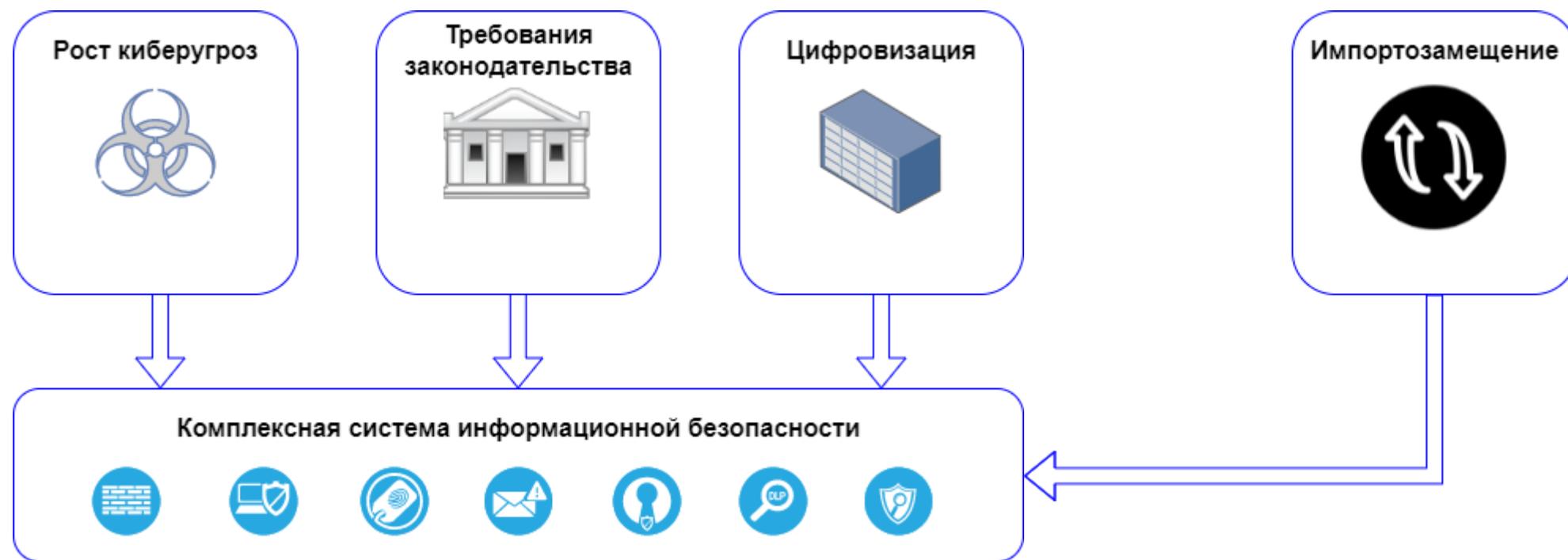




Zero Trust Networking для выполнения требований регуляторов

Проблема



Zero Trust Networking

- Zero Trust – это набор руководящих принципов для проектирования систем информационной безопасности
- ZTN, ZTNA, ZTA – концепции реализации нулевого доверия (Zero Trust)



- Zero Trust – парадигма кибербезопасности, основывающаяся на том, что доверие не предоставляется неявно, а должно постоянно оцениваться

Доступ по Zero Trust

- Какой уровень доверия к субъекту?
- Должен ли быть доступ для данного субъекта?
- Имеет ли устройство, используемое для доступа, должный уровень безопасности?
- Должны ли учитываться другие форм-факторы (время, место)?

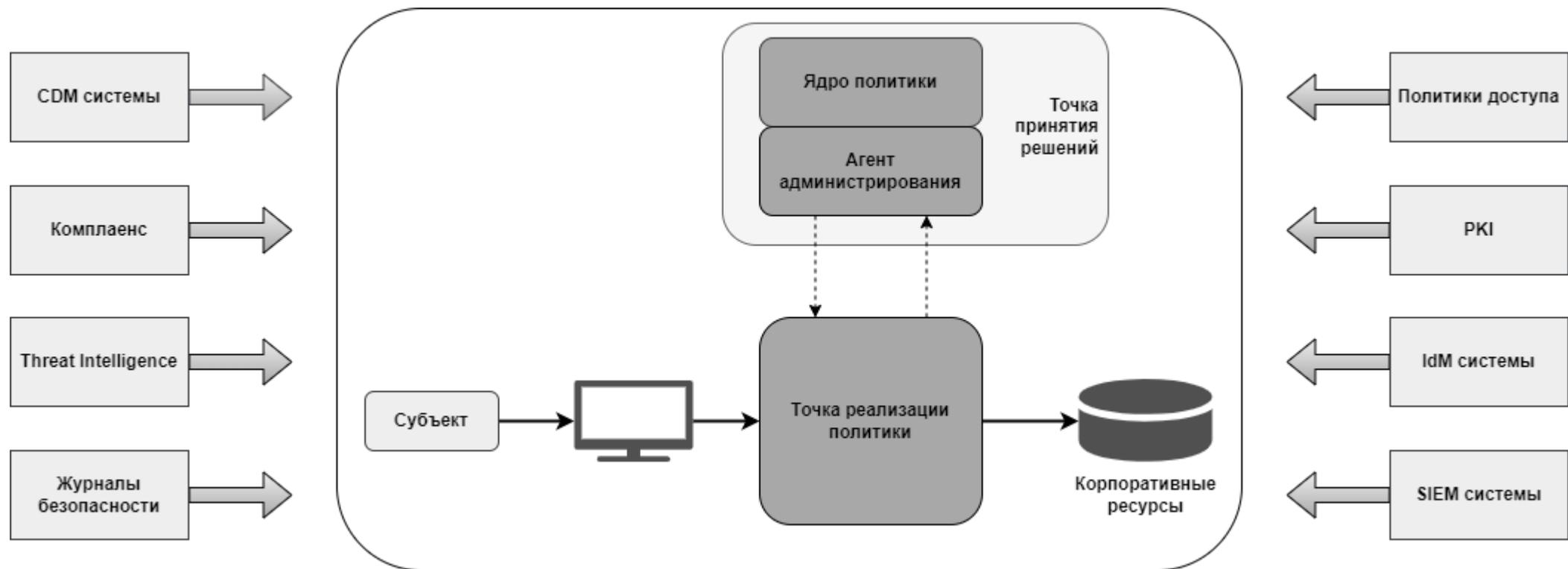


Принципы Zero Trust

- Все источники данных – ресурсы
- Все источники данных защищены независимо от сетевого расположения
- Доступ к ресурсам предоставляется на основе «проверяй - доверяй»
- Доступ к ресурсам определяется динамической политикой
- Авторизация и аутентификация осуществляется перед подключением к ресурсам
- Мониторинг состояния всех устройств



Логические компоненты Zero Trust



Архитектура нулевого доверия

Расширенная идентификация активов

Для идентификации должен использоваться устойчивый к фальсификации фактор

Микросегментация

Сегментация реализуется на уровне сетевой топологии

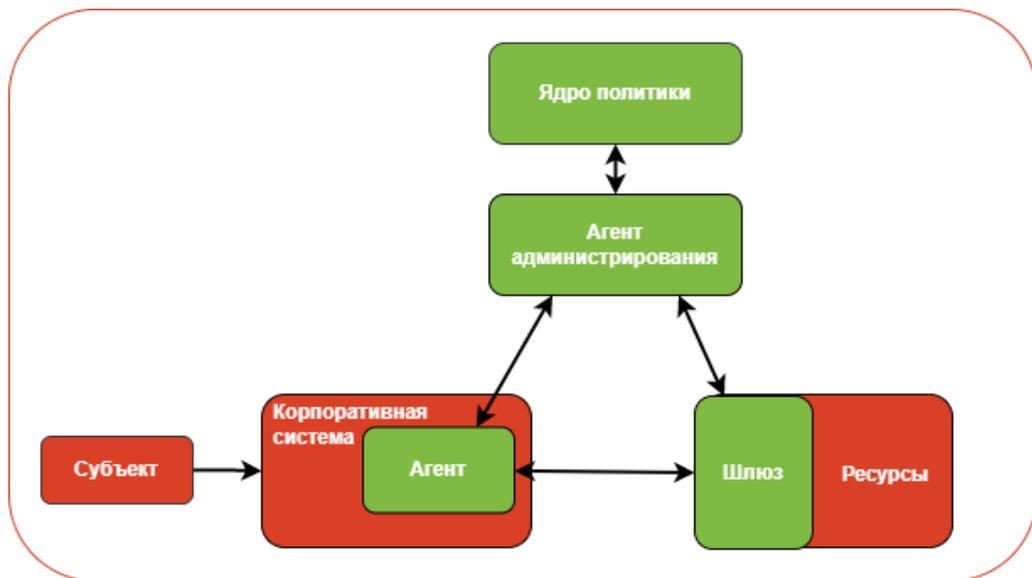
Программно-определяемый периметр

Сегментация реализуется "поверх" сетевой топологии

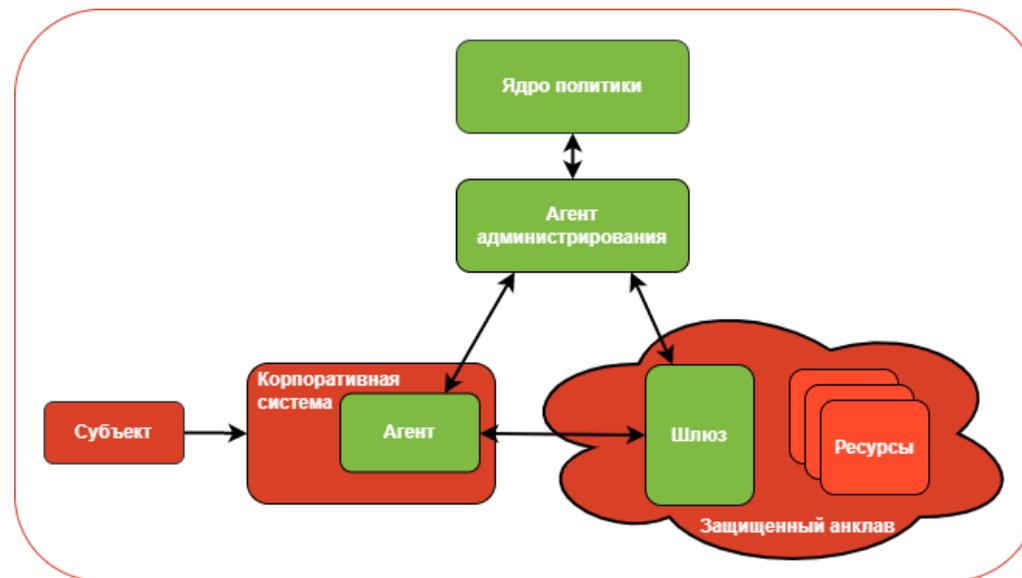


Архитектура нулевого доверия

Агентская архитектура

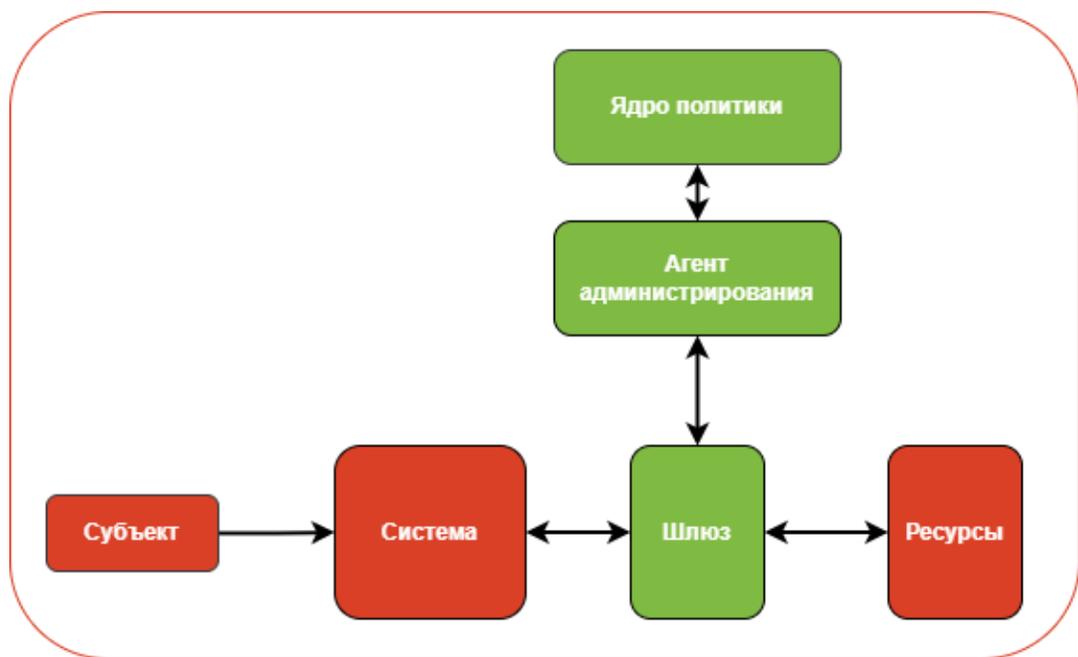


Защищенный анклав

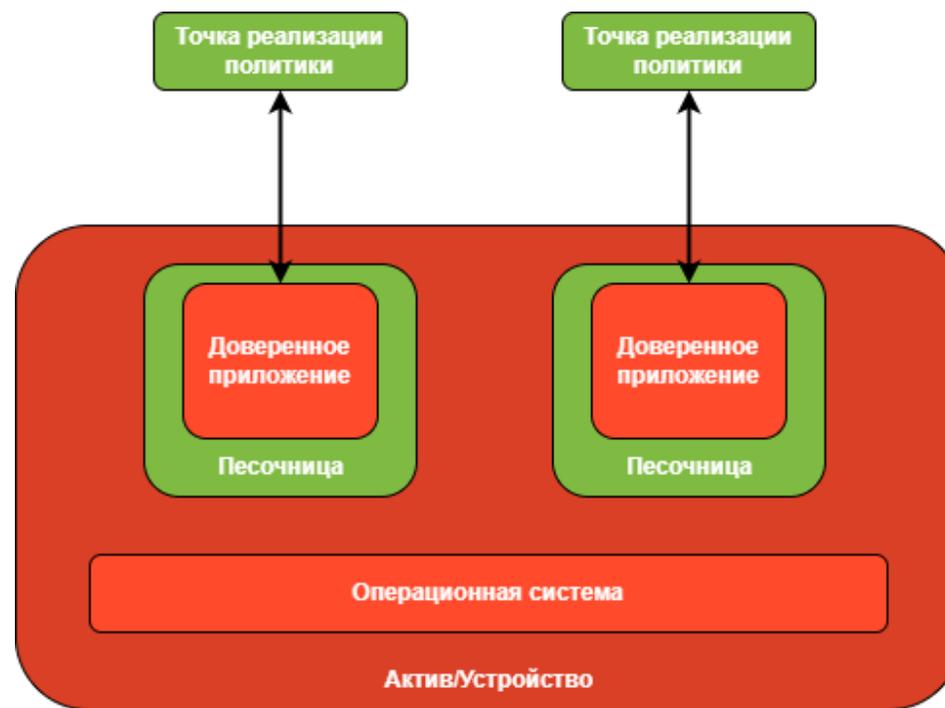


Архитектура нулевого доверия

Ресурсный портал



Песочница



Zero Trust с точки зрения нормативных правовых актов ФСТЭК России

Приказ ФСТЭК России № 239

Местонахождение не влияет на уровень доступа

Максимум проверок в точке подключения

Сеть, даже внутренняя, недоверенна

Требуется идентификация пользователей/ПК для создания доверия

Все коммуникации должны быть зашифрованы

Обнаружение аномалий и избыточного риска

Компрометация произошла

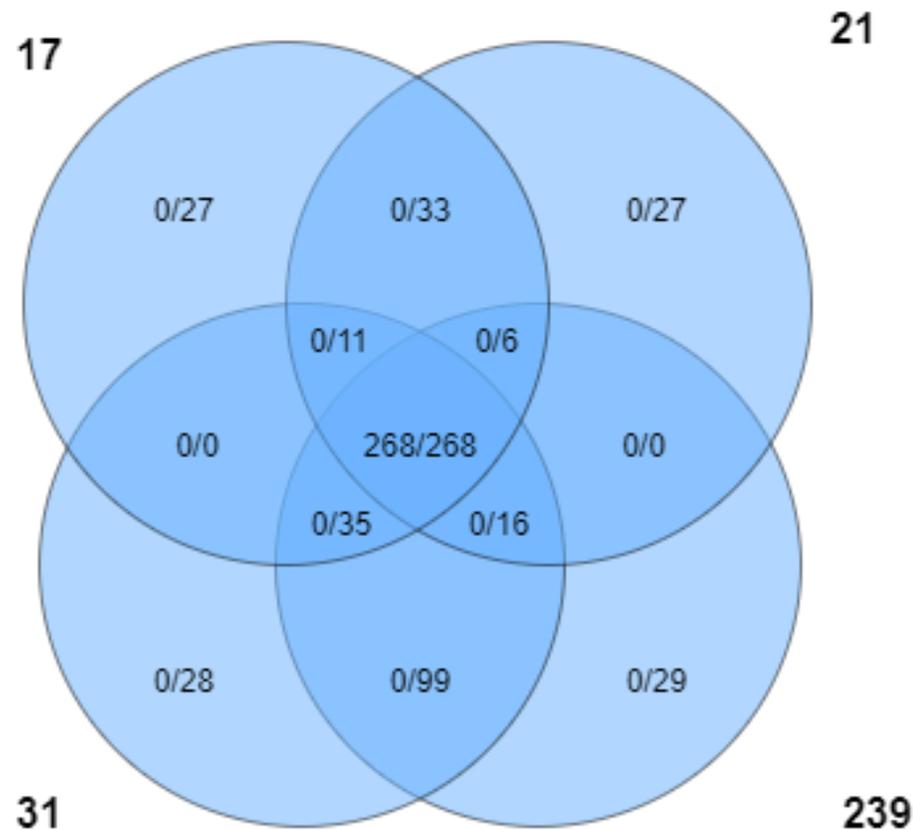
Риск-ориентированный подход и принцип минимальных прав

- **ИАФ.1** Идентификация и аутентификация пользователей и инициируемых ими процессов
- **ИАФ.2** Идентификация и аутентификация устройств
- **ИАФ.5** Идентификация и аутентификация внешних пользователей
- **ИАФ.6** Двусторонняя аутентификация
- **ИАФ.7** Защита аутентификационной информации при передаче
- **УПД.5** Назначение минимально необходимых прав и привилегий
- **УПД.13** Реализация защищенного удаленного доступа
- **УПД.14** Контроль доступа из внешних информационных (автоматизированных) систем
- **ЗИС.3** Эшелонированная защита информационной (автоматизированной) системы
- **ЗИС.4** Сегментирование информационной (автоматизированной) системы
- **ЗИС.6** Управление сетевыми потоками
- **ЗИС.19** Защита информации при ее передаче по каналам связи
- **ЗИС.20** Обеспечение доверенных канала, маршрута
- **ЗИС.27** Обеспечение подлинности сетевых соединений
- **АУД.2** Анализ уязвимостей и их устранение
- **АУД.5** Контроль и анализ сетевого трафика
- **АУД.9** Анализ действий отдельных пользователей
- **ОЦЛ.1** Контроль целостности программного обеспечения
- **ИНЦ** Реагирование на компьютерные инциденты
- **ДНС** Обеспечение действий в нештатных ситуациях

Нормативные документы ФСТЭК России

- Приказ ФСТЭК России №17 – 113 требований
- Приказ ФСТЭК России №21 – 107 требований
- Приказ ФСТЭК России №31 – 149 требований
- Приказ ФСТЭК России №239 – 145 требований

- 20-25% требований уникальны
- 75-80% требований повторяются хотя бы раз
- 46-64% требований одинаковы во всех приказах



Нормативные документы ФСТЭК России

Приказ ФСТЭК России №239

Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)
Управление доступом (УПД)
Ограничения программной среды (ОПС)
Защита машинных носителей информации (ЗНИ)
Аудит безопасности (АУД)
Антивирусная защита (АВЗ)
Предотвращение вторжений (компьютерных атак) (СОВ)
Обеспечение целостности (ОЦЛ)
Обеспечение доступности (ОДТ)
Защита технических средств и систем (ЗТС)
Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)
Реагирование на компьютерные инциденты (ИНЦ)
Управление конфигурацией (УКФ)
Управление обновлениями программного обеспечения (ОПО)
Планирование мероприятий по обеспечению безопасности (ПЛН)
Обеспечение действий в нештатных ситуациях (ДНС)
Информирование и обучение персонала (ИПО)

Приказ ФСТЭК России №21

Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)
Управление доступом субъектов доступа к объектам доступа (УПД)
Ограничения программной среды (ОПС)
Защита машинных носителей информации (ЗНИ)
Регистрация событий безопасности (РСБ)
Антивирусная защита (АВЗ)
Обнаружение вторжений (СОВ)
Контроль (анализ) защищенности персональных данных (АНЗ)
Обеспечение целостности информационной системы и персональных данных (ОЦЛ)
Обеспечение доступности персональных данных (ОДТ)
Защита среды виртуализации (ЗСВ)
Защита технических средств (ЗТС)
Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)
Выявление инцидентов и реагирование на них (ИНЦ)
Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)



Zero Trust на примере продуктов компании Код Безопасности

Сценарий 1.

Корпоративная сеть передачи данных

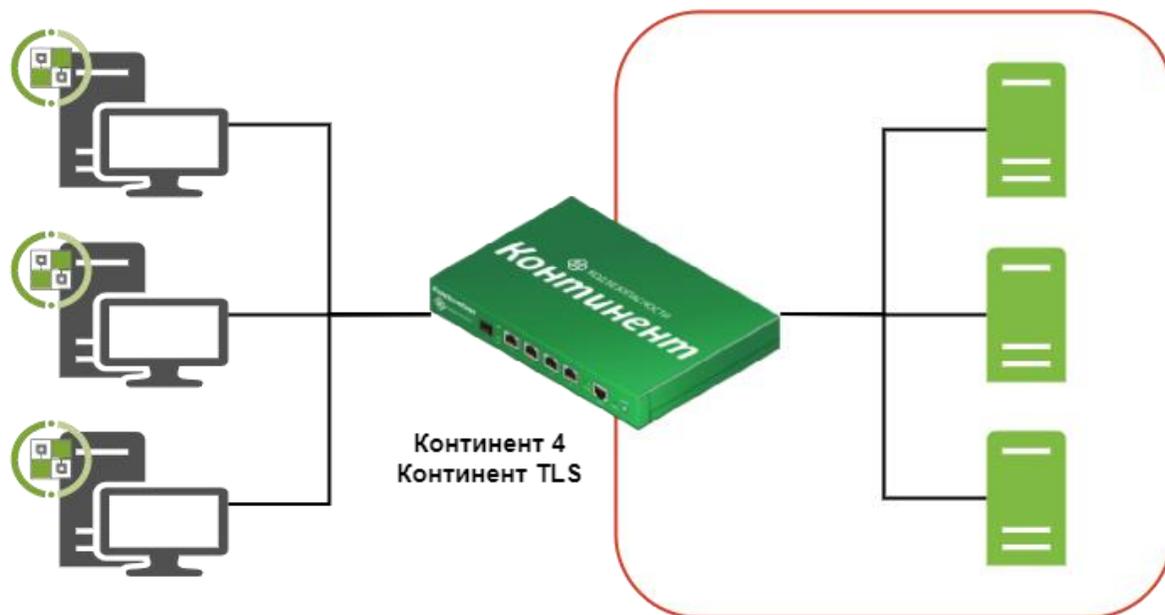
- Много удаленных пользователей
- Пункт принятия решений находится в центральном офисе
- Предпочитаема агентская архитектура или защищенный анклав



Решение

- Континент 4
- Континент TLS
- Континент ZTN-клиент
- Secret Net Studio

Защищенный анклав



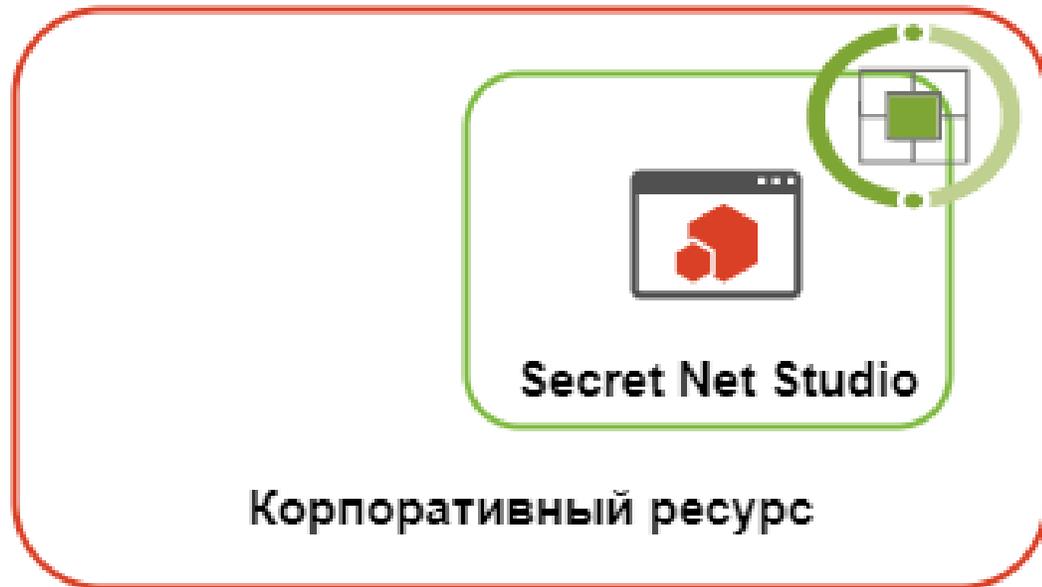
Континент 4 / Континент TLS

- Организация удаленного доступа
- Разграничение удаленного доступа на основе группы пользователя, данных сертификата

Континент ZTN-клиент

- Организация удаленного доступа
- Выполнение проверок соответствия рабочей станции пользователя требованиям по информационной безопасности

Агентская архитектура

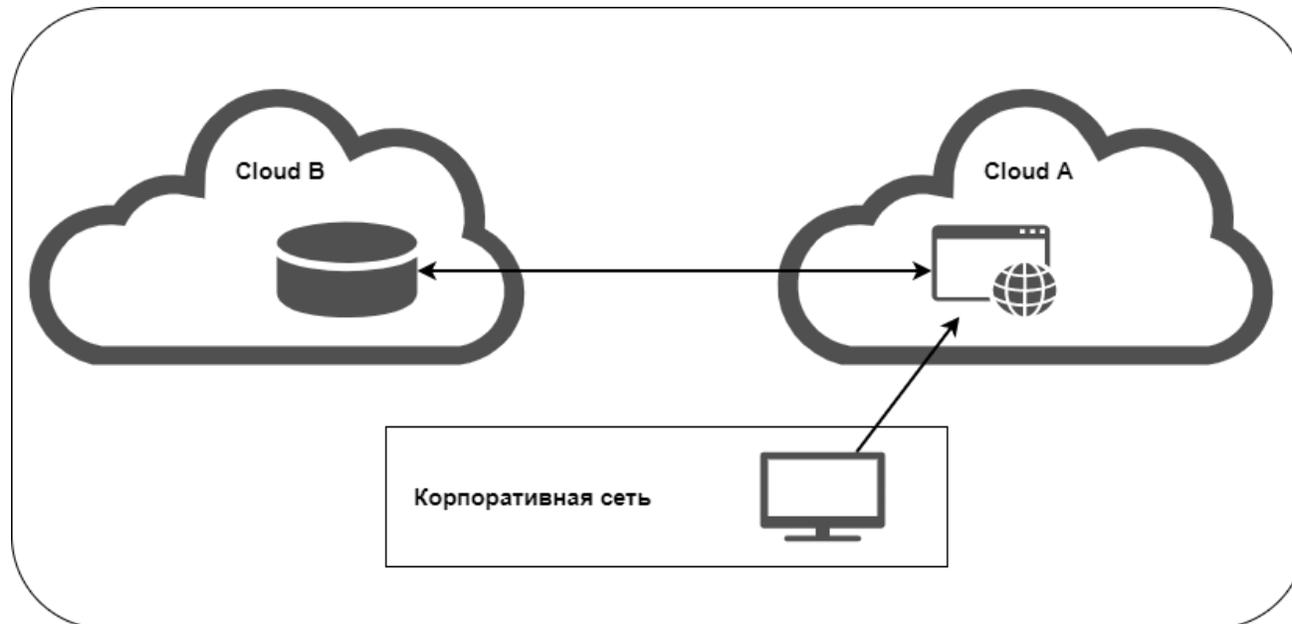


Secret Net Studio

- Разрешение определенным процессам ходить в сеть
- Доступ только для уполномоченных пользователей
- Реализация минимальных привилегий

Сценарий 2. Облачная/виртуальная архитектура

- Приложения распределены по нескольким облакам/гипервизорам
- Пункт принятия решений находится в одном из облаков/гипервизоров
- Для доступа пользователей используется ресурсный портал



Решение

- vGate

Ресурсный портал



vGate

- Микросегментация виртуальных машин
- Разграничение доступа к управлению инфраструктурой
- Безагентная защита трафика между виртуальными машинами
- Управление правами доступа к защищаемым ресурсам

Итоги

Объединение
комплаенса и лучших
практик по
информационной
безопасности

Организация
комплексной системы
защиты информации
(сеть, рабочие станции,
сервера, виртуальные
среды)

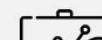
- NIST SP-800-207 -
<https://csrc.nist.gov/publications/detail/sp/800-207/final>
- Вебинар AntiMalware про ZTNA -
<https://www.youtube.com/watch?v=7mUutYXKPJQ>
- Телеком LinkMeUp про ZTA -
<https://www.youtube.com/watch?v=C4uD0cl24dU&t>
- Вебинар TS Solution & Код Безопасности
<https://youtu.be/gavyNcSEmMA>

TS SOLUTION

СИСТЕМНЫЙ ИНТЕГРАТОР

Успешно работаем на рынке IT с 2010 года. Обеспечиваем информационную безопасность бизнеса и оптимизируем процессы с помощью анализа машинных данных.

ИМПОРТОЗАМЕЩЕНИЕ И НИВЕЛИРОВАНИЕ САНКЦИОННЫХ РИСКОВ



TS Solution. Специализации

- Комплексные внедрения СЗИ

TS Solution. Специализации

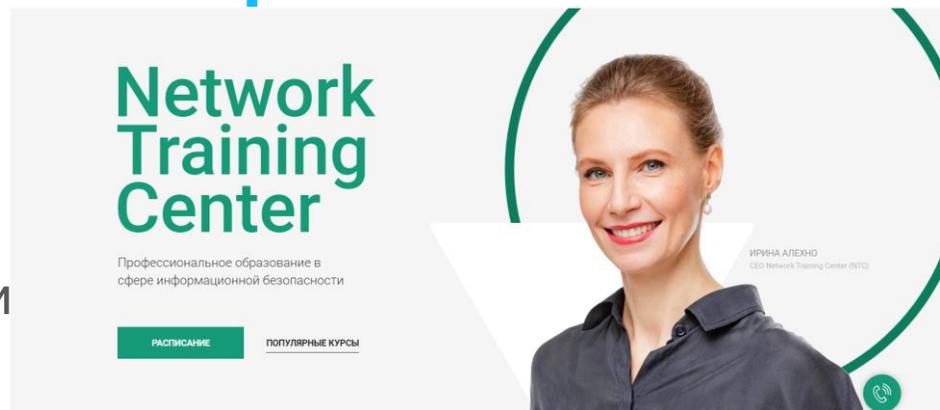
- Комплексные внедрения СЗИ
- Сопровождение проектов и оказание технической поддержки

The screenshot displays the CPSUPPORT website interface. At the top, the logo 'CPSUPPORT certified professional support' is on the left, and navigation links 'Вендоры', 'База знаний', 'Партнерам', 'О нас', and the phone number '8 800 555-86-91' are in the center. A red 'Вход в систему' button is on the right. The main banner features the text 'База знаний' (Knowledge Base) in large white font on a dark background. Below it, a smaller line of text reads: 'Не нашли ответа на свой вопрос? Задайте его нашим экспертам, и мы предоставим бесплатную консультацию.' (Didn't find an answer to your question? Ask it to our experts, and we will provide free consultation.) At the bottom of the banner are two buttons: 'ЗАДАТЬ ВОПРОС' (ASK A QUESTION) and 'БЕСПЛАТНЫЙ ТИКЕТ' (FREE TICKET). The background of the banner is a collage of various technical articles and guides, including titles like 'Check Point Getting Started R80.20', 'PT ANTI-APT', 'PT NETWORK ATTACK DISCOVERY', and 'UserGate Getting Started v6'.



TS Solution. Специализации

- Комплексные внедрения СЗИ
- Сопровождение проектов и оказани
- Обучение пользователей. Учебный центр NTC и University



УЧЕБНЫЕ КУРСЫ

Поиск

НАПРАВЛЕНИЕ

- ИБ
- ИТ
- Импортозамещение

ВЕНДОР

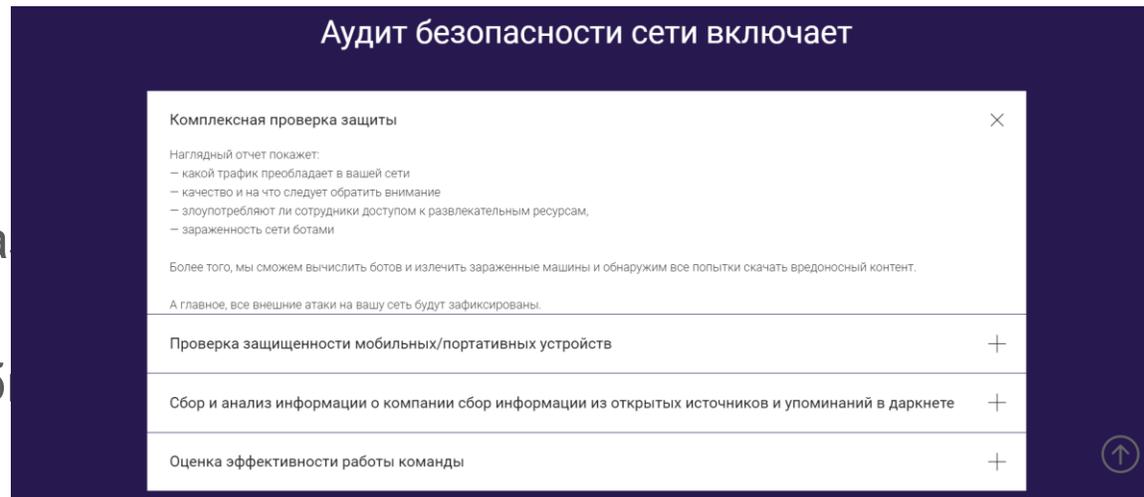
- Check Point
- Cisco
- Extreme Networks
- Flowmon
- Fortinet
- Fudo
- Linux
- TS Solution
- UserGate
- Yandex Cloud

# TS SOLUTION Основы виртуализации онлайн-курс	# USERGATE Site-to-site VPN UserGate v6 on-premise, Cloud Managed, Fortinet и pfSense видеоинструкция	# CHECK POINT Check Point Quantum Spark Getting Started онлайн-курс	# TS SOLUTION Создание и настройка UserGate в публичном облаке Yandex инструкция
# USERGATE UserGate Getting Started v6 онлайн-курс	# FORTINET Fortinet Security Fabric онлайн-курс	# TS SOLUTION Основы документирования СЕТЕЙ онлайн-курс	# FUDO Fudo Getting Started онлайн-курс
# TS SOLUTION User Security Awareness онлайн-курс	# КОД БЕЗОПАСНОСТИ Континент 4 Getting Started онлайн-курс	# CHECK POINT Remote Access Pack онлайн-курс	# CHECK POINT Remote Access VPN онлайн-курс



TS Solution. Специализации

- Комплексные внедрения СЗИ
- Сопровождение проектов и оказание услуг
- Обучение пользователей. Учебные курсы
- Проведение аудитов ИБ



СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

Обеспечим защиту, соответствующую
законодательству РФ



TS Solution. Специализации

ПОЧЕМУ МЫ?

ЛИЦЕНЗИИ ФСТЭК И ФСБ



Лицензия ФСТЭК на ТЗКИ, Лицензия ФСБ на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств

СЕРТИФИЦИРОВАННЫЕ ИНЖЕНЕРЫ



Команда сертифицированных специалистов имеет глубокую экспертизу в работе с различными классами решений в области информационной безопасности на всех этапах: от аудита до технического сопровождения

ОБУЧЕНИЕ ЗАКАЗЧИКОВ



Проводим обучение сотрудников наших клиентов для повышения эффективности использования средств защиты информации



- Построение комплексных систем ИБ

TS Solution. Специалисты



Остались вопросы?

Лебедев Дмитрий
Инженер отдела интеграций, TS Solution

dl@tssolution.ru

