КОД БЕЗОПАСНОСТИ

КОМПЛЕКСНЫЙ ПОДХОД В ЗАЩИТЕ ИНФОРМАЦИИ

Ставрополь 2019

КОД БЕЗОПАСНОСТИ

ФАКТЫ О КОМПАНИИ

Компания «Код Безопасности» - российский разработчик программных и аппаратных средств, обеспечивающих защиту информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

Более 20 лет на страже безопасности крупнейших предприятий России. Ведет свою деятельность на основании **9 лицензий ФСТЭК, ФСБ и Минобороны РФ.**

Технологии защиты обеспечивают безопасность **1 200 000 компьютеров** в **32 000 организаций.**
3 центра разработки: Москва, Санкт-Петербург, Пенза.

Более **400 квалифицированных специалистов R&D**, имеющих уникальные компетенции.

Более **50 разработанных СЗИ и СКЗИ.**

Более **60 действующих сертификатов (а всего более 250)** соответствия подтверждают высокое качество продуктов.

Партнерская сеть компании насчитывает **более 900 авторизованных партнеров.**

Компетентность «Кода Безопасности» в 2015-2016гг. подтверждена независимыми аналитиками:

- **«Крупнейшие производители высокотехнологичного оборудования»: №1** («Эксперт РА»), **№3** («Коммерсант»).
- **«Крупнейшие разработчики программного обеспечения»: №3** («Эксперт РА»), **№9** («Коммерсант»).
- **«Крупнейшие ИТ-компании России»: №30** («Коммерсант»), **№34** (TAdviser).

ФЗ-187 «КИИ»

Подписан Закон о безопасности критической информационной инфраструктуры России. Он регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Документ определяет основные понятия в этой сфере: «автоматизированная система управления», «безопасность критической информационной инфраструктуры», «значимый объект критической информационной инфраструктуры», «компьютерная атака», «компьютерный инцидент», «критическая информационная инфраструктура», «объекты критической информационной инфраструктуры» и «субъекты критической информационной инфраструктуры».

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 26 ИЮЛЯ 2017 Г. N 187-ФЗ "О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ"

ВЕРХНЕУРОВНЕВО

Определяются полномочия государственных органов РФ в области обеспечения ее безопасности, а также права и обязанности субъектов критической информационной инфраструктуры.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

КТО «ПОД УДАРОМ»

Объекты КИИ – информационные системы, сети, автоматизированные системы управления:

- Госорганов
- Предприятий оборонной промышленности
- Учреждений здравоохранения
- Научных организаций
- Транспортных организаций
- Телеком-операторов
- Организаций кредитно-финансовой сферы
- Предприятий энергетики
- Предприятий топливно-энергетического комплекса
- Предприятий Атомной промышленности
- Предприятий Ракетно-космической промышленности
- Предприятий Горнодобывающей промышленности
- Предприятий Металлургической промышленности
- Предприятий Химической промышленности.
- Организации, которые осуществляют взаимодействие указанных выше систем и сетей

ОБЯЗАННОСТИ

Субьекты КИИ **должны**:

- ✓ Категорировать объекты КИИ которыми они владеют
  - Занизить уровень категорирования нельзя, у ФСТЭК есть право перекатегорирования
- ✓ Создать выделенную службы ИБ КИИ
- ✓ Подключиться к ГосСОПКА согласно требованиям ФСБ
- ✓ Создать систему защиты КИИ согласно требованиям ФСТЭК
- ✓ Регулярно проходить проверки регуляторов
- ✓ Своевременно сообщать об инцидентах ИБ в своей ИТ-инфраструктуре

КРИТЕРИИ ОТНЕСЕНИЯ К КИИ

- Ущерб здоровью людей и окружающей сред
- Нарушение функционирования ГИС
- Нарушение функционирование объектов жизнедеятельности, транспорта, связи
- Причинение значительного ущерба гос.предприятиям или бюджету
- Нарушение функционирования или подмена сайта госоргана
- Нарушение проведения финансовых транзакций
- Отсутствие доступа к госуслугам

О БОЛЬНОМ…

- При наличии АСУ ТП в качестве объекта КИИ, многие организации столкнутся с рядом трудностей.
- Будет два выхода из сложившихся реалий.
- Попробовать выполнить все требования регуляторов в своём промышленном сегменте (при неполном перечне готовых решений по ИБ для этого сегмента).
- Минимизировать расходы на производственный сегмент за счёт сегментации участка АСУ ТП как локальной подсистемы.

ТРЕБОВАНИЯ ФСТЭК

Направление	Endpoint	Network	Virtualization
Идентификация и аутентификация (ИАФ)	+	+	+
Управление доступом (УПД)	+	+	+
Ограничение программной среды (ОПС)	+		+
Защита машинных носителей информации (ЗНИ)	+		
Аудит безопасности (АУД)	+	+	+
Антивирусная защита (АВЗ)	+		
Предотвращение вторжений (компьютерных атак) (СОВ)	+	+	
Обеспечение целостности (ОЦЛ)	+	+	+
Обеспечение доступности информации (ОДТ)	+	+	+
Защита технических средств и систем (ЗТС)	Организационные меры		
Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	+ (+Терминал, MDM)	+	+
Реагирование на инциденты информационной безопасности (ИНЦ)	+	+	+
Управление конфигурацией (УКФ)	+		+
Управление обновлениями программного обеспечения (ОПО)	+		+
Планирование мероприятий по обеспечению безопасности (ПЛН)	Организационные меры		
Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)	+	+	+
Информирование и обучение персонала (ИПО)	Организационные меры		

ТРЕБОВАНИЯ ФСБ

Направление	Продукт
Обнаружение компьютерных атак	SIEM
Предупреждение компьютерных атак	Сканер уязвимостей
Ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты	исходя из требований – управление инцидентами на основе SIEM
Поиск признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ	СОВ/СОА
Криптографическая защита обмена информацией необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак	СКЗИ

СКЗИ
строго сертифицированные

Отсутствие НДВ в ПО

Средства защиты должны быть РОССИЙСКИМИ

СРЕДСТВА ЗАЩИТЫ ПО ФСТЭК

Что потребуется для защиты	Что мы можем предложить
СЗИ от НСД	Secret Net Studio (АРМ), vGate (виртуализация), Secret MDM (мобильные устройства)
Межсетевой экран	АПКШ «Континент» (сеть), Secret Net Studio (АРМ)
Средство обнаружения вторжений	АПКШ «Континент» (сеть), Secret Net Studio (АРМ)
Средства антивирусной защиты	Secret Net Studio
Средства контроля защищенности	---
Средства управления событиями безопасности	---
Средства защиты каналов передачи данных	АПКШ «Континент»

СРЕДСТВА ЗАЩИТЫ ПО ФСБ

Что потребуется для защиты	Что мы можем предложить
SIEM	-
Сканеры уязвимостей	-
Средство обнаружения вторжений	АПКШ «Континент» (СОВ)
Средства обнаружения атак	АПКШ «Континент» (СОА)
Средства криптографической защиты информации	АПКШ «Континент»

КОНКРЕТИКА

3 категория	2 категория	1 категория
Антивирус	Антивирус	Антивирус
СЗИ от НСД для АРМ и серверов	СЗИ от НСД для АРМ и серверов	СЗИ от НСД для АРМ и серверов
СЗИ от НСД для виртуальной инфраструктуры	СЗИ от НСД для виртуальной инфраструктуры	СЗИ от НСД для виртуальной инфраструктуры
Сканер уязвимостей	Сканер уязвимостей	Сканер уязвимостей
Система сбора и анализа событий безопасности	Система сбора и анализа событий безопасности	Система сбора и анализа событий безопасности
Система контроля подключенных USB-устройств	Система контроля подключенных USB-устройств	Система контроля подключенных USB-устройств
Межсетевой экран (сетевой, хостовый)	Межсетевой экран (сетевой, хостовый)	Межсетевой экран (сетевой, хостовый)
Система защиты информации на мобильных устройствах	Система защиты информации на мобильных устройствах	Система защиты информации на мобильных устройствах
Система управления обновлениями ПО	Система управления обновлениями ПО	Система управления обновлениями ПО
Система защищенного удаленного доступа	Система защищенного удаленного доступа	Система защищенного удаленного доступа
Система резервного копирования	Система резервного копирования	Система резервного копирования
Защита от DoS и DDoS-атак	Защита от DoS и DDoS-атак	Защита от DoS и DDoS-атак
	Система обнаружения вторжений	Система обнаружения вторжений
	Модуль доверенной загрузки	Модуль доверенной загрузки
	Анти-спам	Анти-спам

КОНКРЕТИКА ПО КБ

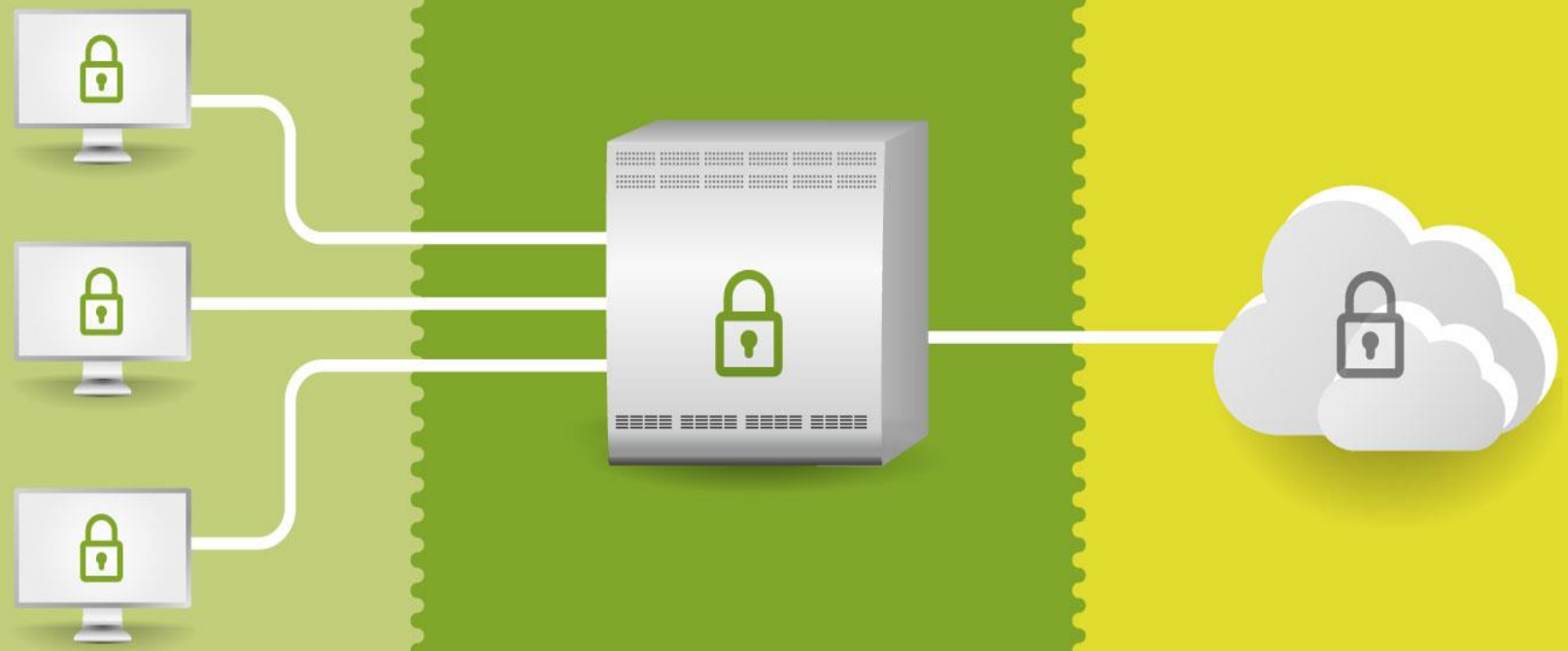
3 категория	2 категория	1 категория
Антивирус	Антивирус	Антивирус
СЗИ от НСД для АРМ и серверов	СЗИ от НСД для АРМ и серверов	СЗИ от НСД для АРМ и серверов
СЗИ от НСД для виртуальной инфраструктуры	СЗИ от НСД для виртуальной инфраструктуры	СЗИ от НСД для виртуальной инфраструктуры
Сканер уязвимостей	Сканер уязвимостей	Сканер уязвимостей
Система сбора и анализа событий безопасности	Система сбора и анализа событий безопасности	Система сбора и анализа событий безопасности
Система контроля подключенных USB-устройств	Система контроля подключенных USB-устройств	Система контроля подключенных USB-устройств
Межсетевой экран (сетевой, хостовый)	Межсетевой экран (сетевой, хостовый)	Межсетевой экран (сетевой, хостовый)
Система защиты информации на мобильных устройствах	Система защиты информации на мобильных устройствах	Система защиты информации на мобильных устройствах
Система управления обновлениями ПО	Система управления обновлениями ПО	Система управления обновлениями ПО
Система защищенного удаленного доступа	Система защищенного удаленного доступа	Система защищенного удаленного доступа
Система резервного копирования	Система резервного копирования	Система резервного копирования
Защита от DoS и DDoS-атак	Защита от DoS и DDoS-атак	Защита от DoS и DDoS-атак
	Система обнаружения вторжений	Система обнаружения вторжений
	Модуль доверенной загрузки	Модуль доверенной загрузки
	Анти-спам	Анти-спам

СОВСЕМ КОНКРЕТНО

3 категория	2 категория	1 категория
SECRET NET STUDIO (СЗИ от НСД, Контроль устройств) АПКШ Континент (СКЗИ, МЭ) vGate (СЗИ ВИ) + Антивирус SIEM Сканер уязвимостей Резервное копирование	SECRET NET STUDIO (СЗИ от НСД, Контроль устройств) АПКШ Континент (СКЗИ, МЭ, СОВ) vGate (СЗИ ВИ) ПАК СОБОЛЬ (АПМДЗ) + Антивирус SIEM Сканер уязвимостей Резервное копирование	SECRET NET STUDIO (СЗИ от НСД, Контроль устройств) АПКШ Континент (СКЗИ, МЭ, СОВ) vGate (СЗИ ВИ) ПАК СОБОЛЬ (АПМДЗ) + Антивирус SIEM Сканер уязвимостей Резервное копирование

КОД БЕЗОПАСНОСТИ

КОМПЛЕКСНЫЕ РЕШЕНИЯ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

ЗАЩИТА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

ЗАЩИТА ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

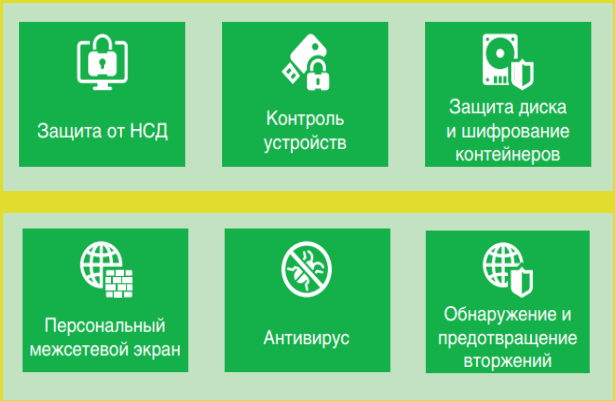
ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

SECRET NET STUDIO

Комплексное решение для обеспечения безопасности рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования



Сертификаты

Продукт сертифицирован на соответствие требованиям ФСТЭК России к защите конфиденциальной информации и государственной тайны.
Применяется для защиты АС до класса 1Б включительно (гостайна с грифом «совершенно секретно»), ИСПДн до УЗ1, ГИС до К1 и АСУ ТП до К1 включительно. СВТ-3, СОВ-4, САВЗ-4, СКСН-4.

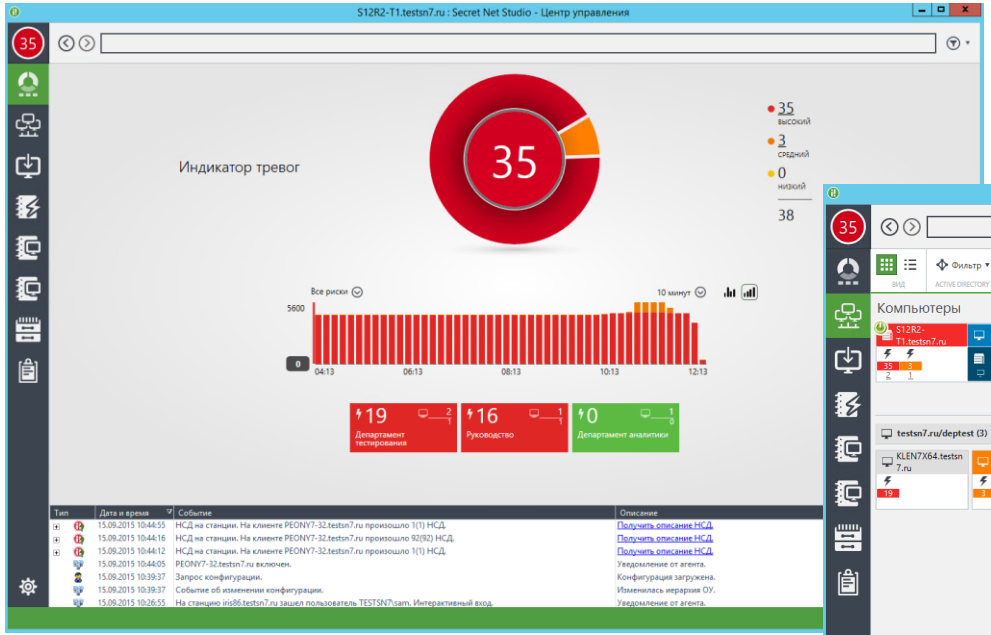
КОД БЕЗОПАСНОСТИ

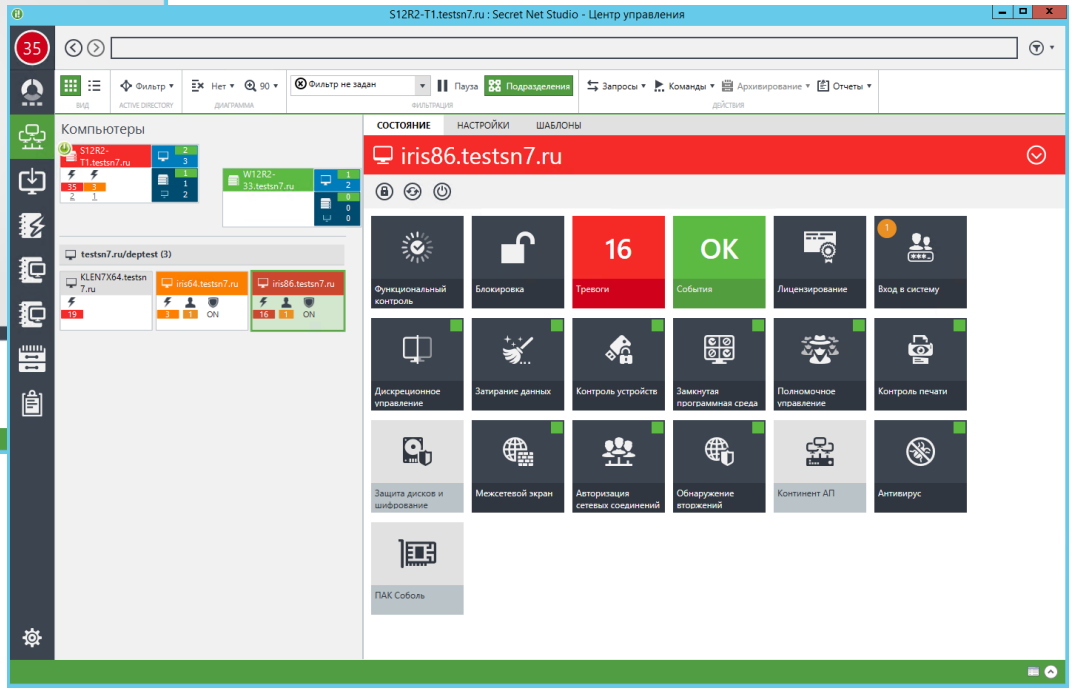
ЗАЩИТНЫЕ МЕХАНИЗМЫ

- Шифрование данных
- Теневое копирование
- Маркировка документов
- Замкнутая программная среда
- Межсетевой экран
- Авторизация сетевых соединений
- Защита от вторжений
- «Континент-АП» (VPN-клиент)
- Усиленный вход в систему
- Контроль целостности
- Антивирус
- Дискреционное управление доступом
- Мандатное управление доступом
- Затирание данных
- Контроль устройств
- Контроль печати
- Интеграция с ПАК «Соболь»

КОД БЕЗОПАСНОСТИ

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ





КОД БЕЗОПАСНОСТИ

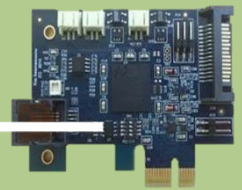
ПОДДЕРЖИВАЕМЫЕ ОС

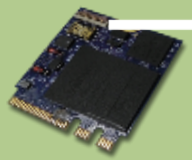
Secret Net LSP 1.6.253	Secret Net LSP 1.7
• МСВС 5.0 (версия ядра 2.6.32); • ALT Linux 7.0.5 Centaurus (версия ядра 3.14.41-std-def-alt1); • Astra Linux Special Edition 1.5 (версия ядра 4.2.0); • Astra Linux Special Edition 1.4 (версия ядра 3.16.0); • CentOS 7.2 (версия ядра 3.10.0-327.el7.x86_64); • CentOS 7.1 (версия ядра 3.10.0-229.el7.x86_64); • CentOS 6.5 (версия ядра 2.6.32-431.el6.x86_64/2.6.32-431.el6.i686); • Debian 8.0 (версия ядра 3.16.0-4-amd64); • Debian 7.6 (версия ядра 3.2.0-4-686-pae/3.2.0-4-amd64); • Red Hat Enterprise Linux 7.2 (версия ядра 3.10.0-327.el7.x86_64); • Red Hat Enterprise Linux 7.0 (версия ядра 3.10.0-123.el7.x86_64); • Red Hat Enterprise Linux 6.5 (версия ядра 2.6.32-431.el6.x86_64/2.6.32-431.el6.i686); • ROSA Enterprise Linux Server 6.5 (версия ядра 2.6.32-431.el6.x86_64)	• МСВС 5.0 (версия ядра 2.6.32); • Astra Linux Special Edition 1.5 (версия ядра 4.2.0); • Astra Linux Special Edition 1.4 (версия ядра 3.16.0); • CentOS 7.3 (версии ядра 3.10.0-514.el7.x86_64 и 3.10.0-693.11.6.el7.x86_64); • CentOS 7.2 (версия ядра 3.10.0-327.el7.x86_64); • CentOS 7.1 (версия ядра 3.10.0-229.el7.x86_64); • CentOS 6.5 (версии ядра 2.6.32- 431.el6.x86_ 64/2.6.32- 431.el6.i686 и 2.6.32-696.18.7.el6.x86_64); • ContinentOS 4.2 (версии ядра 4.4.32/4.4.84 и 4.9.76-1.terminal1.x86_64); • Debian 8.0 (версии ядра 3.16.0-4-amd64 и 3.16.51-3+deb8u1); • Debian 7.6 (версии ядра 3.2.0-4-686-pae/3.2.0-4-amd64 и 3.2.96-3-amd64); • Red Hat Enterprise Linux 7.3 (версия ядра 3.10.0-514.el7.x86_64); • Red Hat Enterprise Linux 7.2 (версия ядра 3.10.0-327.el7.x86_64); • Red Hat Enterprise Linux 7.0 (версия ядра 3.10.0-123.el7.x86_64); • Red Hat Enterprise Linux 6.5 (версия ядра 2.6.32-431.el6.x86_64/2.6.32-431.el6.i686); • Oracle Linux 7.2 (версия ядра 3.10.0-327.el7.x86_64); • Oracle Linux 7.3 (версия ядра 3.10.0-514.el7.x86_64)

КОД БЕЗОПАСНОСТИ

НОВОЕ ПОКОЛЕНИЕ «СОБОЛЕЙ»

- Новая версия прошивки 4.0 с поддержкой новых моделей ПК и последних требований контролирующих органов.
- Новая плата в форм-факторе M.2 для ноутбуков, моноблоков и мини ПК. Поддержка идентификаторов JaCarta
- Функционирование в среде UEFI.
- Поддержка разметки дисков GPT и MBR
- Новая плата формата PCI-Express компактного размера, для установки в мини-корпусах.
- Наличие графического интерфейса, поддерживающего работу с мышью. Переработан процесс инициализации и обновления (без вскрытия корпуса)



КОД БЕЗОПАСНОСТИ

ЗАЩИЩЁННЫЙ ТЕРМИНАЛЬНЫЙ КЛИЕНТ

- Собственная ОС на базе Linux - «Continent OS».
- Доверенная загрузка.
- Защита от НСД и контроль подключения устройств.
- Криптографическая защита канала подключения.
- Централизованное управление и мониторинг.

SECRET MDM
Управление корпоративной мобильностью и защита данных на мобильных устройствах

Предназначен для решения следующих задач:

- Комплексное управление корпоративной мобильностью
- Защита данных на мобильных устройствах
- Защита передаваемых сообщений и телефонии
- Организация защищенного доступа с мобильных устройств к корпоративным службам

Возможности продукта:

- Управление политиками блокировки, длиной и сложностью пароля
- Дистанционная блокировка и затирание данных (wipe при потере или краже устройства)
- Разрешения на использование встроенного
- микрофона, видеокамеры,
- Bluetooth, NFC
- Дистанционная установка и удаление приложений
- Запуск только разрешенных приложений
- Дистанционное распространение настроек для подключения к сервисам Exchange, WiFi точкам доступа
- Обнаружение действий злоумышленника при получении jailbreak и root доступа

ЗАЩИТА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

ПРОДУКТЫ

ЗАЩИТА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

АПКШ «КОНТИНЕНТ»

Многофункциональный комплекс безопасности для всесторонней защиты сетевого периметра организации

«КОНТИНЕНТ TLS VPN»

Сертифицированное решение для обеспечения защищенного доступа удаленных пользователей к корпоративным ресурсам

СОВ «КОНТИНЕНТ» 4.0

Система обнаружения и предотвращения вторжений (IDS/IPS) нового поколения «Континент» 4.0

КОД БЕЗОПАСНОСТИ

СЕРТИФИКАТЫ

АПКШ «КОНТИНЕНТ» 3.7

ФСТЭК России

- 2 класс по РД МЭ
- 3 класс сетевой СОВ (ИТ.СОВ.СЗПЗ)
- 2 уровень контроля отсутствия НДВ

ФСБ России

- 4 класс по РД МЭ
- СКЗИ КС1/КС2/КС3
- СОА В

Продукт сертифицирован для защиты

- автоматизированных систем (АС) до класса защищенности 1Б включительно
- государственных информационных систем (ГИС) до К1 включительно
- информационных систем персональных данных (ИСПДн) до УЗ1 включительно

Экспортный вариант АПКШ Континент 3.7

КОД БЕЗОПАСНОСТИ

АРХИТЕКТУРА АПКШ «КОНТИНЕНТ»

КРИПТОШЛЮЗ

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче на сетевом уровне (создании L3 VPN-сети).

ДЕТЕКТОР АТАК

Аппаратно-программный комплекс, предназначенный для анализа сетевого трафика и обнаружения в нем угроз безопасности.

КРИПТОКОММУТАТОР

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче на канальном уровне (создании L2 VPN-сети).

ЦЕНТР УПРАВЛЕНИЯ СЕТЬЮ

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов АПКШ «Континент».

СКЗИ «КОНТИНЕНТ-АП»

VPN-клиент для персональных компьютеров, выполняющий функции персонального межсетевого экрана.

СЕРВЕР ДОСТУПА

Аппаратно-программный комплекс, предназначенный для организации защищенного удаленного доступа с помощью VPN-клиента СКЗИ «Континент АП».

СКЗИ «КОНТИНЕНТ-АП»

VPN-клиент для подключения мобильных устройств на базе Android и iOS к Серверу доступа .

КОД БЕЗОПАСНОСТИ

ЧТО МЫ СДЕЛАЛИ В КОНТИНЕНТ 3.9

Переход на архитектуру x86_64 FreeBSD

Увеличение производительности МЭ и VPN

Расширенные опции DHCP сервера

Обновление линейки платформ

Групповые операции над узлами

Новый интерфейс ПУ

Отладочный журнал узла

Резервирование БД ЦУС

Плавная смена ключей парной связи

Агрегация интерфейсов

Оптимизация ПО и исправление багов

Изменение методики измерения производительности

КОД БЕЗОПАСНОСТИ

НОВЫЕ ПЛАТФОРМЫ

IPC-10

Производительность
МЭ до 400 Мбит/с
VPN до 100 Мбит/с

Сетевые интерфейсы:
3x Ethernet 10/100/1000

IPC-50

Производительность
МЭ до 940 Мбит/с
VPN до 300 Мбит/с

Сетевые интерфейсы:
4x Ethernet 10/100/1000
1x Gigabit Ethernet SFP

IPC-500F

Производительность
МЭ до 2100 Мбит/с
VPN до 500 Мбит/с

Сетевые интерфейсы:
8x Ethernet 10/100/1000
2x Gigabit Ethernet SFP

IPC-600

Производительность
МЭ до 5000 Мбит/с
VPN до 1100 Мбит/с

Сетевые интерфейсы:
8x Ethernet 10/100/1000

IPC-800F

Производительность
МЭ до 7000 Мбит/с
VPN до 2300 Мбит/с

Сетевые интерфейсы:
8x Ethernet 10/100/1000
4x Gigabit Ethernet SFP

IPC-1000F

Производительность
МЭ до 10000 Мбит/с
VPN до 4400 Мбит/с

Сетевые интерфейсы:
8x Ethernet 10/100/1000
8x Gigabit Ethernet SFP

IPC-3000F

Производительность
МЭ до 13000 Мбит/с
VPN до 6400 Мбит/с

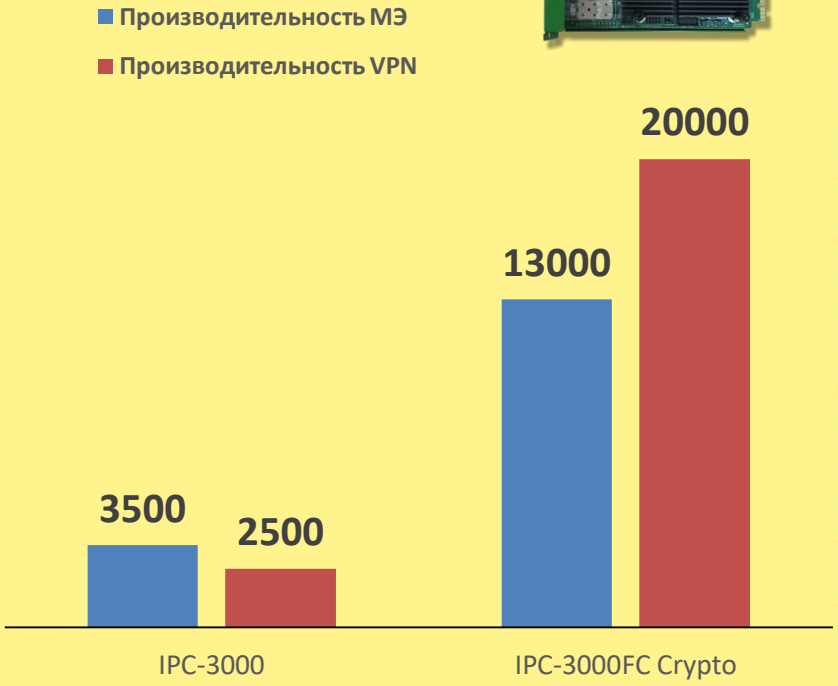
Сетевые интерфейсы:
1x Ethernet 10/100/1000
8x Gigabit Ethernet SFP
4x 10 Gigabit Ethernet Fiber SFP+

КОД БЕЗОПАСНОСТИ

АППАРАТНОЕ ШИФРОВАНИЕ. IPC-3000FC+КРИПТОУСКОРИТЕЛЬ

Сравнение производительности

+



Производительность

МЭ до 13000 Мбит/с

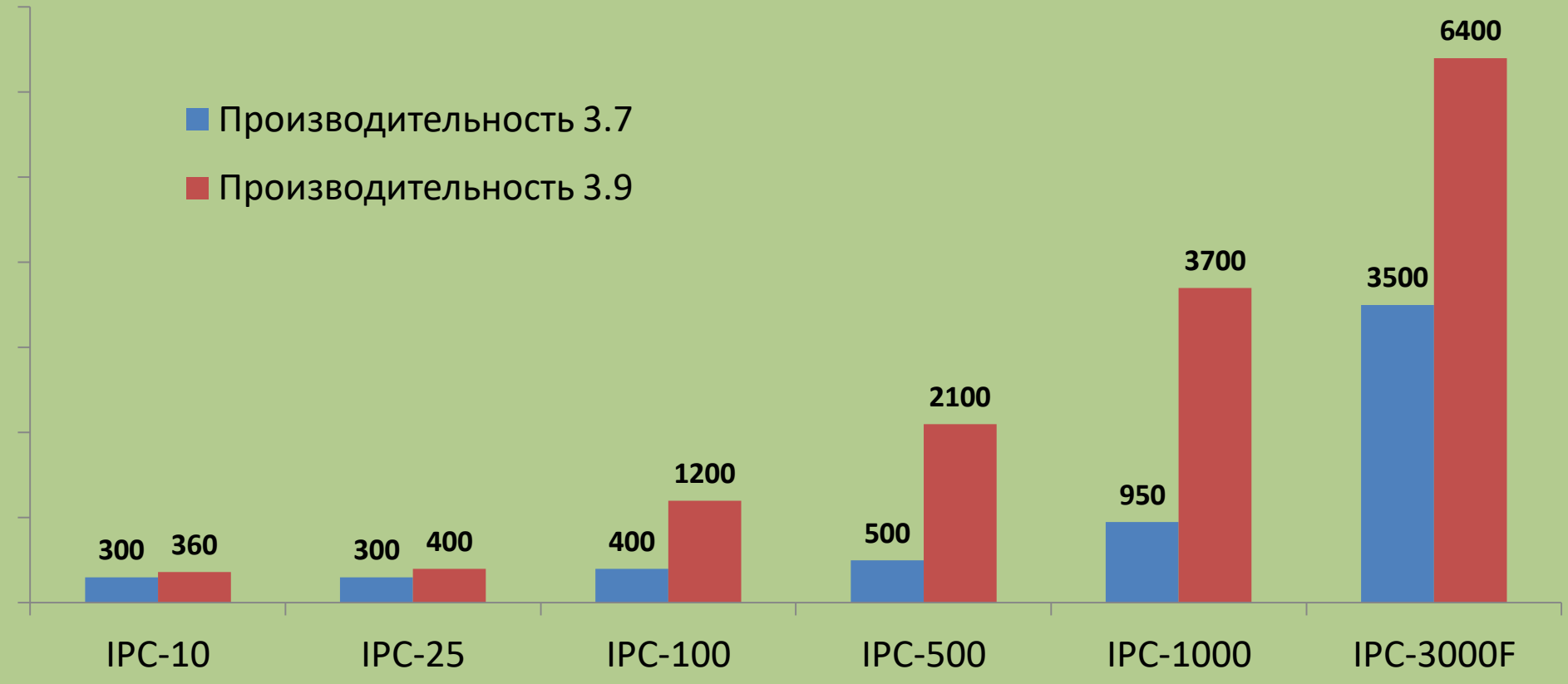
VPN до 20000 Мбит/с

Сетевые интерфейсы:

- 2x Ethernet 10/100/1000
- 8x Gigabit Ethernet SFP
- 4x 10 Gigabit Ethernet Fiber SFP+
- 4x 10 Gigabit Ethernet Fiber SFP+ на **Криптоускорителе**

КОД БЕЗОПАСНОСТИ

НОВЫЕ ПЛАТФОРМЫ. ПРОИЗВОДИТЕЛЬНОСТЬ МЭ



КОД БЕЗОПАСНОСТИ

РЕЗУЛЬТАТЫ КОНТИНЕНТ 3.7

- **На 350% выросли** продажи «Континента» за последние три года
- **Более 20 000** устройств продано с 2013 года
- **Каждая транзакция** по пластиковым картам в России защищена с помощью «Континента»
- Государственная автоматизированная система **«Выборы»** защищена с помощью «Континента»
- **Чемпионат мира по футболу 2018**

СОВ Континент 4.0

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

АРХИТЕКТУРА СОВ «КОНТИНЕНТ»

ЦЕНТР УПРАВЛЕНИЯ СЕТЬЮ
Аппаратно-программный комплекс,
для управления и мониторинга
всех компонентов системы защиты

ДЕТЕКТОР АТАК
Аппаратно-программный комплекс,
предназначенный для анализа сетевого трафика,
обнаружения и предотвращения вторжений

БАЛАНСИРОВЩИК НАГРУЗКИ
Аппаратно-программный комплекс, предназначенный
для распределения сетевого трафика между узлами
фермы, состоящей из Детекторов атак

ВАРИАНТЫ ПРИМЕНЕНИЯ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

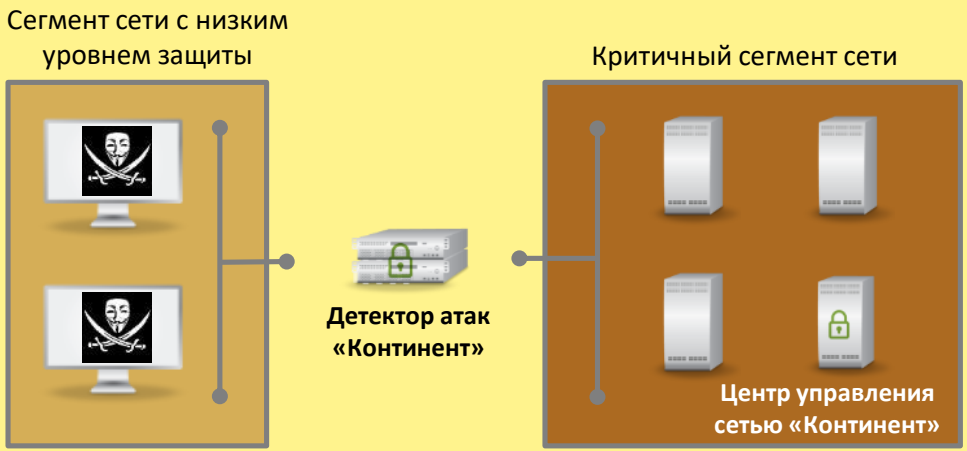
ЗАЩИТА КРИТИЧНЫХ СЕГМЕНТОВ СЕТИ

Задачи:

- Автоматическое предотвращение атаки на критичные ресурсы

Компоненты:

- Центр управления сетью «Континент»
- Детектор атак «Континент»



КОД БЕЗОПАСНОСТИ

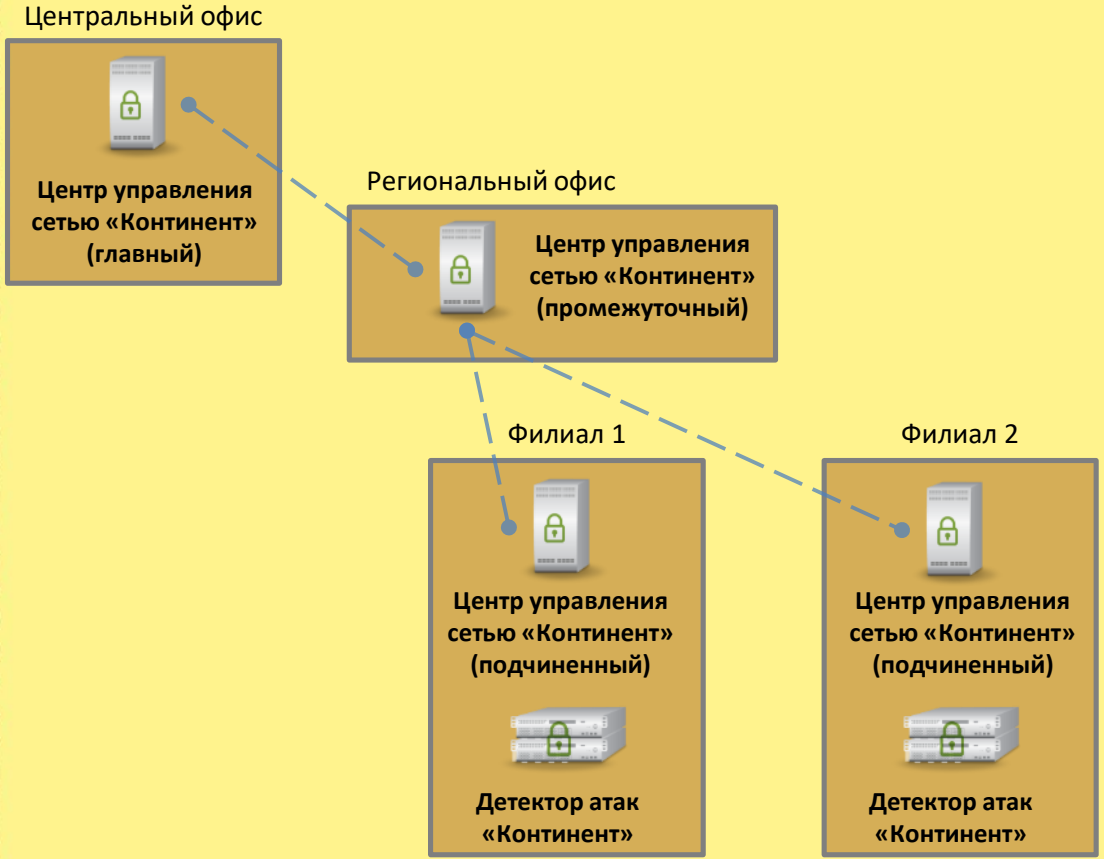
ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ В РАСПРЕДЕЛЕННЫХ СЕТЯХ

Задачи:

- Обнаружение вторжений
- Выполнение глобальной политики безопасности
  - Сквозная система мониторинга и управления
  - Выделение ограниченных прав администраторам «на местах»

Компоненты:

- Центр управления сетью «Континент»
- Детектор атак «Континент»



КОД БЕЗОПАСНОСТИ

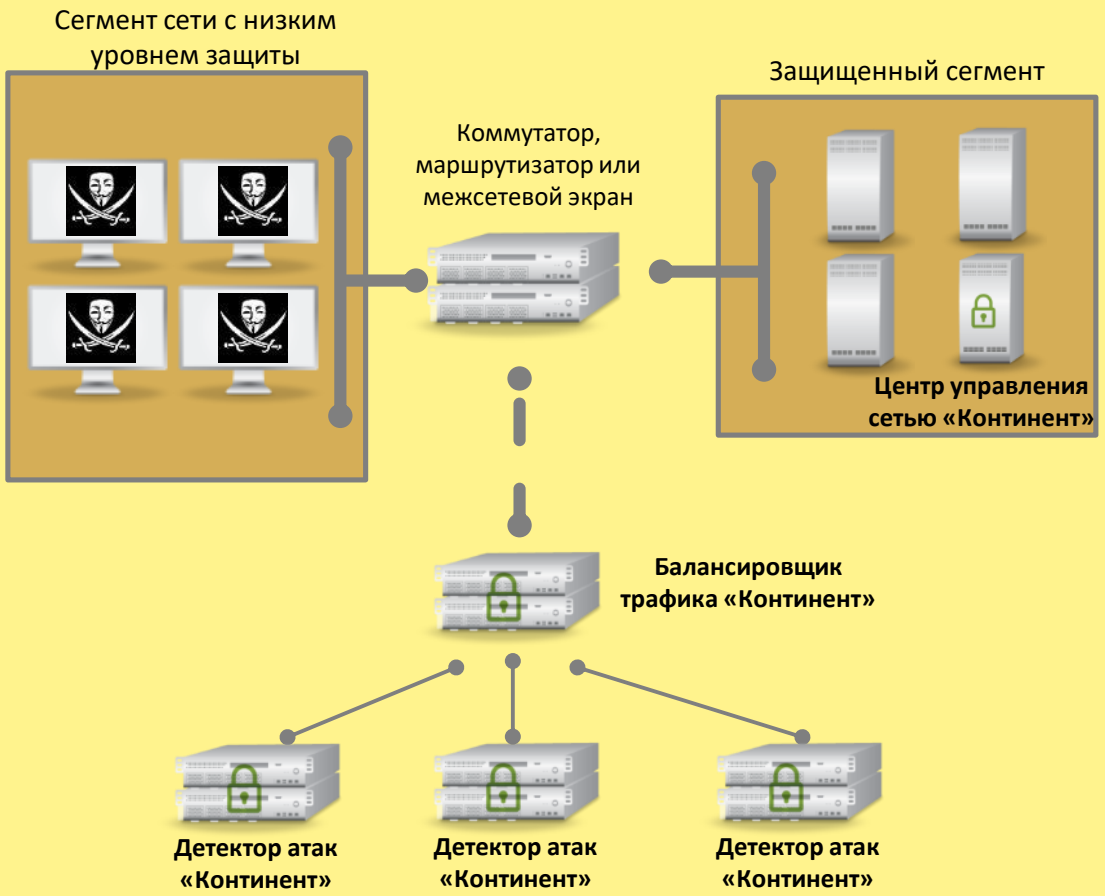
ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ В ВЫСОКОНАГРУЖЕННЫХ СЕТЯХ

Задачи:

- Защита сети с высокой пропускной способностью (до 10 Гбит/с)
- Обеспечение отказоустойчивости сетевых сенсоров

Компоненты:

- Центр управления сетью «Континент»
- Детектор атак «Континент»
- Балансировщик трафика «Континент»



КОМПОНЕНТЫ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

УПРАВЛЕНИЕ ИНФРАСТРУКТУРОЙ СОВ «КОНТИНЕНТ»

ЦЕНТР УПРАВЛЕНИЯ СЕТЬЮ «КОНТИНЕНТ»

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов СОВ «Континент»

Мониторинг событий в реальном времени

Дистанционное обновление компонентов комплекса

Автоматическое обновление базы решающих правил с серверов «Кода Безопасности»

Гибкая система отчетов

Экспорт событий

- **Экспорт в SIEM**

КОД БЕЗОПАСНОСТИ

УПРАВЛЕНИЕ ИНФРАСТРУКТУРОЙ СОВ «КОНТИНЕНТ»

ЦЕНТР УПРАВЛЕНИЯ СЕТЬЮ «КОНТИНЕНТ»

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов СОВ «Континент»

Система иерархического управления большой инфраструктурой

- **Делегирование прав в рамках глобальной политики безопасности**
- **Сквозной мониторинг всей инфраструктуры СОВ «Континент» 4.0**
- **Три уровня иерархии**

Взаимная аутентификация главного и подчиненных ЦУС с помощью сертификатов

Возможность управления большим количеством узлов безопасности

КОД БЕЗОПАСНОСТИ

УПРАВЛЕНИЕ ИНФРАСТРУКТУРОЙ СОВ «КОНТИНЕНТ»

ЦЕНТР УПРАВЛЕНИЯ СЕТЬЮ «КОНТИНЕНТ»

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов СОВ «Континент»

Новые консоли управления и мониторинга

Высокопроизводительная система хранения и обработки событий безопасности

Ролевая модель доступа администраторов

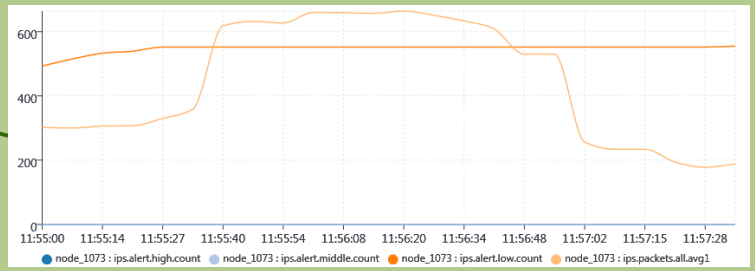
КОД БЕЗОПАСНОСТИ

ПАНЕЛЬ МОНИТОРИНГА СОВ «КОНТИНЕНТ»

Состояние центра управления сетью и детекторов атак

Мониторинг	0	1	0	Аудит	11	1	СОВ	5	2	15

Распределение событий детекторов атак в реальном времени



Сводная информация по состоянию всей инфраструктуры СОВ

Группы

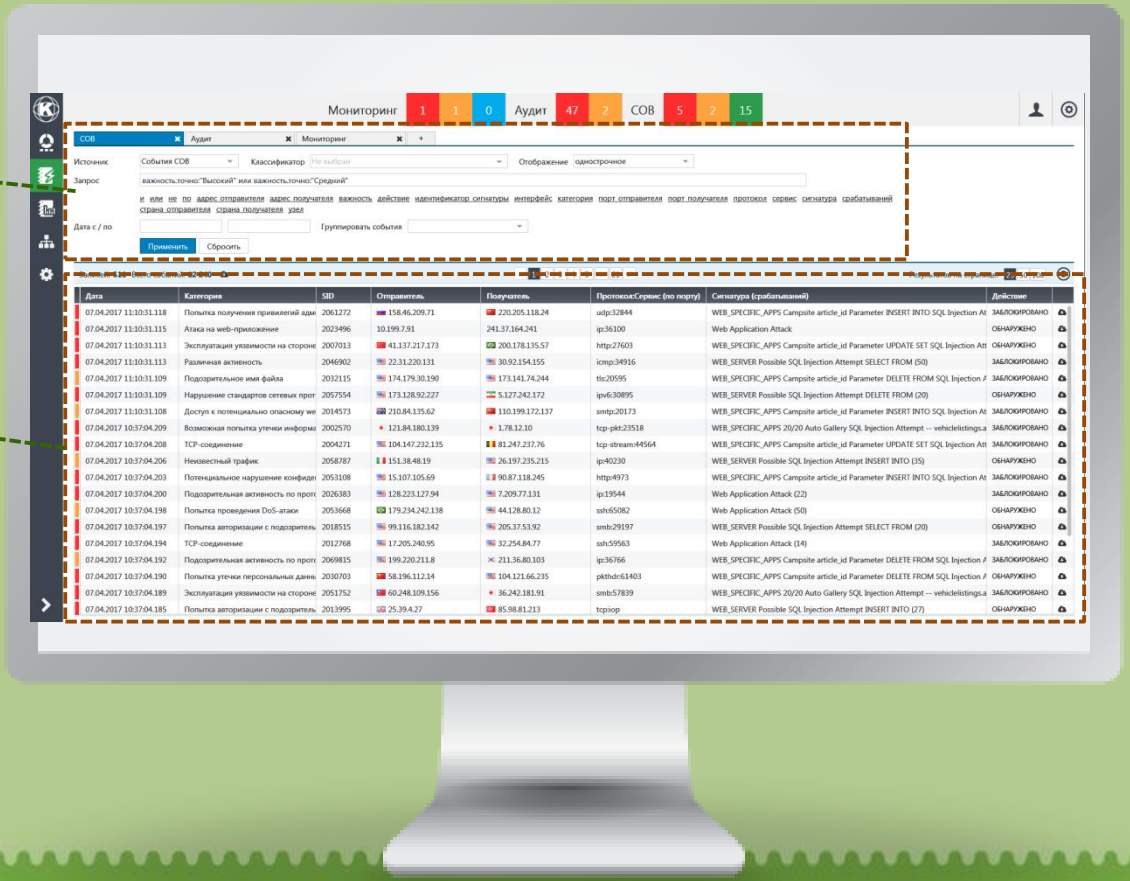
DOM_75 Информация	DOM_70 Информация	Несортирован... Информация	Удаленные Информация
0 1 0	0 0 0	0 0 0	0 0 0

КОД БЕЗОПАСНОСТИ

СПИСОК СОБЫТИЙ БЕЗОПАСНОСТИ СОВ «КОНТИНЕНТ»

Поисковая строка - фильтр по событиям безопасности

Список событий безопасности



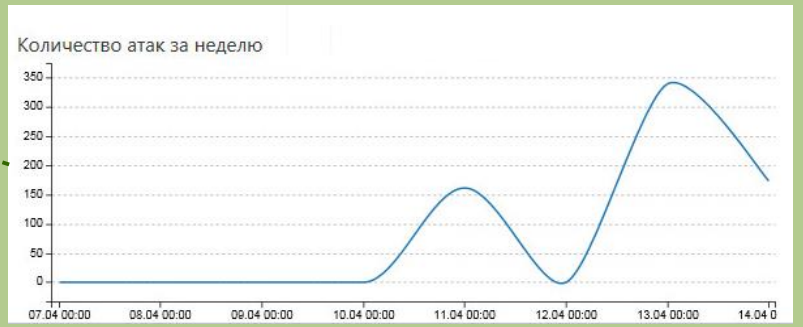
КОД БЕЗОПАСНОСТИ

ПОДРОБНАЯ ИНФОРМАЦИЯ ПО СОБЫТИЮ СОВ «КОНТИНЕНТ»

КОД БЕЗОПАСНОСТИ

СТАТИСТИКА СОВ «КОНТИНЕНТ»

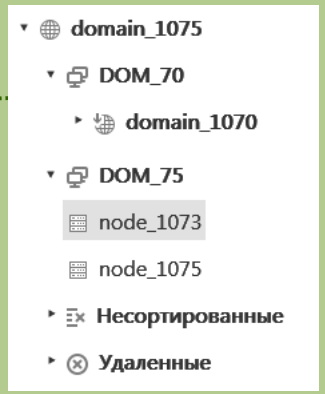
Настраиваемые виджеты статистики работы СОВ



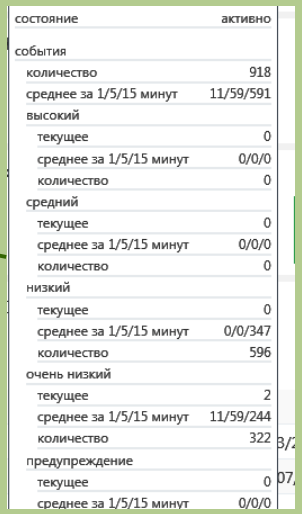
КОД БЕЗОПАСНОСТИ

МОНИТОРИНГ ИЕРАРХИЧЕСКОЙ СТРУКТУРЫ СОВ «КОНТИНЕНТ»

Иерархия системы управления



События подсистемы



состояние	активно
события	
количество	918
среднее за 1/5/15 минут	11/59/591
высокий	
текущее	0
среднее за 1/5/15 минут	0/0/0
количество	0
средний	
текущее	0
среднее за 1/5/15 минут	0/0/0
количество	0
низкий	
текущее	0
среднее за 1/5/15 минут	0/0/347
количество	596
очень низкий	
текущее	2
среднее за 1/5/15 минут	11/59/244
количество	322
предупреждение	
текущее	0
среднее за 1/5/15 минут	0/0/0

Уровень загрузки ресурсов Детектора атак

КОД БЕЗОПАСНОСТИ

ОБНАРУЖЕНИЕ АТАК

ДЕТЕКТОР АТАК «КОНТИНЕНТ»

Аппаратно-программный комплекс, сетевой сенсор, предназначенный для анализа сетевого трафика, обнаружения и предотвращения вторжений

Двухуровневая система анализа трафика

- **Сигнатурный анализ**
- **Эвристический анализ**

Установка политики безопасности без перерыва в работе сервисов

Дистанционное обновление системного ПО и сигнатур (базы решающих правил)

КОД БЕЗОПАСНОСТИ

ОБНАРУЖЕНИЕ АТАК
СИГНАТУРНЫЙ АНАЛИЗ ТРАФИКА

ДЕТЕКТОР АТАК «КОНТИНЕНТ»

Аппаратно-программный комплекс, сетевой сенсор, предназначенный для анализа сетевого трафика, обнаружения и предотвращения вторжений

Более 25000 сигнатур в базе решающих правил

Автоматическое обновление базы решающих правил с серверов «Кода Безопасности»

Собственная лаборатория, разрабатывающая сигнатуры

КОД БЕЗОПАСНОСТИ

ОБНАРУЖЕНИЕ АТАК
АНАЛИЗ СЕТЕВЫХ ПРИЛОЖЕНИЙ

ДЕТЕКТОР АТАК «КОНТИНЕНТ»

Аппаратно-программный комплекс, сетевой сенсор, предназначенный для анализа сетевого трафика, обнаружения и предотвращения вторжений

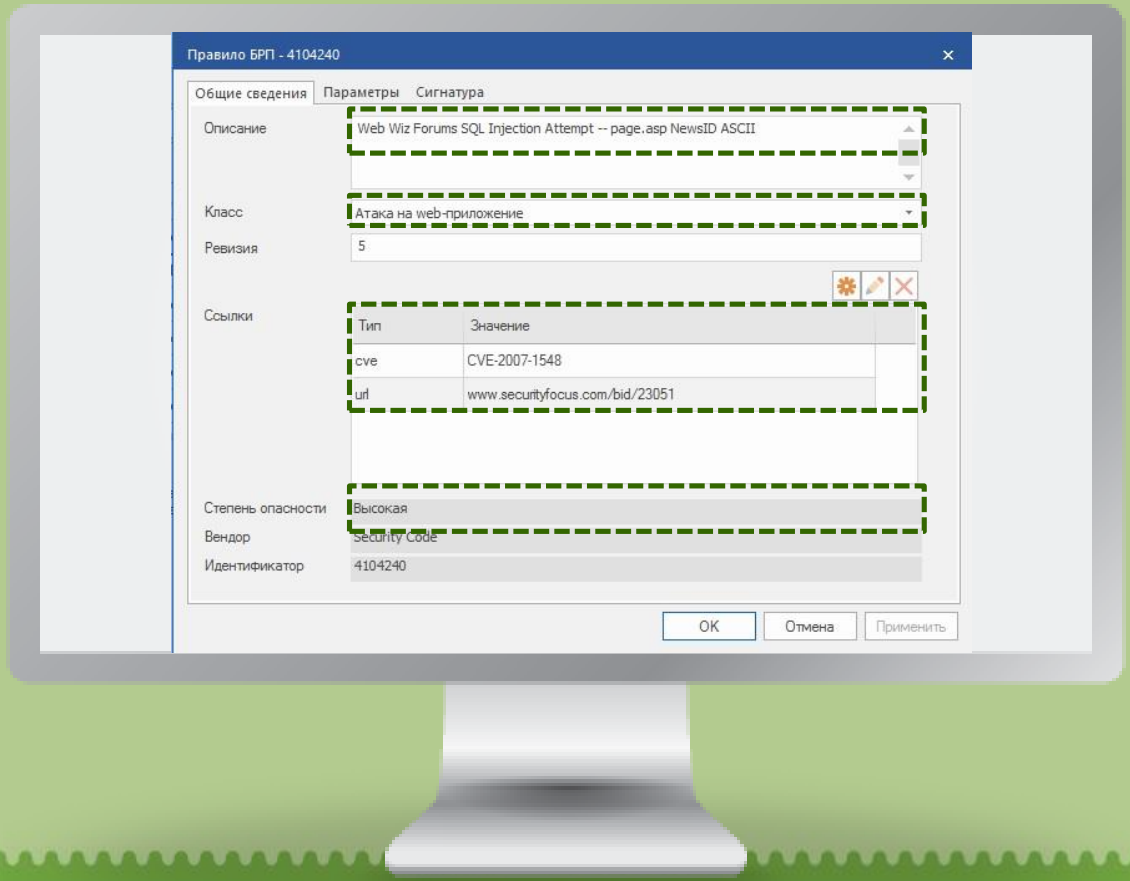
Обнаружение и блокировка сетевых приложений

Несколько типов контролируемых приложений

- **Торренты**
- **Социальные сети**
- **Системы удаленного администрирования**
- **Мессенджеры**
- **Системы туннелирования трафика**

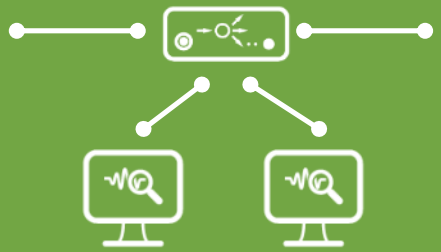
КОД БЕЗОПАСНОСТИ

ПОДРОБНОЕ ОПИСАНИЕ ПРАВИЛА БРП СОВ «КОНТИНЕНТ»



КОД БЕЗОПАСНОСТИ

МАСШТАБИРОВАНИЕ



БАЛАНСИРОВЩИК НАГРУЗКИ «КОНТИНЕНТ»

Аппаратно-программный комплекс для распределения сетевого трафика между узлами фермы, состоящей из Детекторов атак

Обеспечение отказоустойчивости

Линейное наращивание производительности

Высокая общая производительность

- **До 10 Гбит/с**

Объединение до 3 устройств IPC-3000NDF

Гибкая интеграция в сетевую инфраструктуру

- **Установка в режиме мониторинга**
- **Установка в «разрыв»**

КОНТИНЕНТ TLS VPN

КОД БЕЗОПАСНОСТИ

ПАК «КОНТИНЕНТ TLS СЕРВЕР»

ПАК «КОНТИНЕНТ TLS СЕРВЕР»

Система обеспечения защищенного доступа к web-приложениям

Предназначен для решения следующих задач:

- **Защищенный удаленный доступ к корпоративным ресурсам**
- **Защищенный доступ к интернет-порталам с шифрованием по ГОСТ**

КОД БЕЗОПАСНОСТИ

ПРЕИМУЩЕСТВА «КОНТИНЕНТ TLS VPN»

- Высокая производительность – до 20 000 одновременных подключений на одну ноду
- Высокая масштабируемость
- Совместимость с любыми веб-браузерами
- Простота внедрения и эксплуатации
- Удобство управления: все настройки осуществляются администратором через веб-браузер
- Интеграция с SIEM-системами

КОД БЕЗОПАСНОСТИ

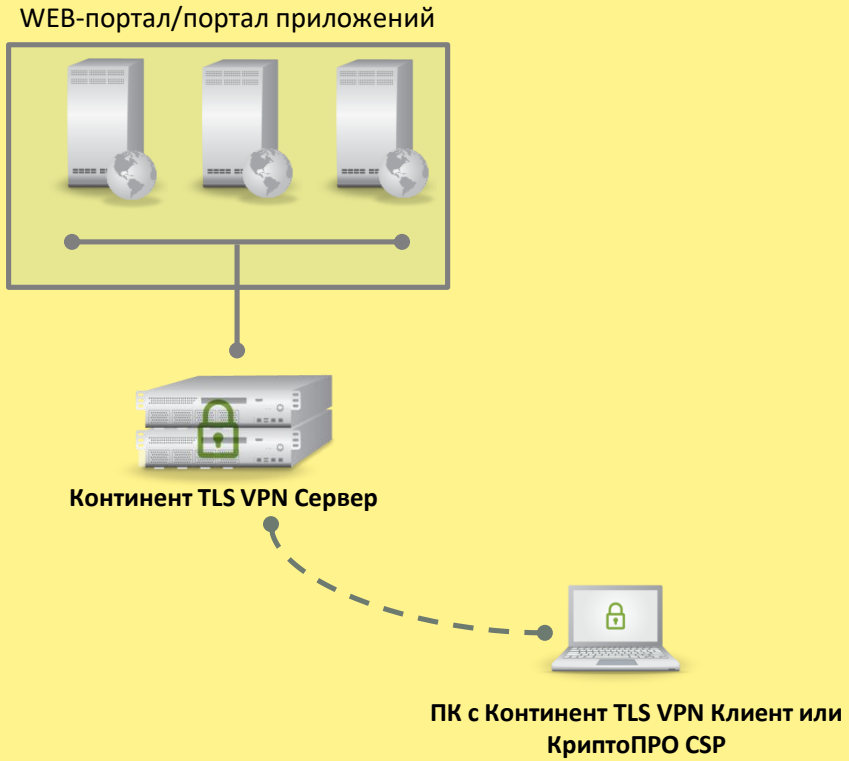
КОНТИНЕНТ TLS VPN

Задачи:

- Доступ удаленных сотрудников к внутренним web-ресурсам
- Разграничение доступа к web-приложениям
- Удаленный доступ с помощью «толстых» клиентов
  - Клиенты ERP-приложений
  - Доступ к терминальному серверу/VDI

Компоненты:

- Континент TLS VPN Сервер
- Континент TLS VPN Клиент или КриптоПРО CSP



КОД БЕЗОПАСНОСТИ

АРХИТЕКТУРА TLS СЕРВЕРА

Код Безопасности

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

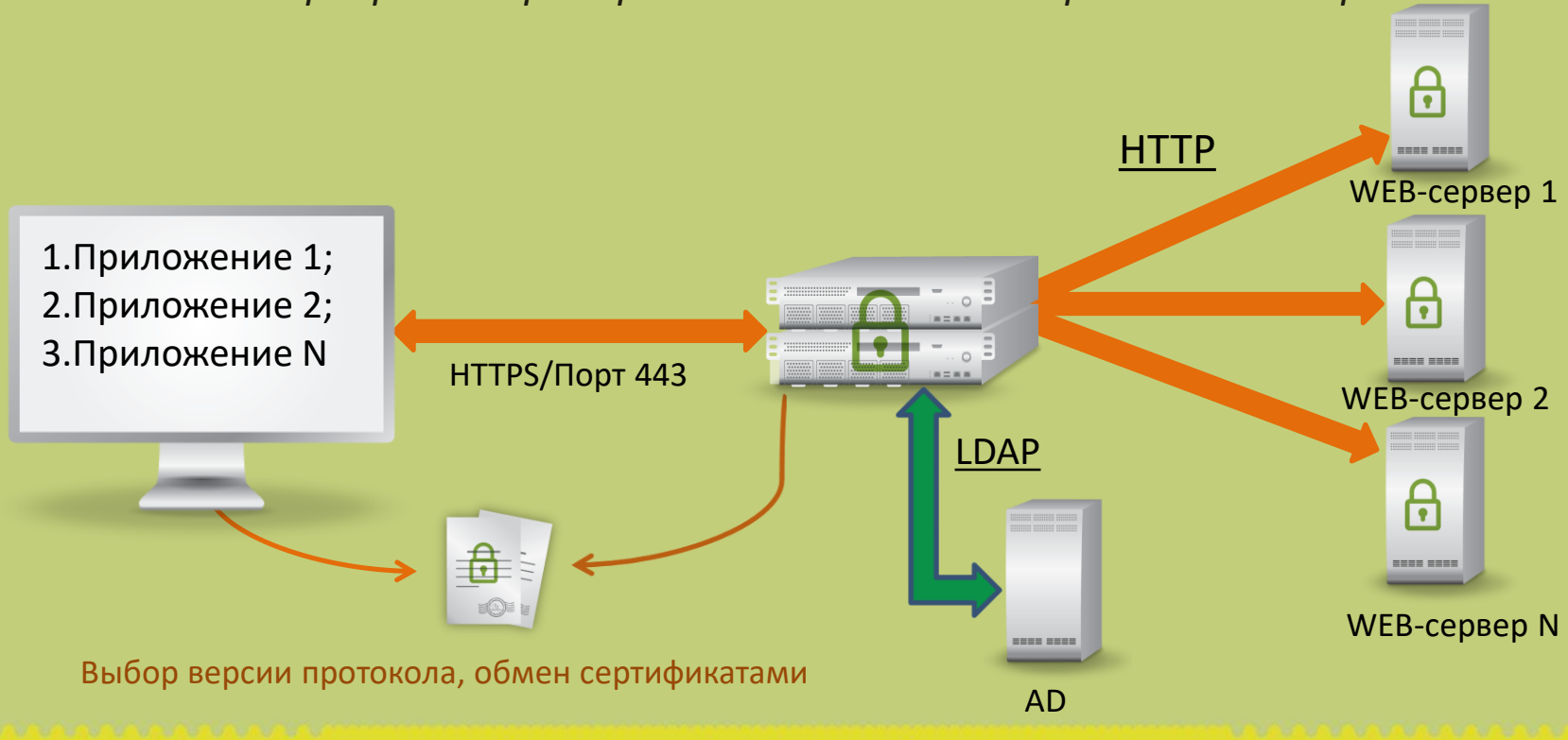
- HTTPS - прокси
- Портал приложений
- TLS-туннель

TLS сервер

Код безопасности

ПОРТАЛ ПРИЛОЖЕНИЙ

Один серверный сертификат – множество приложения портала

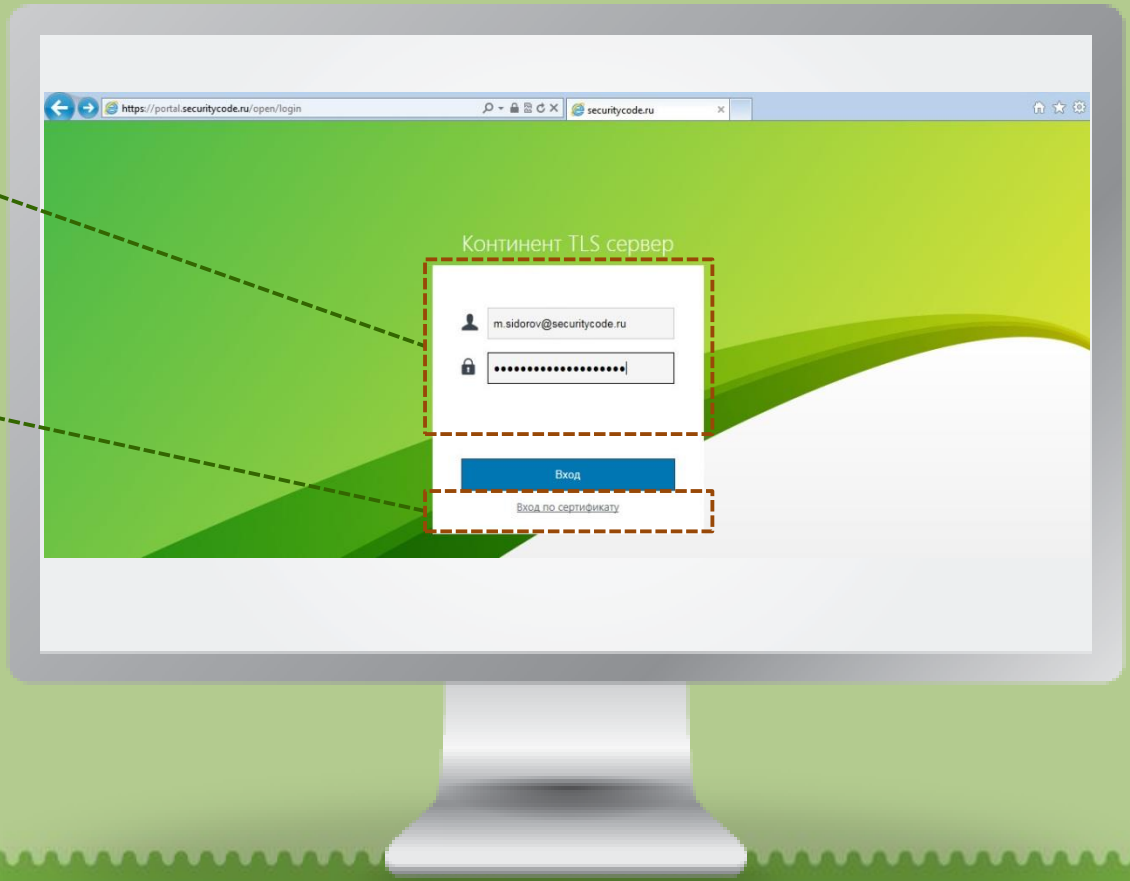


КОД БЕЗОПАСНОСТИ

ПОРТАЛ ПРИЛОЖЕНИЙ «КОНТИНЕНТ TLS СЕРВЕР»

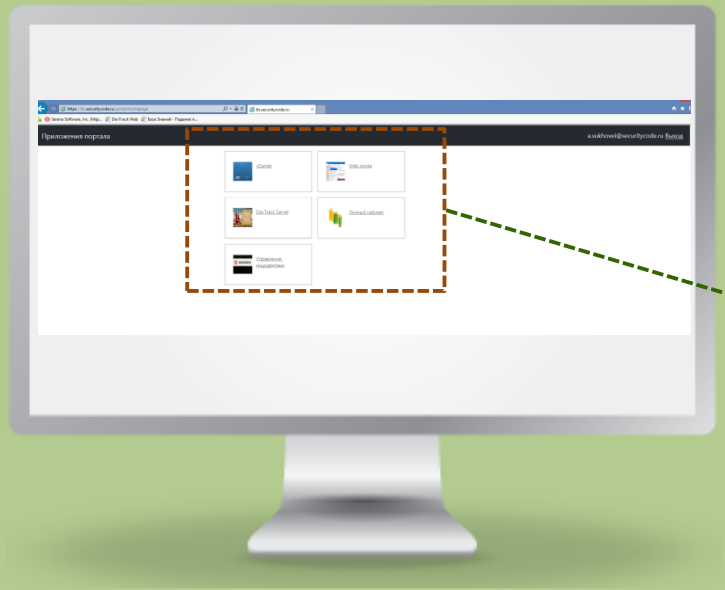
Авторизация по паре логин/пароль

Авторизация по сертификату



КОД БЕЗОПАСНОСТИ

ПОРТАЛ ПРИЛОЖЕНИЙ «КОНТИНЕНТ TLS СЕРВЕР»

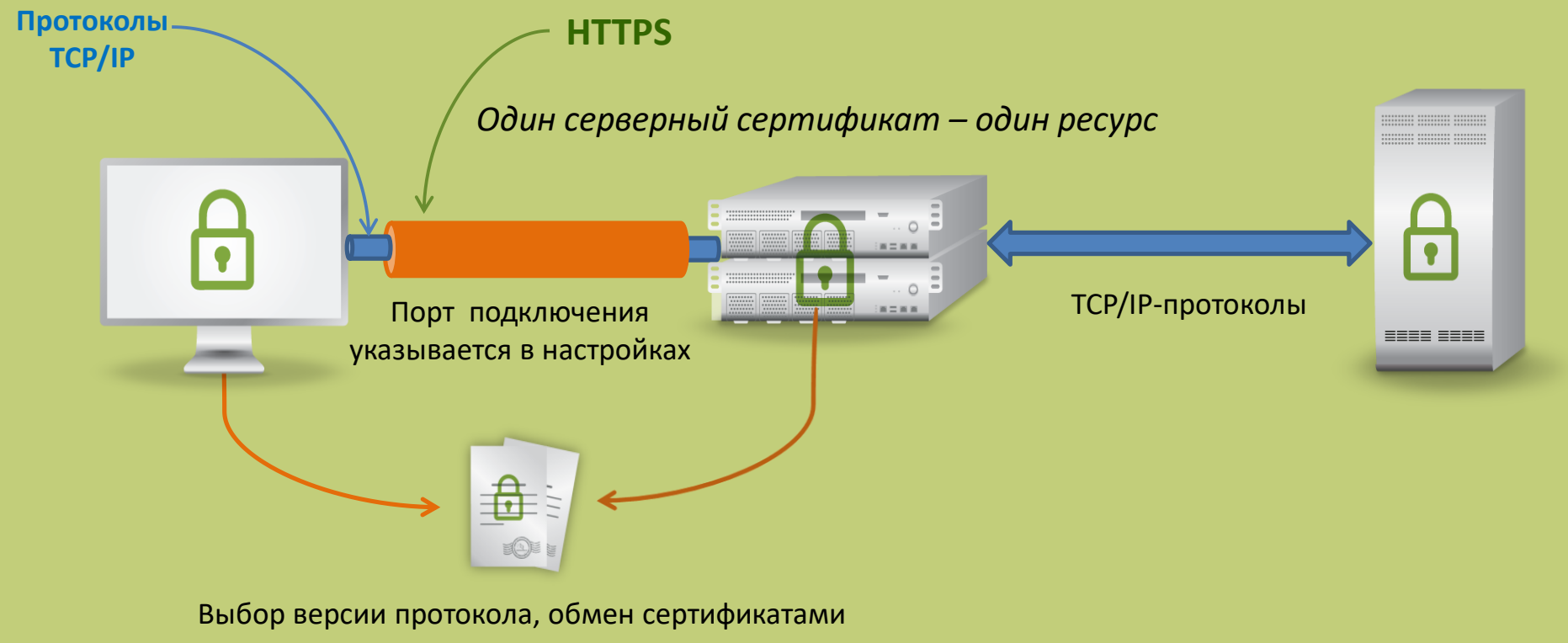


Доступные для пользователя web-приложения

- vCenter
- Web почта
- DevTrack Server
- Личный кабинет
- Управление инцидентами

Код безопасности

РЕЖИМ TLS-ТУННЕЛЬ



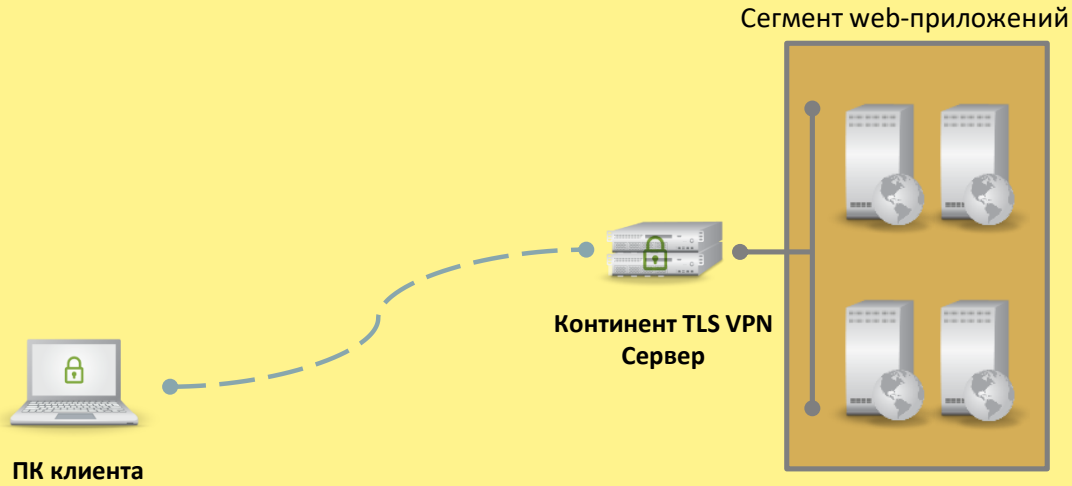
КОД БЕЗОПАСНОСТИ

АНОНИМНЫЙ ДОСТУП К WEB-ПРИЛОЖЕНИЮ

Задачи:

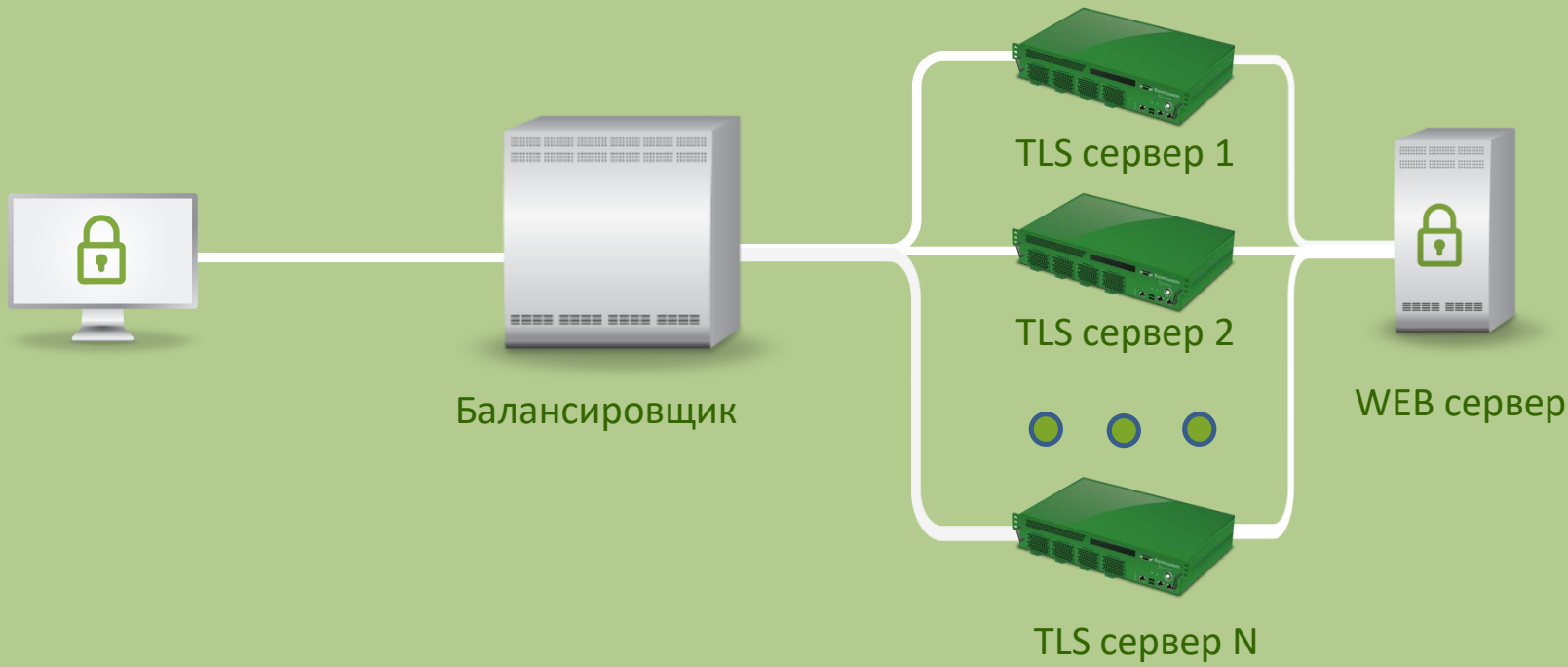
- Доступ к порталу госуслуг
- Доступ к «электронной регистратуре», «электронному дневнику» и т.д.

TLS сервер не запрашивает сертификат пользователя.



КОД БЕЗОПАСНОСТИ

АРХИТЕКТУРА КЛАСТЕРА TLS СЕРВЕРОВ



КОД БЕЗОПАСНОСТИ

ШИФРОВАНИЕ НА СТОРОНЕ КЛИЕНТА

КОНТИНЕНТ TLS VPN КЛИЕНТ

Туннелирование TCP-трафика

Удаленный доступ с использованием толстых клиентов. Например:

- **Терминальный клиент**
- **ERP-клиент**

Поддержка любых браузеров

Поддержка ОС Windows

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows 8/8.1**

Не нужен криптопровайдер «КриптоПро»

Клиент бесплатен для конечных пользователей

Континент WAF

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

АНАЛИЗ ТРАФИКА

КОНТИНЕНТ WAF

Аппаратно-программный комплекс, предназначенный для защиты веб-приложений

Гибкая настройка моделей работы приложений

- **Валидация протокола HTTP**
- **Синтаксический анализ запросов и ответов**
- **Определение бизнес-логики приложения**
- **Идентификация, аутентификация пользователей и контроль сессий**

Автоматическое построение модели работы приложения (профилирование)

Анализ соответствия поведения пользователя позитивной модели работы приложения (запрещено всё, что явным образом не разрешено)

Расшифровка SSL-трафика (MitM)

Пакет преднастроенных сигнатур

КОД БЕЗОПАСНОСТИ

ОБНАРУЖЕНИЕ АНОМАЛИЙ

КОНТИНЕНТ WAF

Аппаратно-программный комплекс, предназначенный для защиты веб-приложений

Обнаружение аномалий как в HTTP-запросах, так и в ответах

Обнаружение аномалий на основе модели работы приложения

- **Совпадение с моделью**
- **Отклонение от модели**

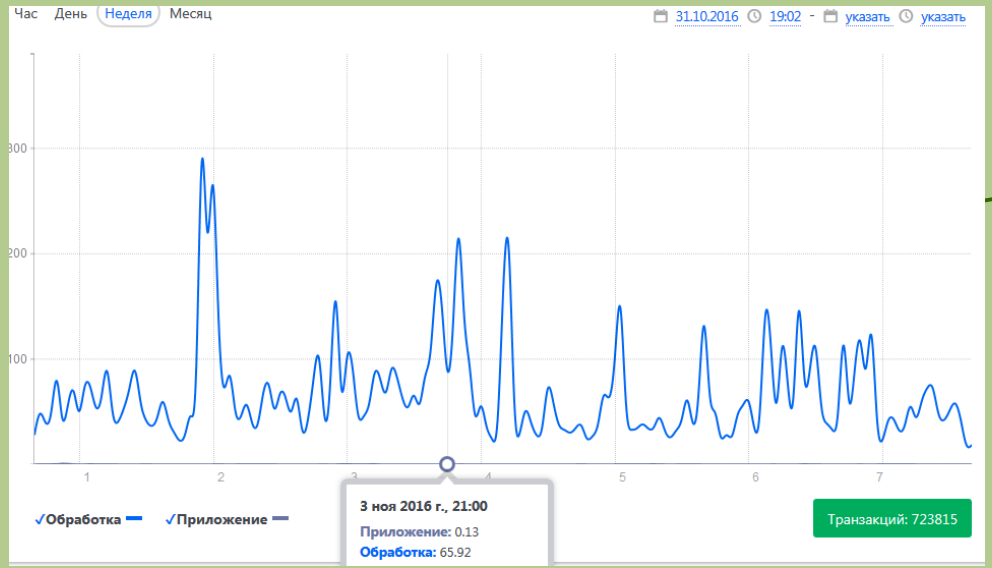
Обнаружение аномалий внутри вложенных данных, передаваемых по протоколу HTTP

Обнаружение Bruteforce-атак

КОД БЕЗОПАСНОСТИ

ИНФОРМАЦИЯ ОБ АНОМАЛИЯХ

Статистика задержек ответов веб-сервера



ЗАЩИТА ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

ПРОДУКТ

ЗАЩИТА ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

vGATE

Сертифицированное средство защиты виртуальной инфраструктуры

Сертификаты

ФСТЭК России:
vGate R2: СВТ 5/НДВ 4, применяется для защиты АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до К1 и АСУ ТП до К1 включительно.
vGate-S R2: ТУ/НДВ 2, применяется для защиты АС до класса 1Б включительно и ИСПДн до УЗ1 включительно.

КОД БЕЗОПАСНОСТИ

ВОЗМОЖНОСТИ vGATE

КОД БЕЗОПАСНОСТИ

ЗАЩИТА ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ С VGATE 4.1

- Реализован межсетевой экран уровня гипервизора (аналог VMware NSX, Check Point vSEC)
  - Для микросегментации виртуализованных сред
  - Планируется сертификат по МЭ тип «Б» класс 4
- Поддержка Скала-Р
- Поддержка среды KVM

Спасибо за внимание!

КОД БЕЗОПАСНОСТИ

info@securitycode.ru
http://securitycode.ru