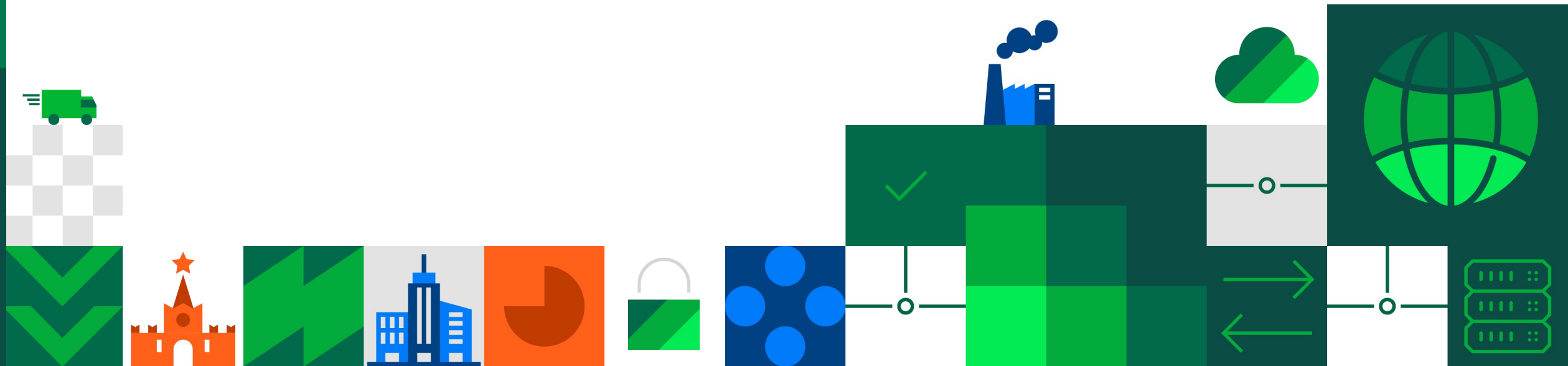
КОД безопасности

Защита периметра сети средствами Континент 4



КОД безопасности

Сценарии использования NGFW

Функции

- Централизованное управление
- Эргономика
- Контроль приложений
- Защита от вторжений и вредоносного ПО
- Масштабируемость и отказоустойчивость
- VPN и удаленный доступ
- Сетевые функции

Сценарии использования

- В датацентре организации
- На периметре организации
- В геораспределенной сети
- Для малого и среднего бизнеса

КОД безопасности

Функционал NGFW

Централизованное управление

- Управление большим количеством устройств через единую платформу
- Единый мониторинг для всей инфраструктуры межсетевых экранов
- Быстрая миграция со сторонних межсетевых экранов

Идентификация пользователей

- Прозрачная аутентификация пользователей через Kerberos
- Captive-портал
- Агент идентификации

Контроль приложений

- Обнаружение и классификация приложений
- Блокировка и разрешение доступа к приложениям

Эшелонированная защита

- Предотвращение
- Поиск известных угроз
- Поиск неизвестных угроз

VPN

- IPsec по международным алгоритмам (Q3 2023)

КОД безопасности

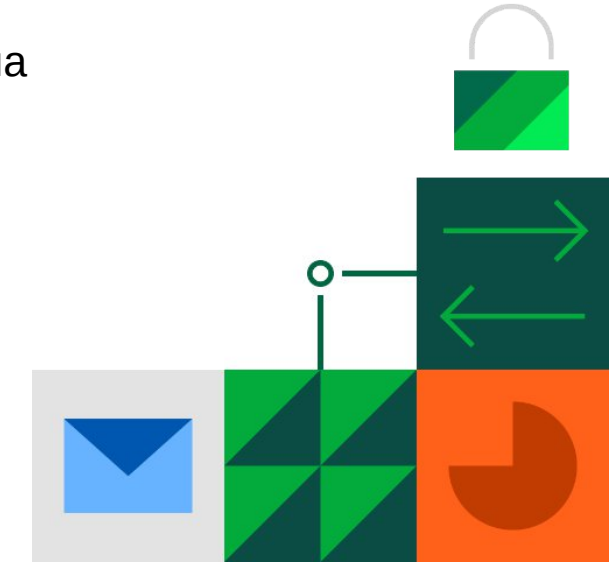
О продукте

Континент 4

Многофункциональный межсетевой экран (NGFW/UTM)

Предназначен для решения следующих задач:

- Централизованная защита периметра корпоративной сети
- Контроль доступа пользователей в Интернет
- Предотвращение сетевых вторжений
- Организация защищенного удаленного доступа



Получен сертификат соответствия техническому регламенту ТР 2013/027/BY

НАЦИОНАЛЬНАЯ СИСТЕМА ПОДТВЕРЖДЕНИЯ СООТВЕТСТВИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
Аккредитованный орган по сертификации
средств защиты информации и продукции по требованиям безопасности информации
Оперативно-аналитический центр при Президенте Республики Беларусь
Республика Беларусь, 220030, г. Минск, ул. Кирова, 49, т. 309-24-24
(аттестат аккредитации № BY/112 036.01, дата регистрации 15.10.1997 г.)

СЕРТИФИКАТ СООТВЕТСТВИЯ

TP BY

Зарегистрирован в реестре № BY/112 02.01. ТР027 036.01 00750

Дата регистрации 19 апреля 2023 г.
Действителен по 18 апреля 2028 г.

Заявитель Общество с ограниченной ответственностью «Код Безопасности», 129075, г.Москва, Мурманский проезд, д.14, корп.1, Российская Федерация.

Изготовитель Общество с ограниченной ответственностью «Код Безопасности», 129075, г.Москва, Мурманский проезд, д.14, корп.1, Российская Федерация.

Продукция Комплекс безопасности «Континент». Версия 4. АМБС.26.20.40.140.001 (модели: IPC-10, IPC-50, IPC-50M, IPC-3000F, IPC-3000NF2, IPC-3000FM, IPC-600, IPC-600M, IPC-800F, IPC-1000F, IPC-1000FM, IPC-1000NF2, IPC-R300, IPC-R550, IPC-500, IPC-500M, IPC-500F, IPC-R10, IPC-R50, IPC-R800, IPC-R1000, IPC-R3000), серийное производство.

Код ОКП РБ 26.20.30.400
Код ТН ВЭД ЕАЭС 8517620003

соответствует требованиям ТР 2013/027/BY (СТБ 34.101.8-2006 (пункты 6.5, 6.6, 6.8), СТБ 34.101.14-2017, СТБ 34.101.73-2017 (пункты 7.2-7.6), СТБ 34.101.75-2017 (пункты 7.2, 7.4, 7.6, 7.8)).

Сертификат соответствия выдан на основании отчета об анализе состояния производства от 07.04.2023, протоколов испытаний от 13.02.2023 № ПИ 020/2023, № ПИ 021/2023 испытательной лаборатории общества с ограниченной ответственностью «Секьюрити Лаб», аттестат аккредитации BY/112 2.5155.

Дополнительная информация Продукцию не допускается использовать в информационных системах класса 1 согласно СТБ 34.101.30-2017.

Заместитель начальника Центра — С.В.Жерносек

Эксперт-аудитор — П.В.Ильючек

№ 0301931

- **СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования»**
- **СТБ 34.101.14-2017 «Информационные технологии. Методы и средства безопасности. Программные лицензирование средства маршрутизатора. Общие требования»**
- **СТБ 34.101.73-2017 «Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования»**
- **СТБ 34.101.75-2017 «Информационные технологии. Системы обнаружения и предотвращения вторжений. Общие требования».**

КОД безопасности

Континент 4

Узел безопасности (УБ)

FW | IPS | App control | IPsec VPN | MGMT | Log | URL Filtering | User Identity

Antivirus | GeoIP

КОД безопасности

Компоненты

1. Центр управления сетью	**Обеспечивает централизованное управление сетевыми узлами, правилами фильтрации трафика, настройками маршрутизации, VPN-сетями и криптографическими ключами**
2. Межсетевой экран	Фильтрация трафика на границе сети
2.1 Контроль протоколов и приложений	Детальная фильтрация трафика по сигнатурам приложений и протоколов
2.2 Защита от вредоносных веб-сайтов	Блокировка вредоносных сайтов по протоколам HTTP, HTTPS, FTP
2.3 URL-фильтрация по категориям	Категоризация интернет-ресурсов
2.4 Антивирус	Проверка трафика потоковым антивирусом
2.5 Модуль GeoProtection	Фильтрация трафика по географической принадлежности IP-адресов

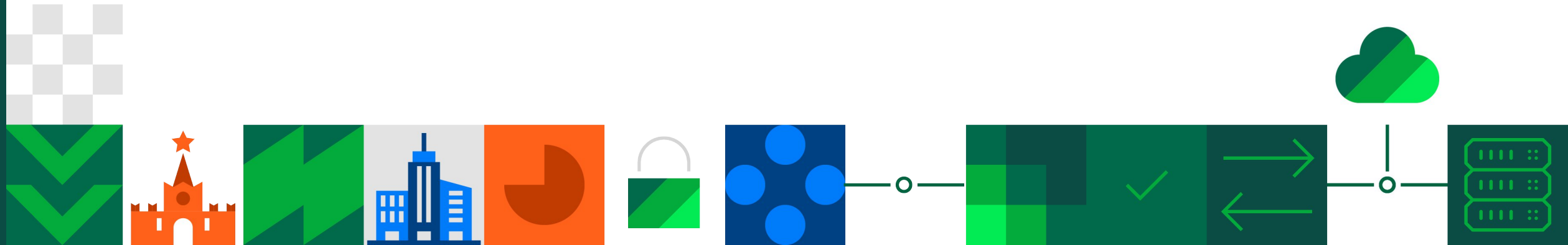
КОД безопасности

Компоненты

3. IPsec VPN	**Организация VPN-соединений**
4. Сервер доступа	Позволяет осуществить защищенное подключение удаленных пользователей, использующих программный VPN-клиент «Континент-АП» или «Континент ZTN-клиент»
5. Идентификация пользователей	Использование идентификаторов пользователей в правилах фильтрации
6. Система обнаружения вторжений	Обнаружение и предотвращение сетевых атак
7. Модуль поведенческого анализа	Обнаружение и предотвращение аномального трафика, атак сканирования и атак на основе корректности протоколов и угроз типа «отказ в обслуживании»

КОД безопасности

Управление



КОД безопасности

Система управления Континент 4

Единая база сетевых объектов хранится на ЦУС.

Любой объект из базы ЦУС может быть использован в правилах фильтрации.

Для каждого правила могут быть выбраны узлы, на которые оно будет установлено.

Администратору безопасности не придется вручную настраивать каждый узел при внесении изменений в корпоративную сеть.

КОД безопасности

Система управления Континент 4

Группы пользователей из общего корпоративного каталога можно добавлять в правила фильтрации в качестве источника.

Прозрачная аутентификация SSO

Интеграция упрощает процессы администрирования, аудита и логирования.

Нет необходимости заводить новых пользователей локально.

КОД безопасности

Система управления Континент 4

Централизованное управление настройками всех устройств Континент в сети: их политиками, правилами маршрутизации и фильтрации трафика.

Массовое развёртывание узлов безопасности.

Импорт политик со сторонних МСЭ/Миграция.

Планировщик обновлений.

Централизованная настройка и управление устройствами упрощает администрирование и аудит.

КОД безопасности

Система управления Континент 4

Мониторинг осуществляется из независимого от консоли управления веб-интерфейса.

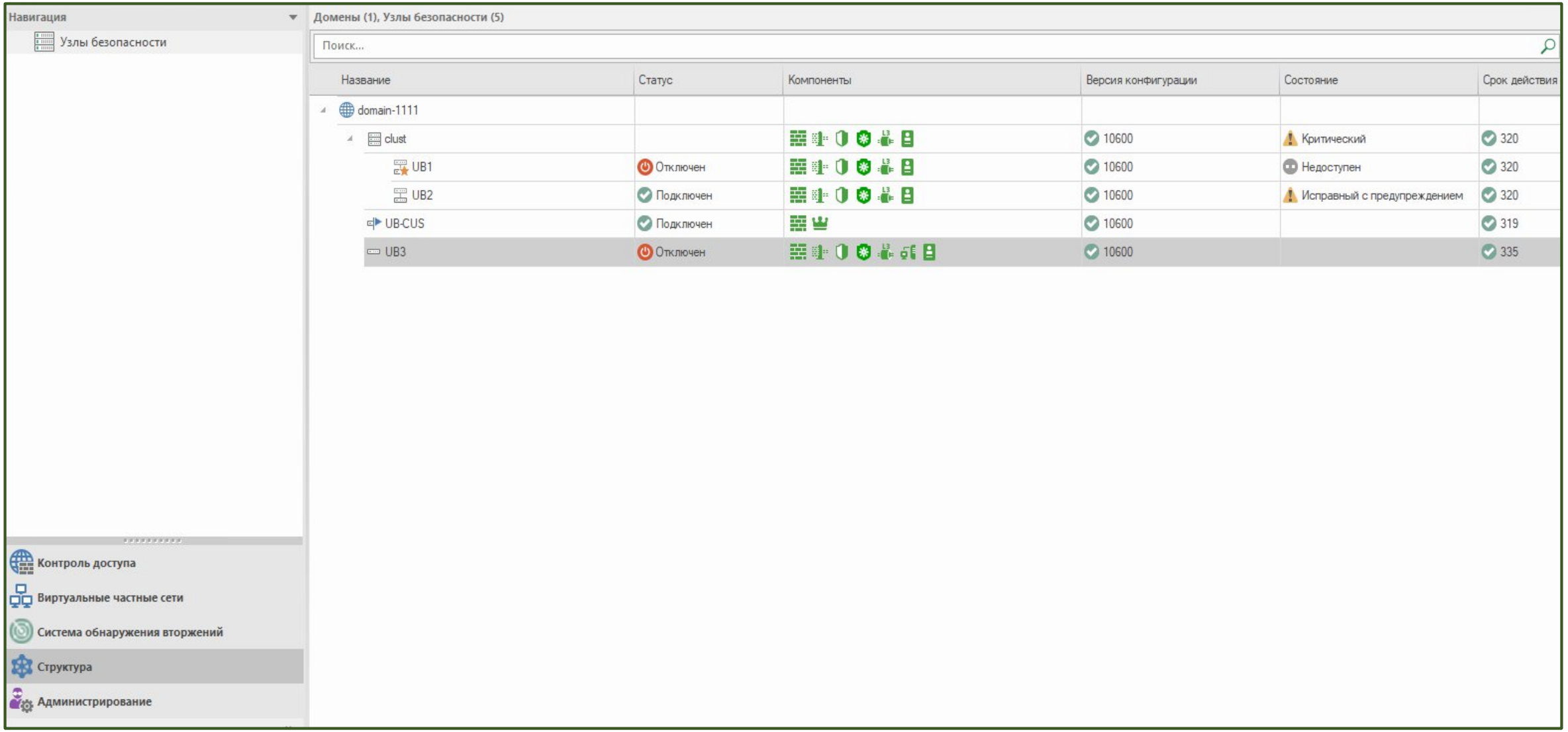
Отправка логов в сторонние системы для анализа по протоколам syslog, NetFlow, SNMP.

Получение оповещений об установке политик.

Мониторинг позволяет обеспечить быстрое реагирование на инциденты.

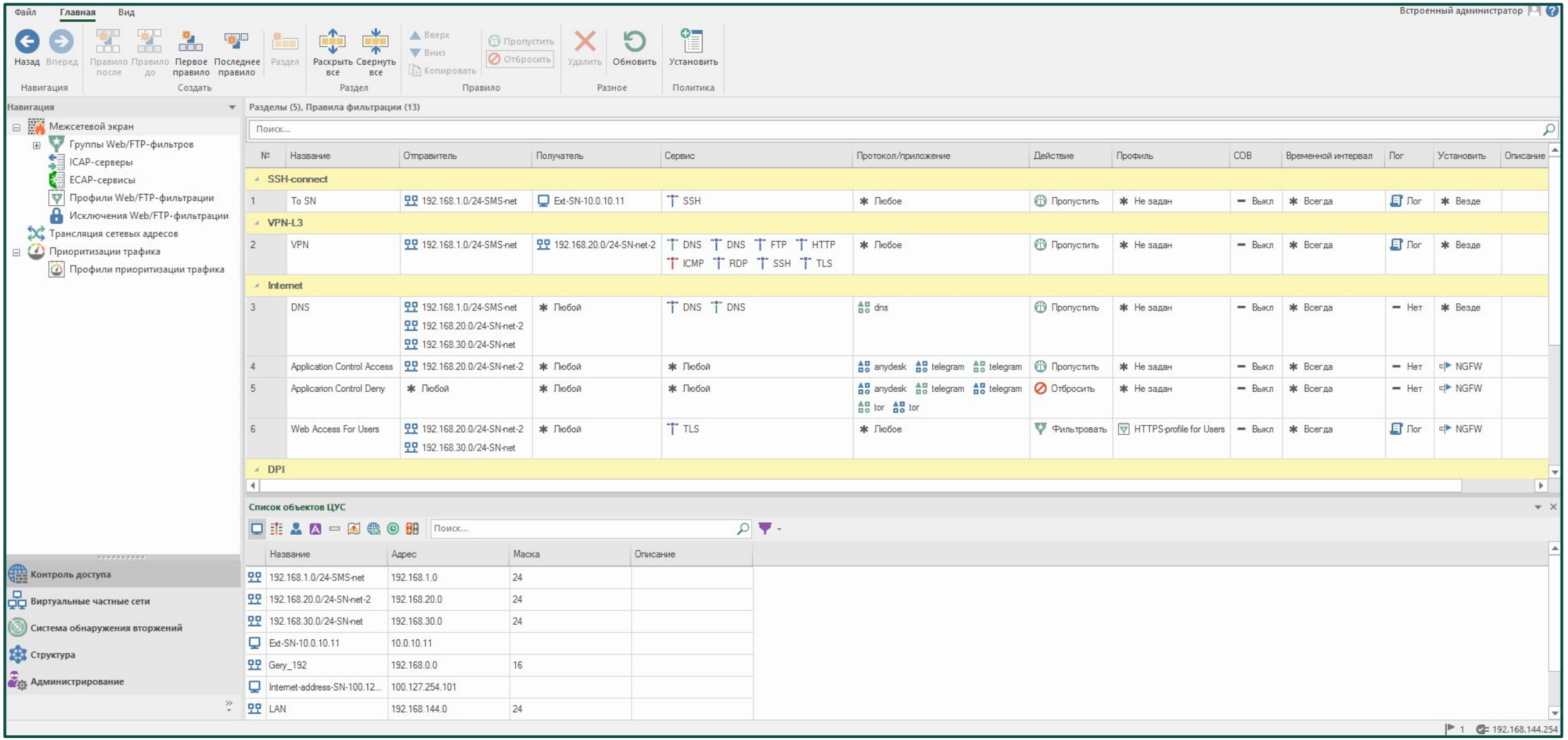
КОД безопасности

Интерфейс управления Континент 4



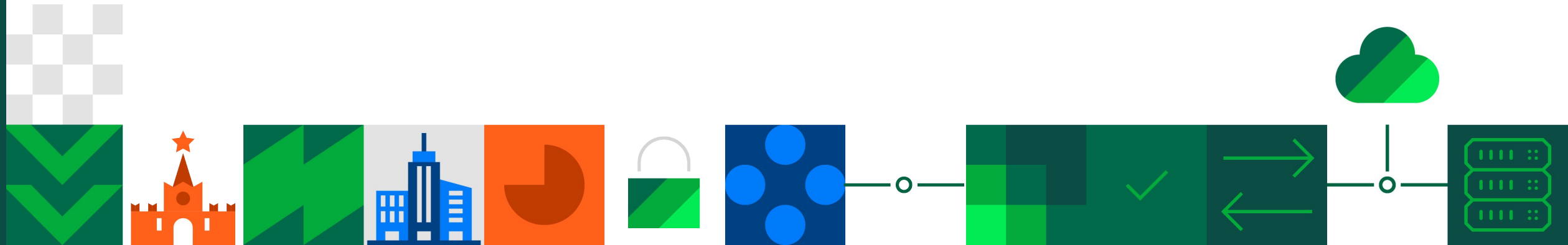
КОД безопасности

Интерфейс управления Континент 4



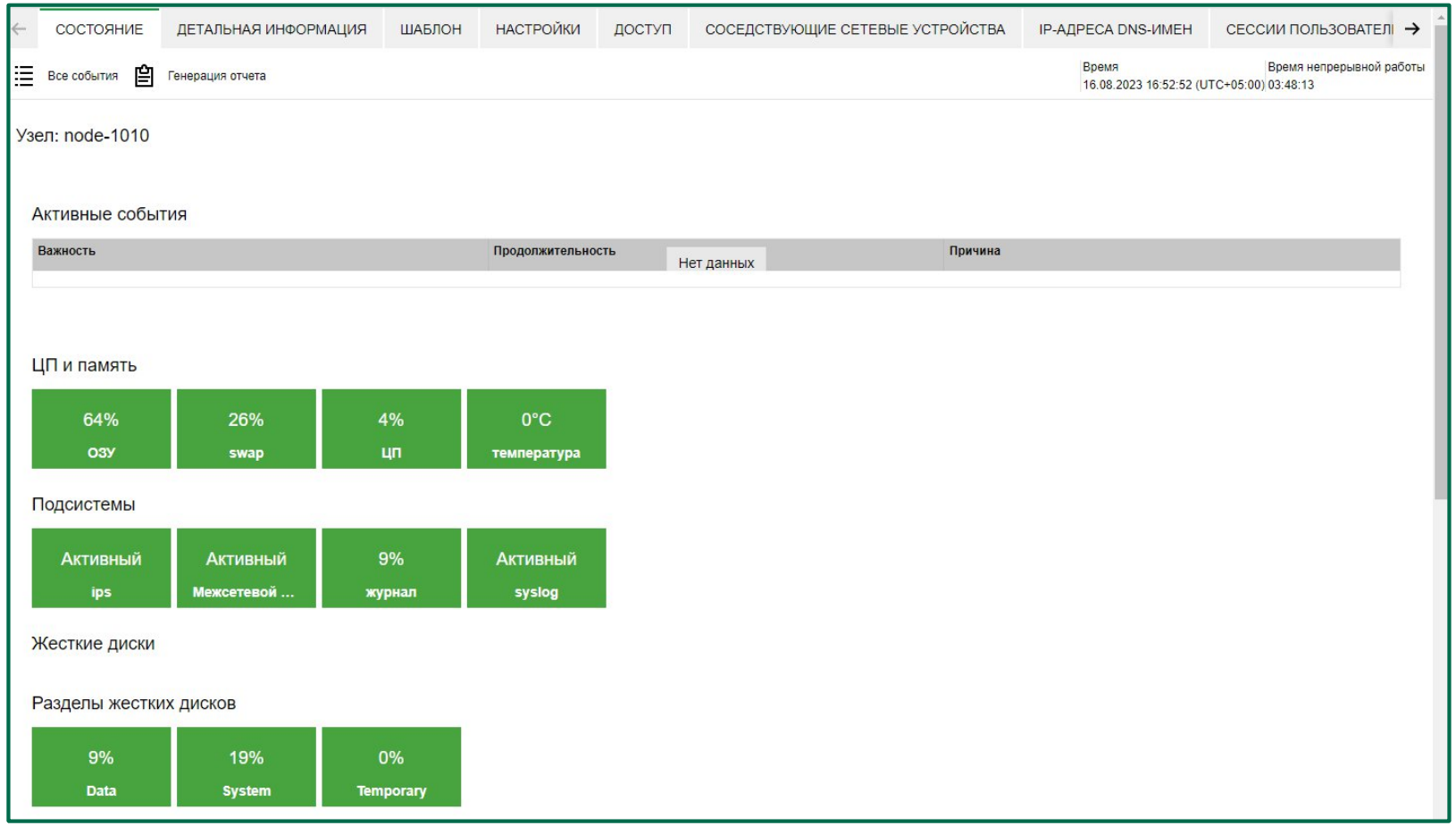
КОД безопасности

Мониторинг



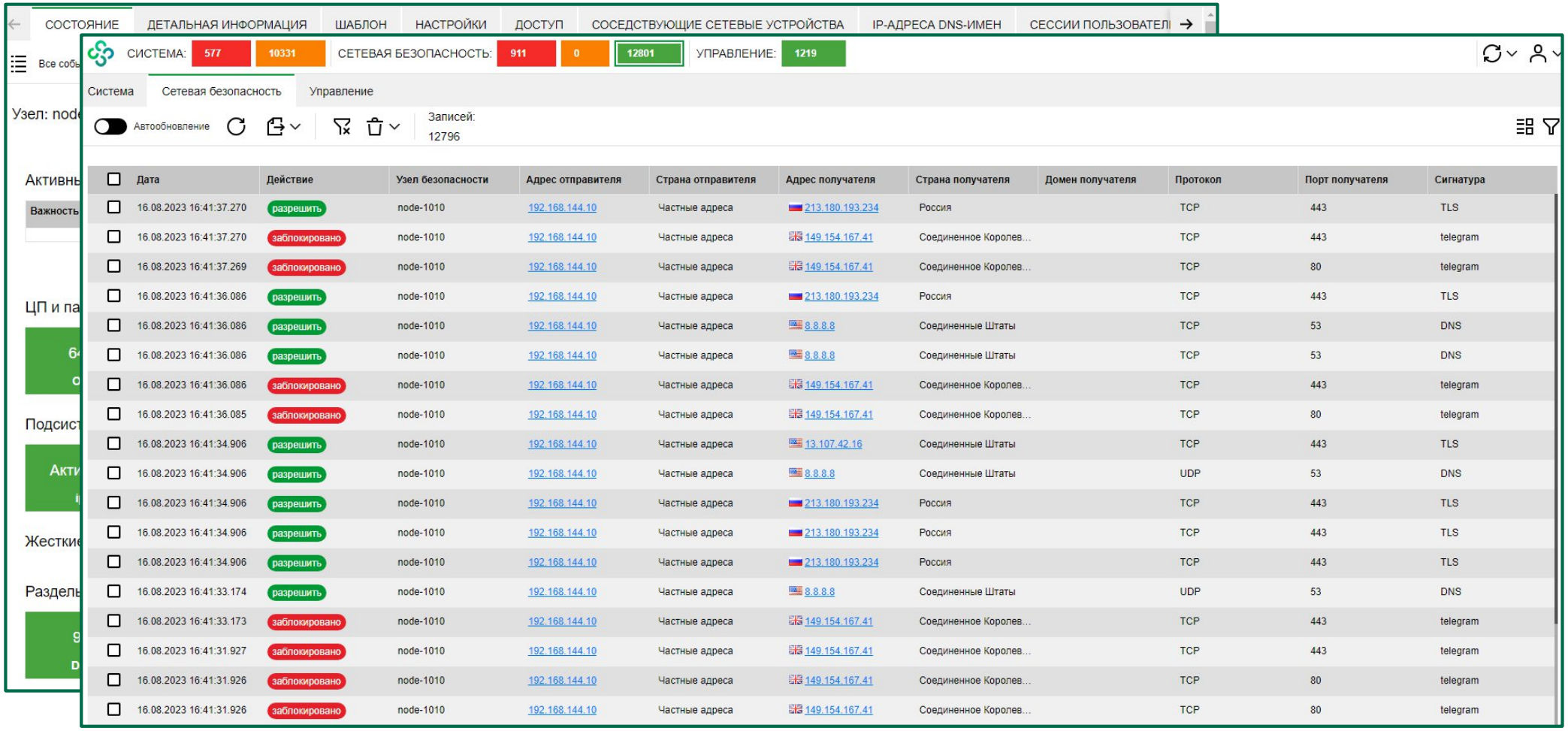
КОД безопасности

Мониторинг в Континент 4



КОД безопасности

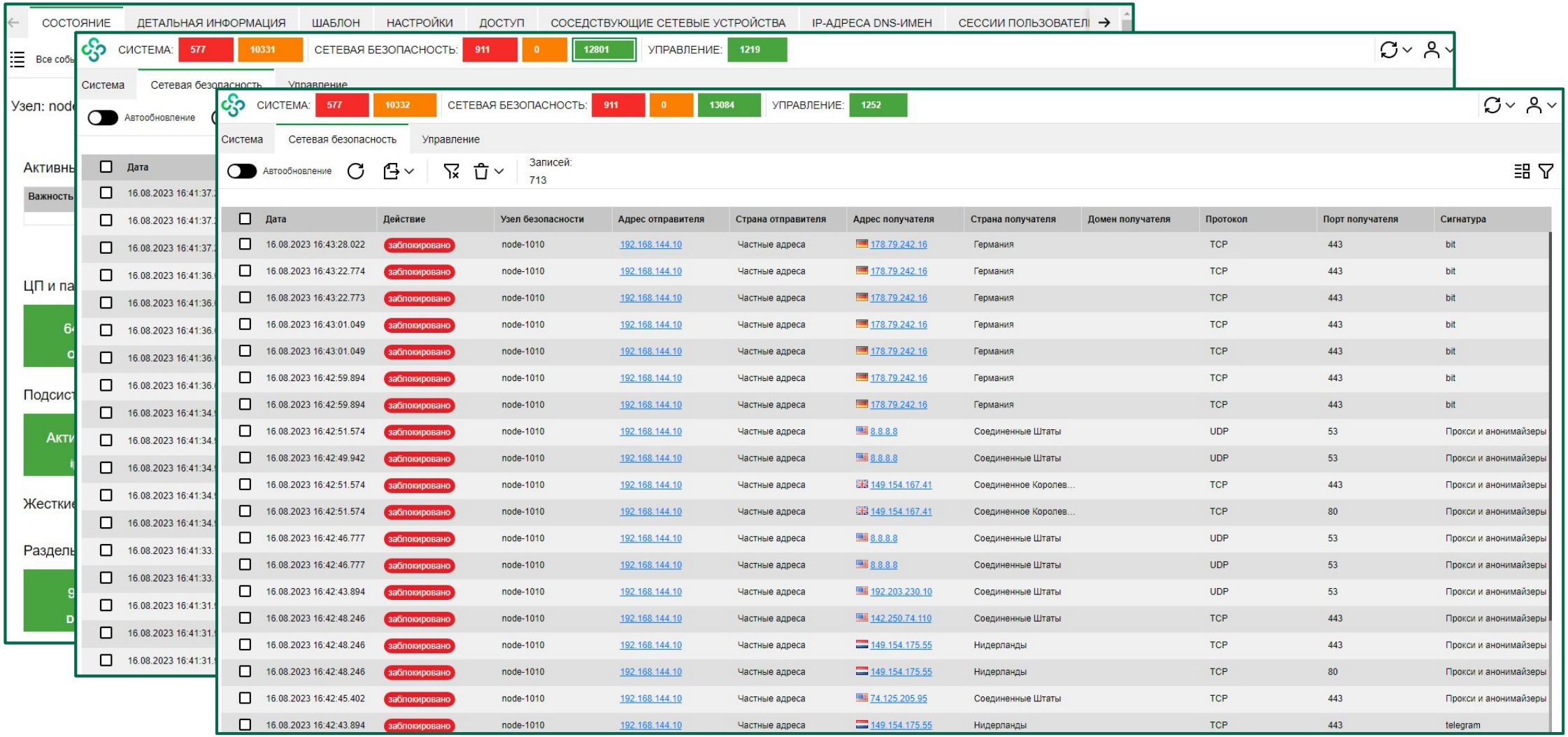
Мониторинг в Континент 4



Дата	Действие	Узел безопасности	Адрес отправителя	Страна отправителя	Адрес получателя	Страна получателя	Домен получателя	Протокол	Порт получателя	Сигнатура
16.08.2023 16:41:37.270	разрешить	node-1010	192.168.144.10	Частные адреса	213.180.193.234	Россия		TCP	443	TLS
16.08.2023 16:41:37.270	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.167.41	Соединенное Королев...		TCP	443	telegram
16.08.2023 16:41:37.269	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.167.41	Соединенное Королев...		TCP	80	telegram
16.08.2023 16:41:36.086	разрешить	node-1010	192.168.144.10	Частные адреса	213.180.193.234	Россия		TCP	443	TLS
16.08.2023 16:41:36.086	разрешить	node-1010	192.168.144.10	Частные адреса	8.8.8.8	Соединенные Штаты		TCP	53	DNS
16.08.2023 16:41:36.086	разрешить	node-1010	192.168.144.10	Частные адреса	8.8.8.8	Соединенные Штаты		TCP	53	DNS
16.08.2023 16:41:36.086	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.167.41	Соединенное Королев...		TCP	443	telegram
16.08.2023 16:41:36.085	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.167.41	Соединенное Королев...		TCP	80	telegram
16.08.2023 16:41:34.906	разрешить	node-1010	192.168.144.10	Частные адреса	13.107.42.16	Соединенные Штаты		TCP	443	TLS
16.08.2023 16:41:34.906	разрешить	node-1010	192.168.144.10	Частные адреса	8.8.8.8	Соединенные Штаты		UDP	53	DNS
16.08.2023 16:41:34.906	разрешить	node-1010	192.168.144.10	Частные адреса	213.180.193.234	Россия		TCP	443	TLS
16.08.2023 16:41:34.906	разрешить	node-1010	192.168.144.10	Частные адреса	213.180.193.234	Россия		TCP	443	TLS
16.08.2023 16:41:34.906	разрешить	node-1010	192.168.144.10	Частные адреса	213.180.193.234	Россия		TCP	443	TLS
16.08.2023 16:41:33.174	разрешить	node-1010	192.168.144.10	Частные адреса	8.8.8.8	Соединенные Штаты		UDP	53	DNS
16.08.2023 16:41:33.173	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.167.41	Соединенное Королев...		TCP	443	telegram
16.08.2023 16:41:31.927	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.167.41	Соединенное Королев...		TCP	443	telegram
16.08.2023 16:41:31.926	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.167.41	Соединенное Королев...		TCP	80	telegram
16.08.2023 16:41:31.926	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.167.41	Соединенное Королев...		TCP	80	telegram

КОД безопасности

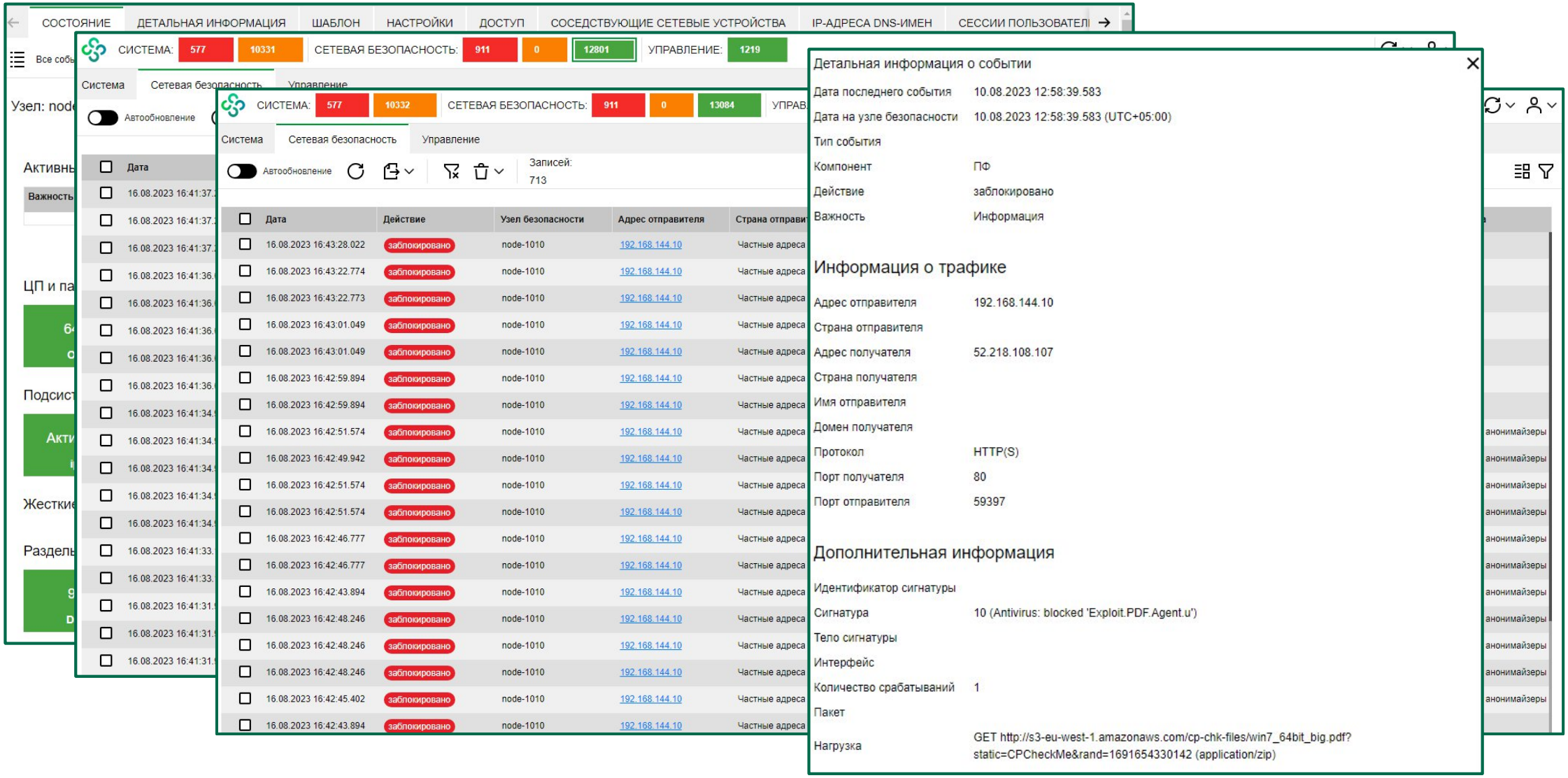
Мониторинг в Континент 4



Дата	Действие	Узел безопасности	Адрес отправителя	Страна отправителя	Адрес получателя	Страна получателя	Домен получателя	Протокол	Порт получателя	Сигнатура
16.08.2023 16:43:28.022	заблокировано	node-1010	192.168.144.10	Частные адреса	178.79.242.16	Германия		TCP	443	bit
16.08.2023 16:43:22.774	заблокировано	node-1010	192.168.144.10	Частные адреса	178.79.242.16	Германия		TCP	443	bit
16.08.2023 16:43:22.773	заблокировано	node-1010	192.168.144.10	Частные адреса	178.79.242.16	Германия		TCP	443	bit
16.08.2023 16:43:01.049	заблокировано	node-1010	192.168.144.10	Частные адреса	178.79.242.16	Германия		TCP	443	bit
16.08.2023 16:43:01.049	заблокировано	node-1010	192.168.144.10	Частные адреса	178.79.242.16	Германия		TCP	443	bit
16.08.2023 16:42:59.894	заблокировано	node-1010	192.168.144.10	Частные адреса	178.79.242.16	Германия		TCP	443	bit
16.08.2023 16:42:59.894	заблокировано	node-1010	192.168.144.10	Частные адреса	178.79.242.16	Германия		TCP	443	bit
16.08.2023 16:42:51.574	заблокировано	node-1010	192.168.144.10	Частные адреса	8.8.8.8	Соединенные Штаты		UDP	53	Прокси и анонимайзеры
16.08.2023 16:42:49.942	заблокировано	node-1010	192.168.144.10	Частные адреса	8.8.8.8	Соединенные Штаты		UDP	53	Прокси и анонимайзеры
16.08.2023 16:42:51.574	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.167.41	Соединенное Королев...		TCP	443	Прокси и анонимайзеры
16.08.2023 16:42:51.574	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.167.41	Соединенное Королев...		TCP	80	Прокси и анонимайзеры
16.08.2023 16:42:46.777	заблокировано	node-1010	192.168.144.10	Частные адреса	8.8.8.8	Соединенные Штаты		UDP	53	Прокси и анонимайзеры
16.08.2023 16:42:46.777	заблокировано	node-1010	192.168.144.10	Частные адреса	8.8.8.8	Соединенные Штаты		UDP	53	Прокси и анонимайзеры
16.08.2023 16:42:43.894	заблокировано	node-1010	192.168.144.10	Частные адреса	192.203.230.10	Соединенные Штаты		UDP	53	Прокси и анонимайзеры
16.08.2023 16:42:48.246	заблокировано	node-1010	192.168.144.10	Частные адреса	142.250.74.110	Соединенные Штаты		TCP	443	Прокси и анонимайзеры
16.08.2023 16:42:48.246	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.175.55	Нидерланды		TCP	443	Прокси и анонимайзеры
16.08.2023 16:42:48.246	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.175.55	Нидерланды		TCP	80	Прокси и анонимайзеры
16.08.2023 16:42:45.402	заблокировано	node-1010	192.168.144.10	Частные адреса	74.125.205.95	Соединенные Штаты		TCP	443	Прокси и анонимайзеры
16.08.2023 16:42:43.894	заблокировано	node-1010	192.168.144.10	Частные адреса	149.154.175.55	Нидерланды		TCP	443	telegram

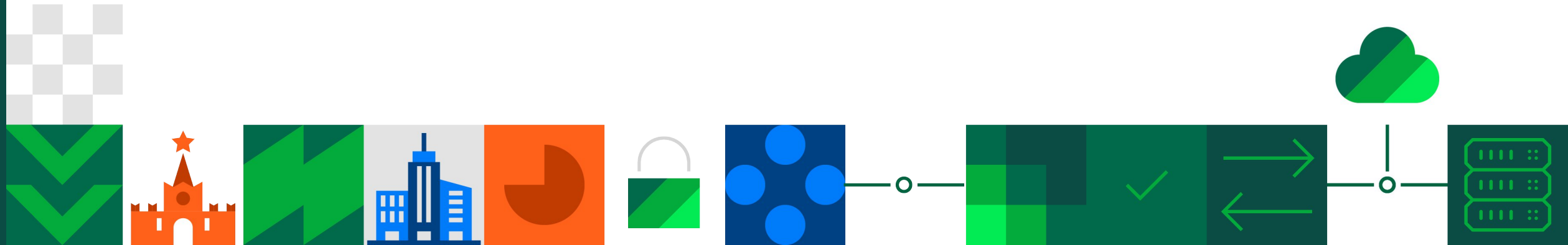
КОД безопасности

Мониторинг в Континент 4



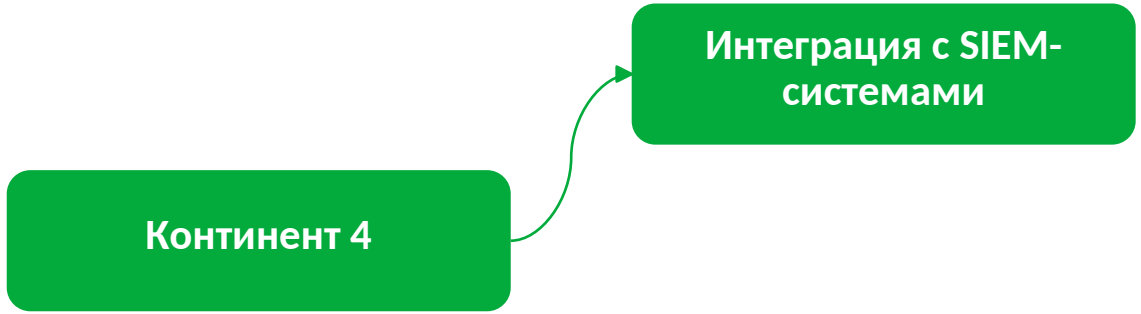
КОД безопасности

Интеграции



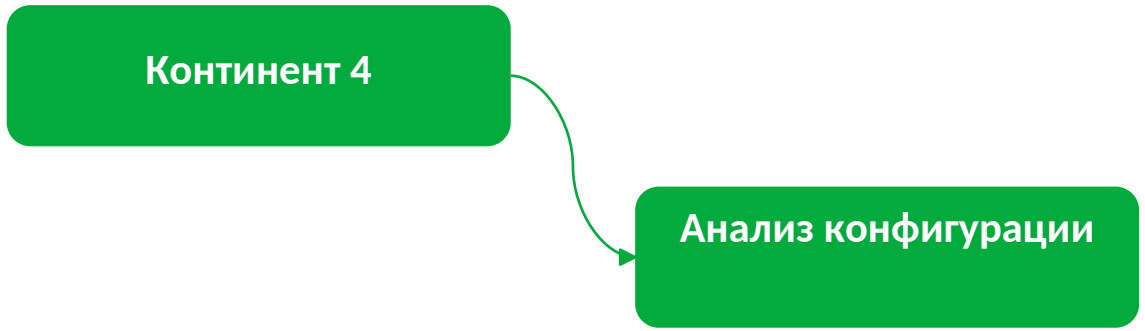
КОД безопасности

Интеграции



- Протестированное взаимодействие:
  1. RuSIEM
  2. Kaspersky Unified Monitoring and Analysis Platform
  3. MaxPatrol SIEM
  4. KOMRAD Enterprise SIEM
- Решение задач:
  1. Контроль сетевого трафика
  2. Поиск и обнаружение инцидентов ИБ

Интеграции



- Интеграция с Efros DefOps
- Решение задач:
  1. Контроль всех получаемых конфигураций
  2. Информирование о наличие теневых, избыточных и неиспользуемых правил
  3. Создание стандартов безопасности для проверки необходимых правил МСЭ

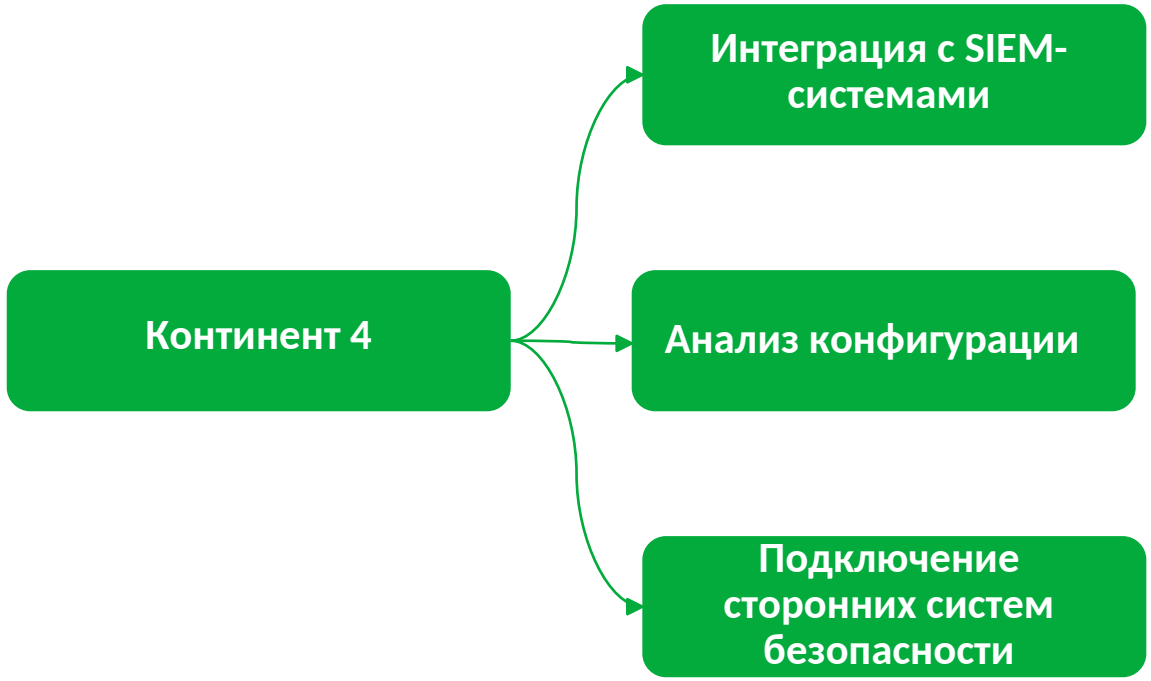
Интеграции

Континент 4

Подключение сторонних систем безопасности

- Интеграция с песочницами, сторонними антивирусами, DLP для повышения уровня безопасности
- Организация высокопроизводительных ферм МСЭ через интеграцию с брокерами сетевых пакетов DS Integrity

Технологическое преимущество



- Отличительная особенность уникального функционала в сравнении с конкурентами – данный функционал **отсутствует у конкурентов или реализован в меньшей степени**
- Отличительная особенность интеграций в сравнении с конкурентами – **все интеграции протестированы и имеются рекомендации по настройкам** как со стороны Кода Безопасности, так и со стороны партнеров

КОД безопасности

Технологические партнеры

Многофакторная аутентификация:

MULTIFACTOR

Avanpost

КОМПАНИЯ ИНДИД

Сакура

Аладдин

Балансировка нагрузки:

ЦИФРОВЫЕ РЕШЕНИЯ

RDP

Анализ правил:

EFROS DEFENCE OPERATIONS

Нетхаб

URL-категории:

SkyDNS

Песочницы:

positive technologies

kaspersky

AVSOFT

Threat Intelligence платформы:

Security Vision

R-Vision

Источники индикаторов компрометации:

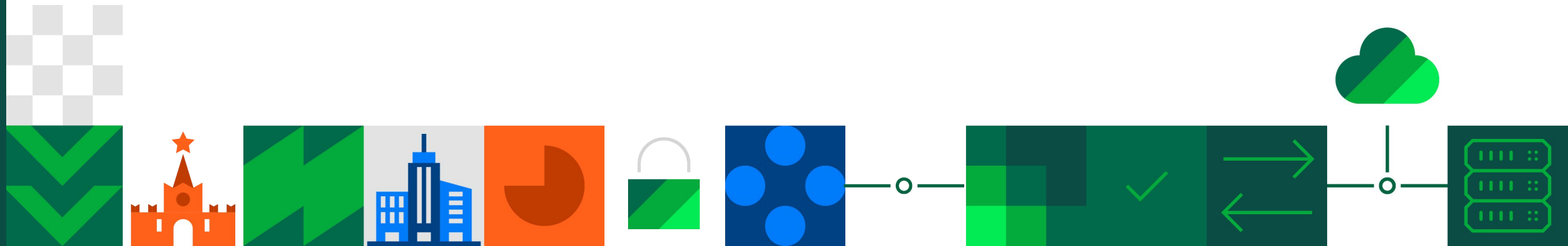
kaspersky

CyberThreatTech

Будет в первом полугодии 2024

КОД безопасности

Миграция с иностранных NGFW на Континент 4



Автоматизация миграции

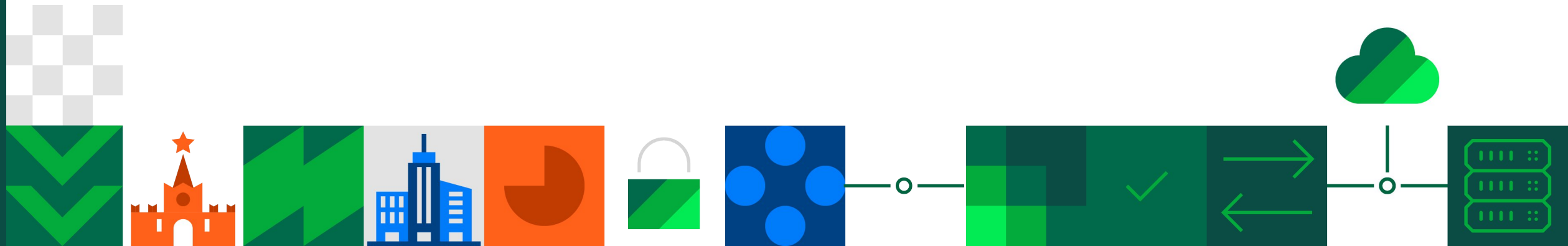
Автоматизированные инструменты миграции:

- Миграция с Check Point
- Миграция с FortiGate
- Миграция с Cisco
- Миграция с Palo Alto, Juniper через промежуточный импорт в Check Point

Репозиторий – https://github.com/itseccode/c4_tools
Телеграм бот – https://t.me/STEPLOGIC_NetCalc_bot

КОД безопасности

Преимущества работы с Кодом Безопасности



КОД безопасности

Преимущества работы с Кодом Безопасности

Опыт защиты сетей федерального уровня

NGFW, VPN и удаленный доступ в одном устройстве

Концепция централизованного управления

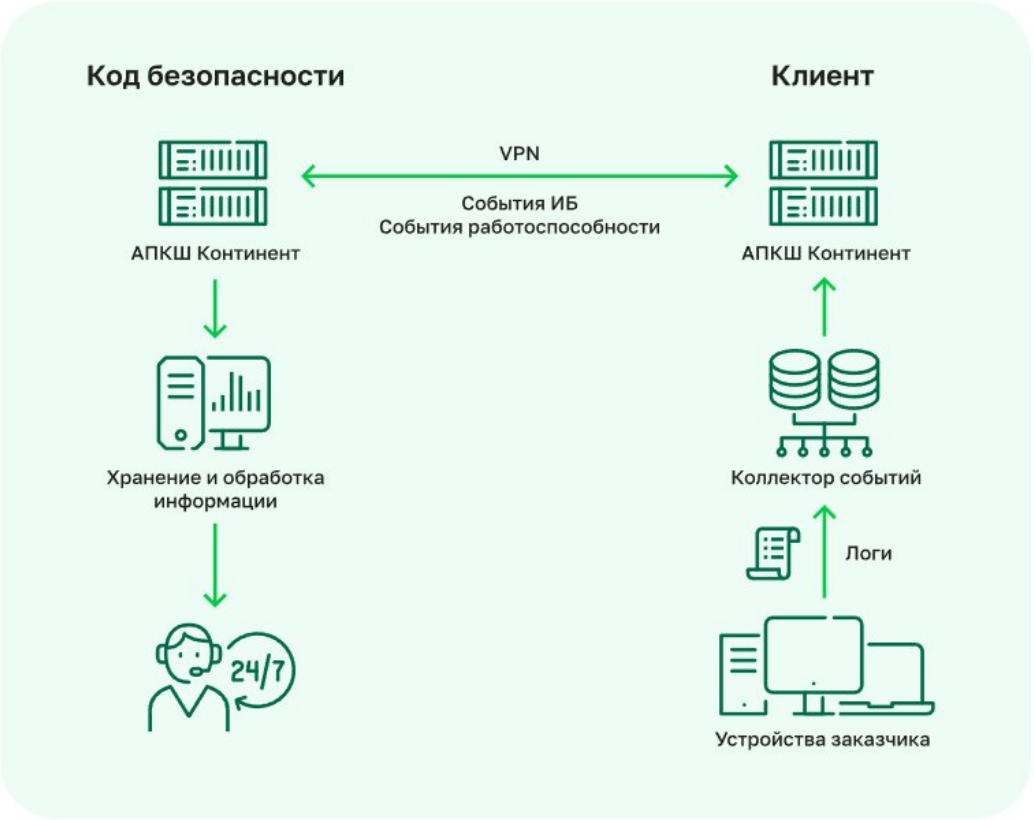
Техническая поддержка и профессиональные сервисы

Широкий выбор платформ под разные задачи

КОД безопасности

Стабильность функционирования

1. Выпуск новых версий только после детального тестирования
2. Развитая техническая поддержка и комьюнити:
   - 14 минут – среднее время реакции на запрос
   - 4,9 – средняя оценка качества работы ТП
   - 2300 – разрешаемых инцидентов в месяц
   - Мониторинг событий и инцидентов ИБ через подключение к Центру мониторинга «Кода Безопасности»
   - Телеграм-чат, в котором эксперты обсуждают и помогают решать проблемы при эксплуатации комплекса
3. Отказоустойчивость и резервирование каналов связи



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 России.**
- Технологии защиты обеспечивают безопасность **3 000 000 компьютеров** в **90 000 организаций.**
- **3 центра разработки:** Москва, Санкт-Петербург, Пенза.
- Более **600 квалифицированных специалистов**, имеющих уникальные компетенции.
- Более **50 разработанных СЗИ и СКЗИ**.
- Более **60 действующих сертификатов** соответствия подтверждают высокое качество продуктов.
- Партнерская сеть компании насчитывает более **1000 авторизованных партнеров.**

Компетентность «Кода Безопасности» подтверждена независимыми аналитиками:

- «Крупнейшие производители высокотехнологичного оборудования»: №1 («Эксперт РА»), №3 («Коммерсант»).
- «Крупнейшие разработчики программного обеспечения»: №7 («Эксперт РА»), №9 («Коммерсант»).
- «Крупнейшие ИТ-компании России»: №30 («Коммерсант»), №47 (TAdviser).

КОД безопасности

Нам доверяют

Государственные организации:

- Федеральное казначейство России
- Федеральная налоговая служба России
- Федеральная таможенная служба России
- Федеральный Фонд обязательного медицинского страхования
- Центральная избирательная комиссия Российской Федерации
- Министерство юстиции Российской Федерации

Силовые структуры:

- Министерство внутренних дел Российской Федерации
- Министерство обороны Российской Федерации
- Федеральная служба безопасности Российской Федерации
- Федеральная служба охраны Российской Федерации

Телекоммуникационные компании:

- ПАО «Ростелеком»
- ПАО «МГТС»
- ГК «АКАДО Телеком»
- АО «Военителеком»

Финансовые организации:

- ПАО «Сбербанк»
- Центральный банк Российской Федерации
- ГК «Внешэкономбанк»
- АО «Газпромбанк»
- ПАО «Промсвязьбанк»
- Банк ВТБ (ПАО)
- ПАО «Московский кредитный банк»
- АО «АЛЬФА-БАНК»

Промышленные предприятия:

- ГК «Ростех»
- АО «Российские космические системы»
- ПАО «ГМК «Норильский никель»

Предприятия ТЭК:

- ГК «Росатом»
- ПАО «Газпром»
- ПАО «АК «Транснефть»
- ПАО «НК «Роснефть»»
- ПАО «Россети»

КОД безопасности

Подробнее

Большой онлайн по Континент 4

Телеграм канал Код на проводе

Телеграм чат по Континенту

КОД безопасности

Спасибо за внимание!

Щур Василий – Представитель по развитию продаж в Республике Беларусь
v.shchur@securitycode.ru

Горбик Евгений - Инженер
e.gorbyk@securitycode.ru

KeyProjects@securitycode.ru
www.securitycode.ru