КОД безопасности

Российские платформы сетевой безопасности

Континент 4

КОД безопасности

Вектора атаки – как проникают…

- Фишинг (от массового к целевому)
- Кража паролей в предыдущих инцидентах (утечки)
- Атака через подрядчика
- Компрометация веб-сервиса организации
- Компрометация сервиса, на который заходят сотрудники
- Проникновение через USB-накопители

КОД безопасности

Инструменты атаки…

Индивидуально разработанные вирусы

«Покупные» вирусы

Вирусы в открытом доступе

Легитимные инструменты

Как можно предотвратить?

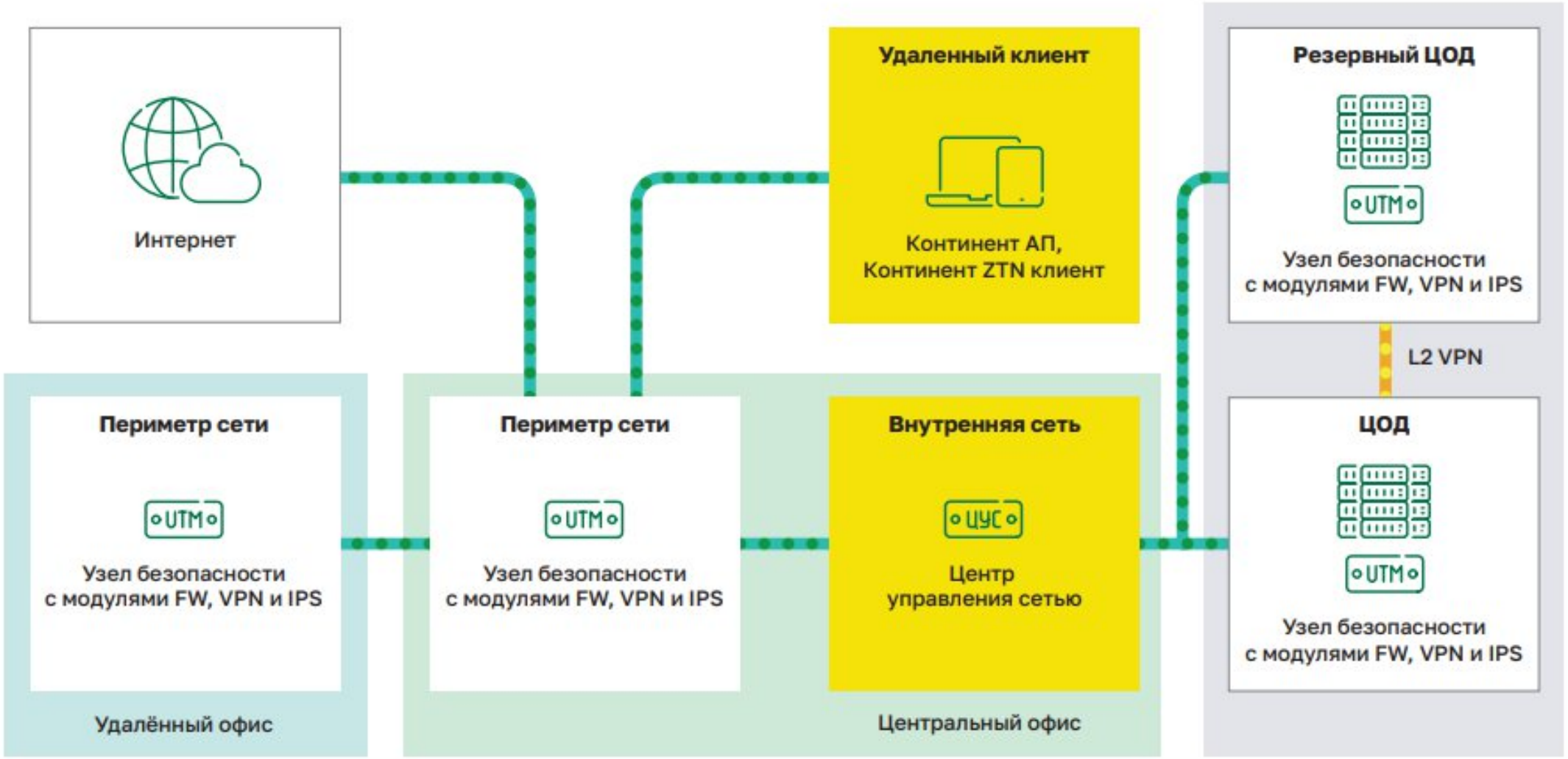
- Сигнатурный анализ
- Эвристический анализ
- Машинное обучение и искусственный интеллект

СЗИ работают не всегда:

- У заказчика могу быть ключевые средства защиты информации (СЗИ)
- Это не означает, что они не нужны. Но если их нет – это повод задуматься

КОД безопасности

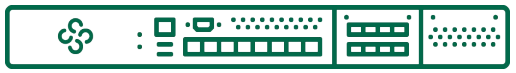
Сценарии - Континент 4



КОД безопасности

Режимы работы

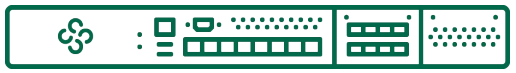
NGFW



Интегрированный межсетевой экран

- Межсетевой экран
- Контроль приложений
- URL - фильтрация
- Поведенческий анализ (на базе машинного обучения)
- Система обнаружения и предотвращения вторжений на сетевом уровне (L3)

Proxy



Прокси-сервер

Прозрачный (Transparent) и явный (Explicit) режимы

L2 IPS

Детектор атак

Система обнаружения вторжений на канальном уровне (L2)

КОД безопасности

Технологическая экосистема

Многофакторная

MULTIFACTOR
Avanpost
КОМПАНИЯ ИНДИД
Аладдин

Балансировка нагрузки

ЦИФРОВЫЕ РЕШЕНИЯ

Анализ правил

EFROS DEFENCE OPERATIONS
Нетхаб
SPACE-BIT

Микросегментация

vGate

Песочницы

positive technologies
AVSOFT
kaspersky

Индикаторы компрометации

kaspersky
Security Vision
CyberThreatTech
R-Vision
BI.ZONE

Удаленный доступ

MacOS
iOS
АВРОРА

Комплаенс-контроль

Континент ZTN клиент
Сакура

Возможности К4

Безопасность

- поддержка ГОСТ VPN
- контроль сетевых приложений (4200+)
- фиды Threat Intelligence (собственные, ЛК, RST Cloud)
- система предотвращения вторжений (СОВ) управление сигнатурами (БРП)
- фильтрация по странам (GeoProtection)
- фильтрация по доменным именам (DNS Resolver)
- фильтрация по категориям URL настройка параметров паттернов атак типа DoS
- потоковый антивирус (хеши KES) с расширением пользовательскими сигнатурами
- интеграция с песочницами (ICAP)
- поведенческий анализ на основе машинного обучения
- собственный VPN-клиент под разные ОС
- расшифровка TLS 1.3
- разграничение доступа групп пользователей к различным сегментам сети на уровне подсетей
- список доступа к центру управления сетью (ЦУС)
- реализация явного веб-прокси

Управление

- централизованное управление всеми устройствами из единой консоли – единая база сетевых объектов – политики, правила маршрутизации и фильтрации…
- расширяемая панель мониторинга (веб-сервис)
- новая система распространения обновлений
- интеграция с LDAP
- идентификация и аутентификации пользователей (локальная база ЦУС, AD, captive-портал, агент)
- сквозная аутентификация пользователей (SSO)
- кластеризация узла безопасности (Active – Passive) с сохранением состояния сессий
- универсальный конвертер политик (утилита)
- мониторинг и уведомление о политике по SMTP
- импорт / экспорт сетевых объектов
- ролевая модель доступа администраторов

КОД безопасности

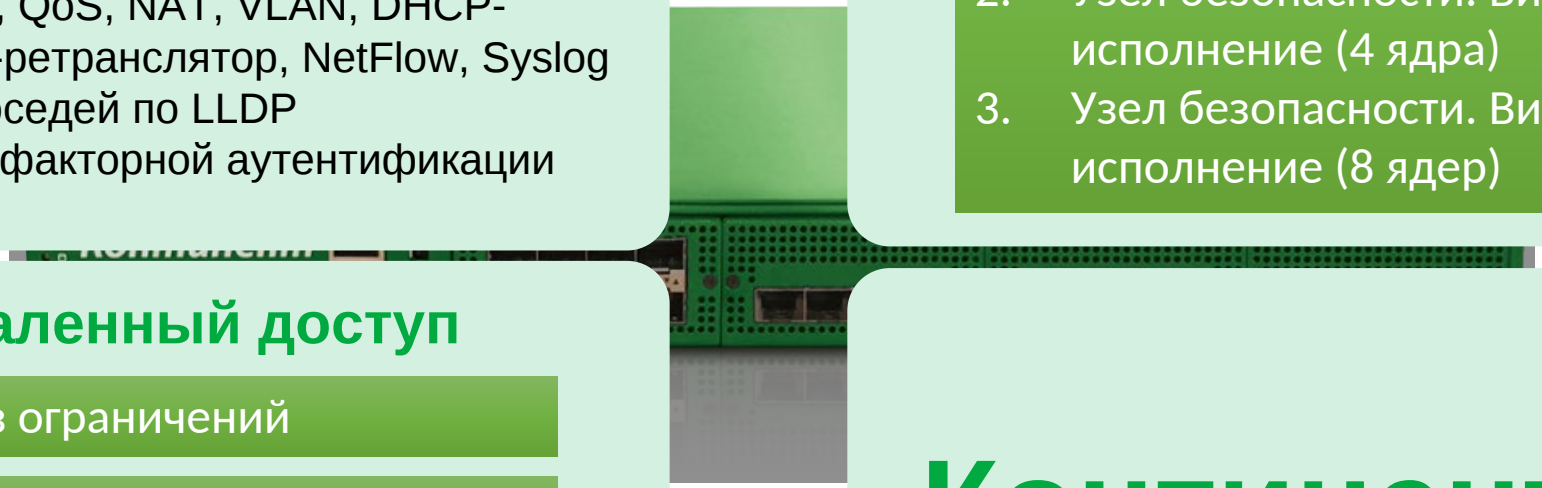
Возможности К4

Сетевые технологии

- динамическая маршрутизация (BGP)
- поддержка нескольких провайдеров (Multi-WAN) и реализация Policy Based Routing (PBR)
- поддержка VRF, QoS, NAT, VLAN, DHCP-сервер и DHCP-ретранслятор, NetFlow, Syslog
- обнаружение соседей по LLDP
- поддержка двухфакторной аутентификации

Виртуальное исполнение

1. Узел безопасности. Виртуальное исполнение (2 ядра)
2. Узел безопасности. Виртуальное исполнение (4 ядра)
3. Узел безопасности. Виртуальное исполнение (8 ядер)



VPN и удаленный доступ

- без ограничений
- доступны только корпоративные ресурсы (запрет незащищенных)
- весь трафик в туннель + правила

Континент ZTN

(мультиплатформенность)

построение сложных VPN топологий уровня «созвездие»

КОД безопасности

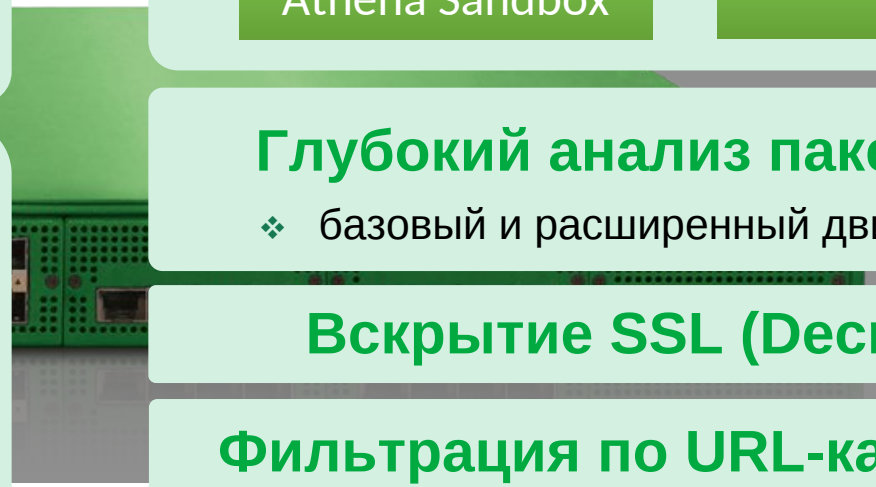
Возможности К4

Надежность и производительность

- проверка трафика только по определенным сигнатурам – исключена перегрузка устройства обработкой потока трафика по всем сигнатурам – оптимизация ресурсов для других механизмов защиты

Управление сигнатурами (БРП)

- собственная лаборатория (>40К сигнатур)
- сигнатуры доступны в открытом виде по всем категориям
- в конкретной сигнатуре возможно отредактировать любой параметр
- создание пользовательских профилей из комбинаций сигнатур самостоятельно без ТП (менеджер конфигураций)
- новая схема получения обновлений сигнатур – поддержка offline – репозитория
- IPS: сетевой и канальный уровень



Поддержка «песочниц»

- PT Sandbox
- ЛК Sandbox
- Athena Sandbox
- .....

Глубокий анализ пакетов (DPI)

- базовый и расширенный движок

Вскрытие SSL (Decryption)

Фильтрация по URL-категориям

Базы зловредных URL

Фильтрация по странам (GeoProtection)

КОД безопасности

Лицензирование

Модуль	Узел Безопасности (УБ)	UTM Базовый	UTM Расширенный
Центр управления сетью (ЦУС)	✓	✓	✓
Межсетевой экран (МЭ)	✓	✓	✓
Сервер Доступа (СД)	✓	✓	✓
Контроль приложений (1700 приложений и протоколов)	✓	✓	✓
URL-фильтрация	✓	✓	✓
Расширенный контроль приложений (4000 приложений и протоколов)		✓	✓
Система обнаружения вторжений		✓	✓
Модуль блокировки трафика по стране происхождения (GeoIP)		✓	✓
Защита от вредоносных сайтов			✓
Преднастроенные категории URL			✓
Потоковый антивирус			✓
L2 VPN	Не входит в состав УБ/UTM, приобретается отдельно. Срок действия лицензии - бессрочно.		

Платформы ТОРП (ПП 878)

Континент 4 IPC-R10

Континент 4 IPC-R300

Континент 4 IPC-R50

Континент 4 IPC-R550

Континент 4 IPC-R1000

Континент 4 IPC-R800

Континент 4 IPC-R3000

Заключение № 123237/11 от 30.11.2022 (срок действия 27.11.2025*).

*) Срок действия заключения продлен для случаев, когда применяется п. 2 ПП РФ от 01.04.2022 № 553 "О некоторых вопросах подтверждения производства промышленной продукции на территории Российской Федерации".

Наименование производимой промышленной продукции	Код промышленной продукции по ОК0342014 (ОКПД2)	Код промышленной продукции по ТНВЭДЕАЭС	Информация о совокупном количестве баллов за выполнение (освоение) на территории Российской Федерации таких операций (условий)	Информация о соответствии количества баллов достаточного для целей закупок промышленной продукции
Комплекс безопасности "Континент". Версия 4. Узел безопасности IPC-R550	26.20.40.140	8473 30	-	-

*платформы со статусом телекоммуникационного оборудования российского происхождения (ТОРП)
https://www.securitycode.ru/products/models/torp/

Производительность

Континент 4
IPC-R300

параметр	значение
Производительность МЭ, Мбит/с	до 4 000
Производительность VPN, Мбит/с	до 500
Производительность UTM, Мбит/с	до 1 200
Производительность L2 IPS, Мбит/с	до 1 100
Производительность ЦУС (количество управляемых устройств)	до 40
Производительность Сервера доступа (количество одновременных подключений)	до 100
Среднее время наработки на отказ	50 000

*платформы со статусом телекоммуникационного оборудования российского происхождения (ТОРП)
https://www.securitycode.ru/products/models/torp/

КОД безопасности

Континент 4.1.9

- Ключевые возможности:

- ✓ Поддержка функционала VRF, в том числе использование VRF в отказоустойчивом кластере
- ✓ Фиды Threat Intelligence от разных поставщиков (RST Cloud и КБ)
- ✓ Прокси-сервер с возможностью SSL инспекции трафика, использования URL-фильтрации, фидов Threat Intelligence, потокового антивируса, GeoIP
- ✓ Поддержка статических ARP-записей
- ✓ Добавление временных интервалов со сроком действия до определенной даты
- ✓ URL-фильтрация на основе SNI с использованием пользовательских категорий
- ✓ Поддержка протокола BFD
- ✓ Рассылка отчетов по расписан

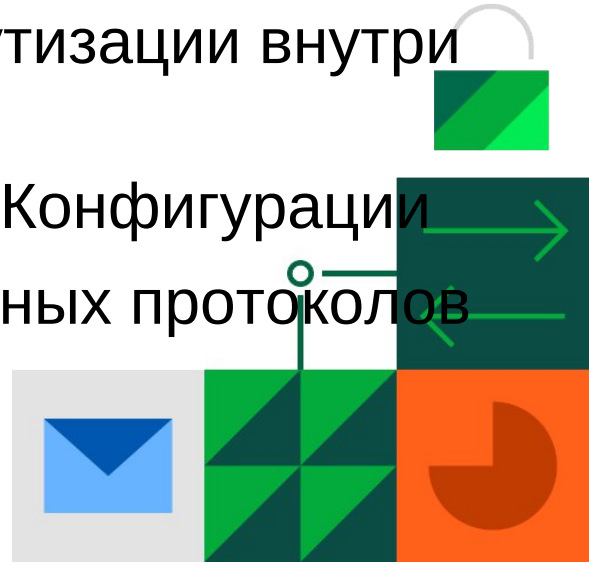
Threat intelligence (данные о киберугрозах) — это информация об актуальных угрозах и группировках киберпреступников, которая позволяет организациям изучить цели, тактику и инструменты злоумышленников и выстроить эффективную стратегию защиты от атак. Компании могут сами собирать данные о киберугрозах или заказывать информацию у сторонних поставщиков.

КОД безопасности

Континент 4.2

- Ключевые возможности:

- ✓ Поддержка VPN на базе IPSec (ГОСТ ТК26)
- ✓ Поддержка протокола RADIUS (проверка на Avanpost FAM и Aladdin JAS)
- ✓ Динамические профили IPS
- ✓ Поддержка работы протоколов динамической маршрутизации внутри VPN
- ✓ Отказ от ОС Windows при использовании Менеджера Конфигурации
- ✓ Доработка функционала для фильтрации промышленных протоколов (АСУТП/SCADA)
- ✓ Поддержка USB-модемов (GSM)



КОД безопасности

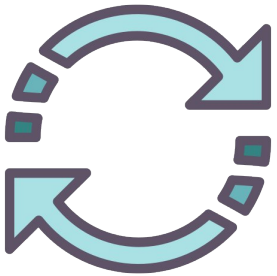
Автоматизация миграции

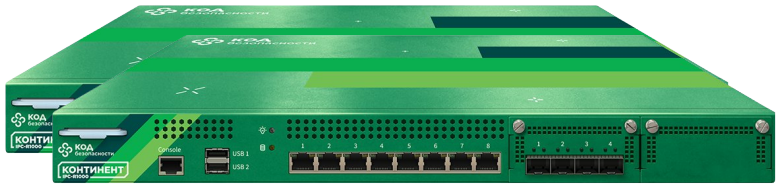
Прямой импорт политик Check Point, FortiGate

Импорт политик с Cisco, Palo Alto, Juniper через промежуточный импорт в Check Point

Миграция с Континент 3 и др. МЭ

Переход с CheckPoint на Континент 4





Этапы

Выгрузка файлов конфигурации с **Check Point**

Преобразование файлов конфигурации **Check Point** в формат **Континент 4**

Импорт политик и объектов в **Континент 4**

VPN и удаленный доступ

Континент АП/ZTN

VPN-клиент для мобильных устройств и ПК

Клиентские приложения для всех популярных платформ

Методы аутентификации удаленных пользователей:

- Сертификат
- Логин/пароль
- Многофакторная аутентификации с помощью сервиса multifactor.ru
- Многофакторная аутентификации с помощью Avanpost MFA new

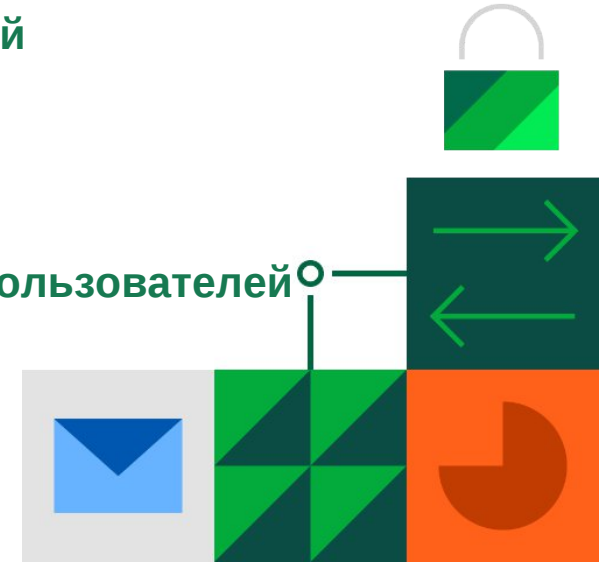
Поддержка Сервером доступа аутентификации по сертификатам ГОСТ 2012 (ТК26)

Поддержка различных ключевых носителей

Возможность установки VPN-соединения до регистрации пользователя в ОС

Режим запрета незащищенных соединений

Разделение пулов ip-адресов удаленных пользователей



VPN и удаленный доступ

Проверка обновлений ОС:

Проверяется именно дата последнего обновления системы. Дата должна быть не старее 40 дней.

Проверка ПО, обязательного к установке:

Проверяем по нашему списку (антивирусы, Соболь, SNS)
Есть возможность добавить «свое» ПО для контроля

- Windows
- Linux
- Aurora
- Android
- IOS
- MACOS (M1+M2)

Проверка запуска служб ПО обязательного к установке:

Если служба не запущена, нарушение комплаенса

Проверка обновления антивирусных баз:

Проверка обновления антивирусных баз. Дата должна быть не старее 7 дней.

Проверка ПО, запрещенного к установке:

Если обнаружено установленное запрещенное ПО, например, telegram, нарушение комплаенса
Есть возможность самостоятельно формировать список запрещенного ПО

КОД безопасности

Сертификация ФСТЭК

«Континент 4.1.7» может использоваться для защиты значимых объектов КИИ до 1 категории, ИСПДн до 1 уровня, ГИС до 1 класса и АС до класса 1Г включительно

4-й класс защиты межсетевых экранов уровня сети (тип «А»)

4-й класс защиты систем обнаружения вторжений уровня сети

4-й уровень доверия средств обеспечения безопасности информационных технологий

*платформы со статусом телекоммуникационного оборудования российского происхождения (ТОРП)
https://www.securitycode.ru/products/models/torp/

КОД безопасности

Подробнее

Большой онлайн по Континент 4

Импортозамещение NGFW

Телеграм канал Код на проводе

Телеграм чат по Континенту

КОД безопасности

Спасибо за внимание!

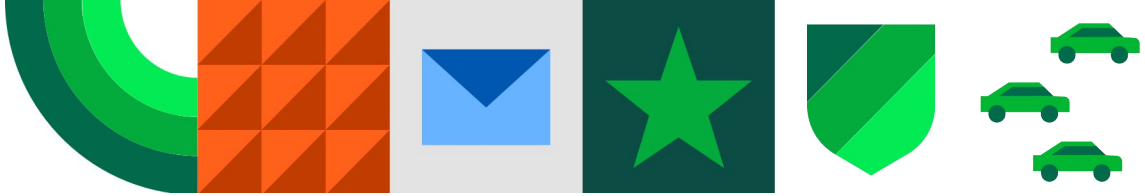
Николай Бабичев

директор по развитию бизнеса УрФО

n.babichev@securitycode.ru, +7 919 949 49 49

info@securitycode.ru

www.securitycode.ru



КОД
безопасности

info@securitycode.ru
www.securitycode.ru