



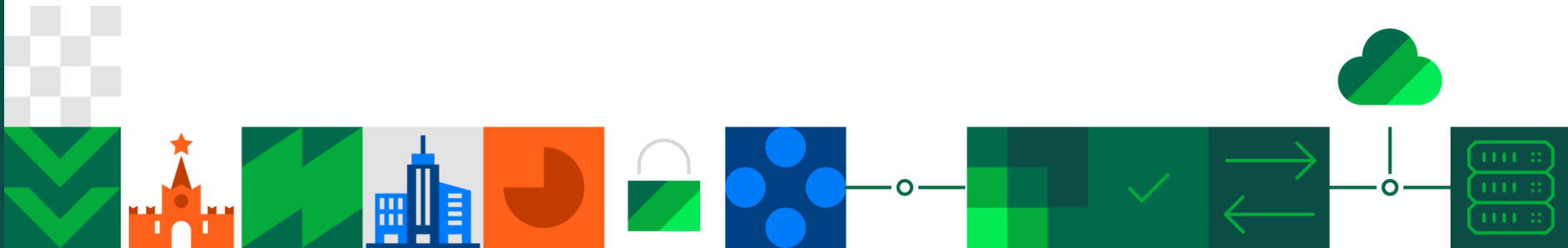
# Континент 3

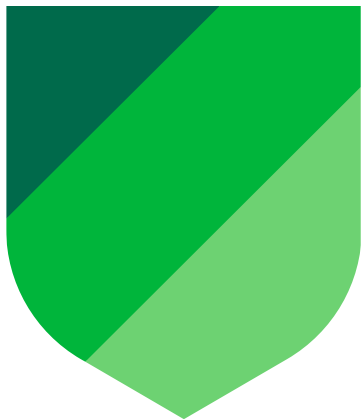
---





# О продукте



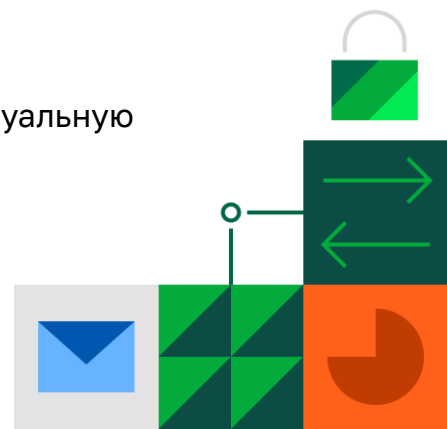


### Континент 3.9

Централизованный комплекс для защиты сетевой инфраструктуры и создания VPN-сетей с использованием алгоритмов ГОСТ

### Предназначен для решения следующих задач:

- ✓ Криптографическая защита информации, передаваемой по открытым каналам связи
- ✓ Объединение филиалов организации в виртуальную частную сеть (VPN)
- ✓ Централизованная защита периметра корпоративной сети
- ✓ Защищенный удаленный доступ
- ✓ Обнаружение вторжений





## ФСТЭК России

- 3-й класс защиты МЭ типа «А»
- 3-й класс защиты СОВ уровня сети
- 3-й уровень доверия

## ФСБ России

- СКЗИ класса КС2/КС3
- Межсетевой экран 4 класса

## Сертифицирован для защиты

- КИИ до 1 категории включительно
- ГИС до 1 класса защищенности включительно
- ИСПДн до класса УЗ1 включительно
- АС до класса 1Г включительно





## Криптошлюз

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



## Криптокоммутатор

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



## Детектор атак

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



## Центр управления сетью

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов Континент 3.



## СКЗИ Континент АП

VPN-клиент для подключения персональных компьютеров на базе Windows и Linux к Серверу доступа.



## Сервер доступа

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



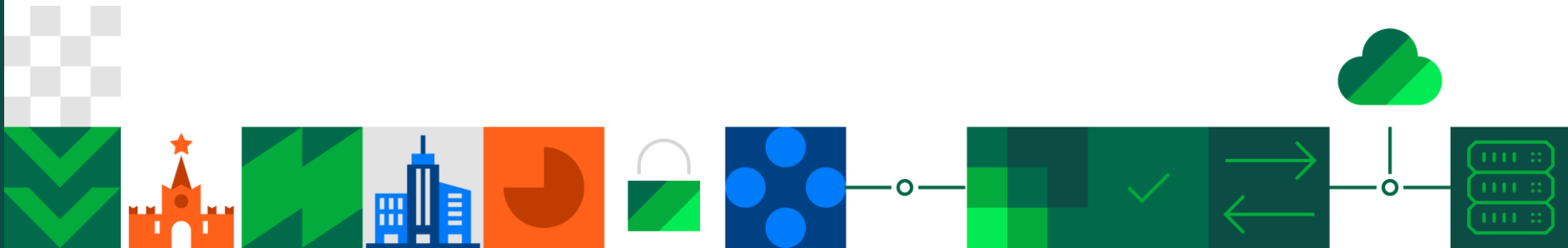
## СКЗИ Континент АП

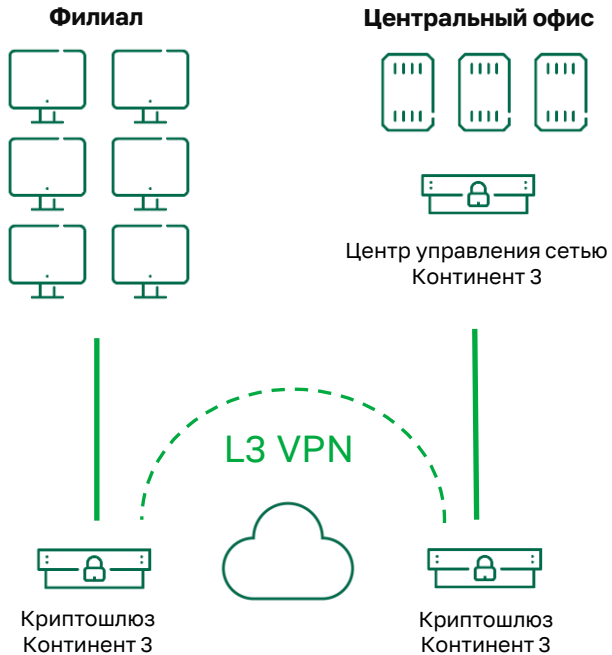
VPN-клиент для подключения мобильных устройств на базе Android, iOS/iPadOS и ОС Аврора к Серверу доступа.



# Варианты применения

---





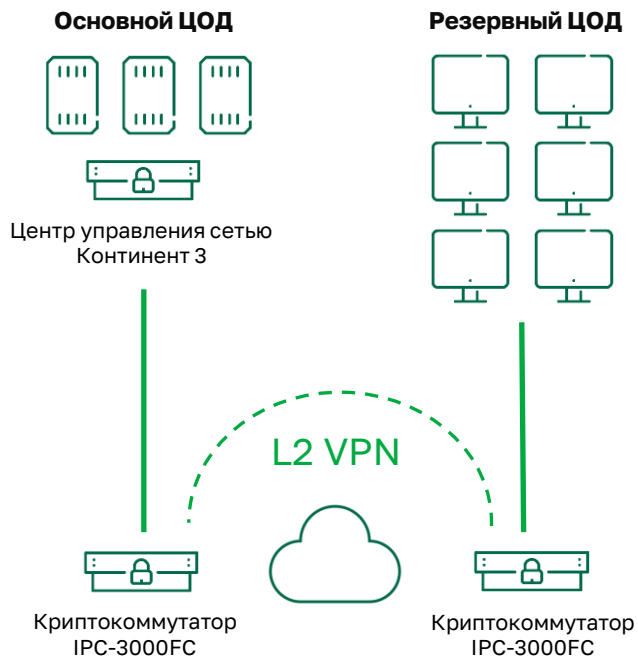
## Задачи

- Защита доступа филиалов к ресурсам центрального офиса
- Защита трафика систем ВКС
- Подключение к СМЭВ
- Защита трафика ИСПДн, ГИС и СОПКА

## Компоненты

- Центр управления сетью
- Криптошлюз





## Задачи

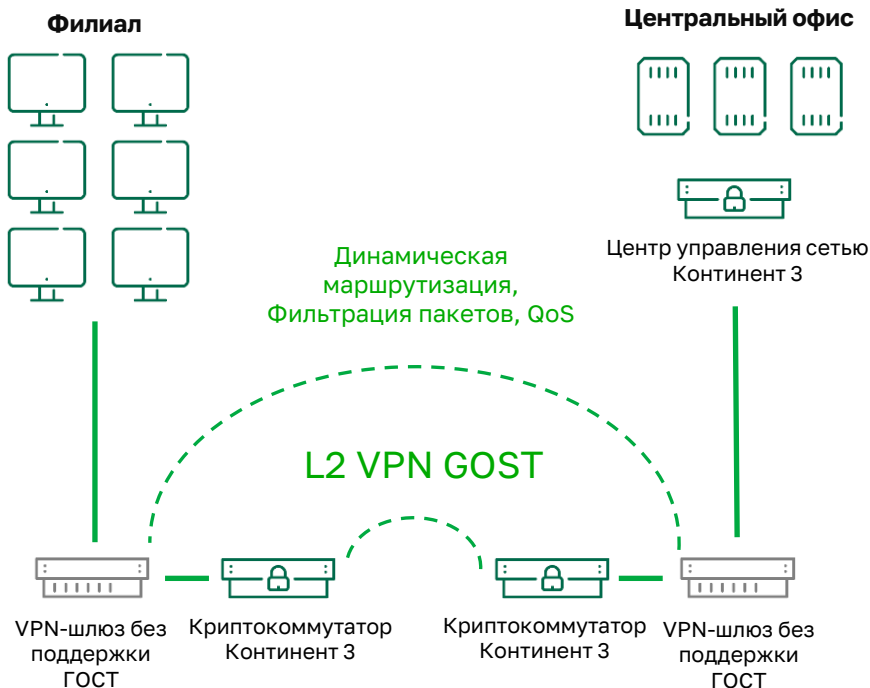
- Защита канала между основным и резервным ЦОД
  - Репликация СХД
  - Кластеризация серверов приложений
- Обеспечение низкой задержки и показателя Round Trip Time

## Компоненты

- Центр управления сетью
- Специализированный криптокоммутатор IPC-3000FC/3000FC-H/3000FC-40G







## Задачи

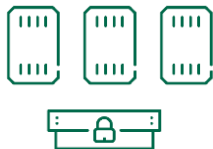
- Развертывание VPN ГОСТ на существующей VPN-сети
- «VPN ГОСТ как услуга» для клиентов операторов связи

## Компоненты

- Центр управления сетью
- Криптокоммутатор



## Критичный сегмент сети



Центр управления сетью  
Континент3



Коммутатор, маршрутизатор  
или межсетевой экран



Детектор атак  
Континент 3

Сегмент сети с низким  
уровнем защиты



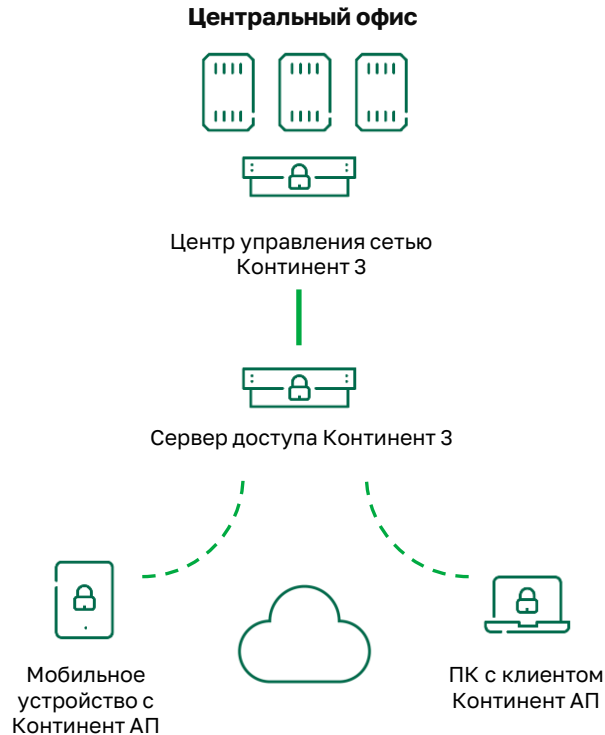
## Задачи

- Обнаружение сетевых угроз
- Выполнение требований приказов ФСТЭК России
  - Приказ №21 (Защита ИСПДн)
  - Приказ №17 (Защита ГИС)
  - Приказ №239 (Защита КИИ)

## Компоненты

- Центр управления сетью
- Детектор атак





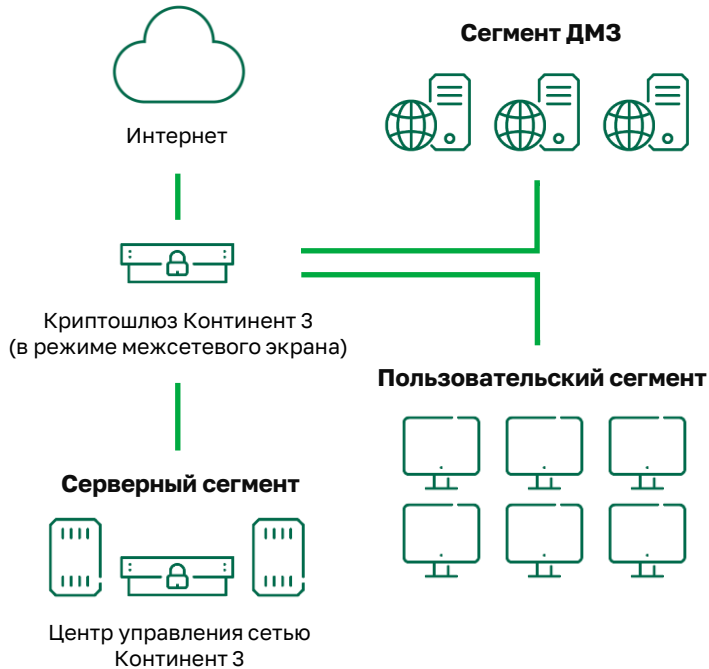
## Задачи

- Защищенный доступ к корпоративным ресурсам
  - С компьютеров
  - С мобильных устройств
- Защищенный доступ к терминальным серверам/VDI

## Компоненты

- Центр управления сетью
- Сервер доступа
- VPN-клиент Континент АП





## Задачи

- Защита периметра сети
  - Контроль сетевых приложений
  - URL - фильтрация
- Единая база правил фильтрации и сетевых объектов для всех межсетевых экранов

## Компоненты

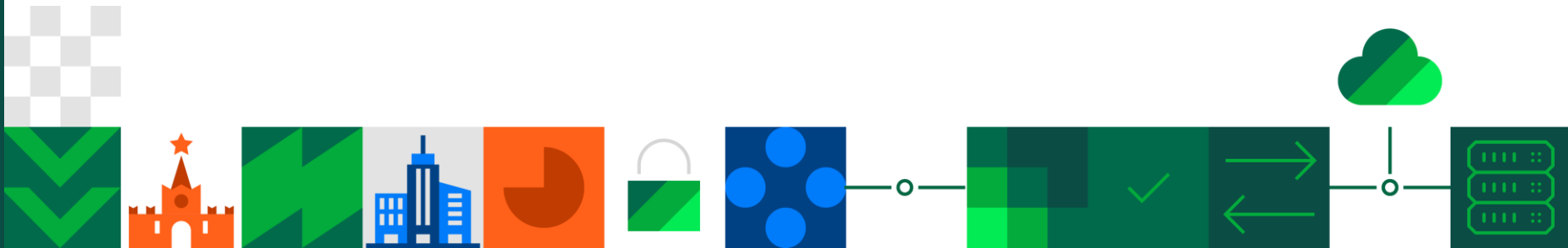
- Центр управления сетью
- Криптошлюз (в режиме межсетевого экрана)

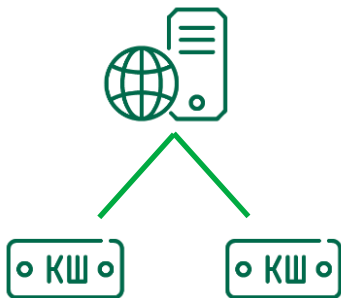




# Компоненты

---





## Центр управления сетью

Аппаратно-программный комплекс,  
предназначенный для управления и  
мониторинга состояния компонентов  
Континент 3

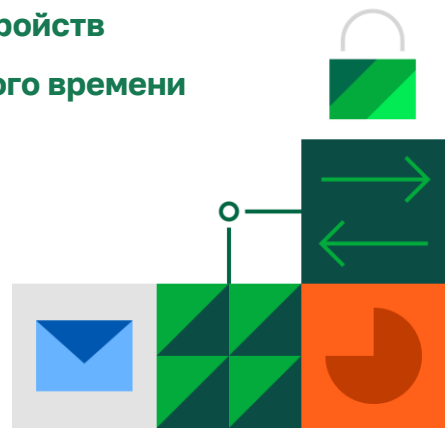
### Централизованное управление

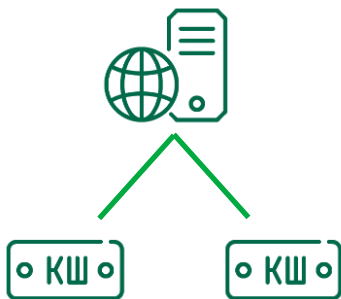
- Узлами сети
- Настройками маршрутизации
- Правилами фильтрации трафика
- VPN - связями
- Криптографическими ключами
- Параметрами SNMP

### Централизованное обновление ПО устройств

### Мониторинг событий в режиме реального времени

### Групповые операции над узлами





## Центр управления сетью

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов Континент 3

## Централизованный сбор и хранение журналов

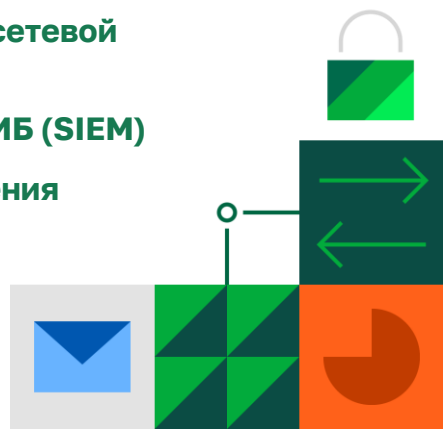
### Расширенная диагностика инфраструктуры

- Централизованный сбор отладочной информации узлов Континент 3
- Доступ к консоли узлов по протоколу SSH
- Удаленное создание локальных пользователей на узлах Континент 3

### Интеграция с системами мониторинга сетевой инфраструктуры (SNMP)

### Интеграция с системами мониторинга ИБ (SIEM)

### Отказоустойчивость серверов управления





## Криптошлюз

Аппаратно-программный комплекс,  
предназначенный для криптографической  
защиты трафика при его передаче  
на сетевом уровне

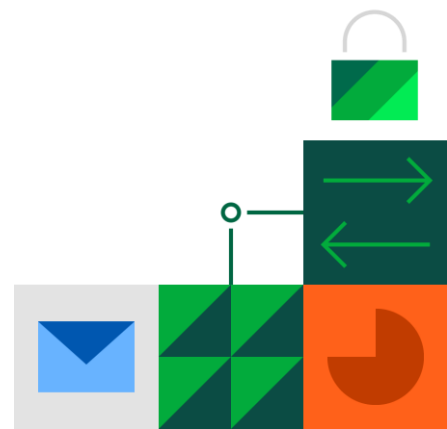
Детальный контроль HTTP и FTP

Инспекция внутри SSL-туннеля

Профили усиленной фильтрации

Идентификация и аутентификация пользователей

Поддержка технологии **Stateful Inspection**







## Криптошлюз

Аппаратно-программный комплекс,  
предназначенный для криптографической  
защиты трафика при его передаче  
на сетевом уровне

Поддержка QoS, ToS и Traffic shaping

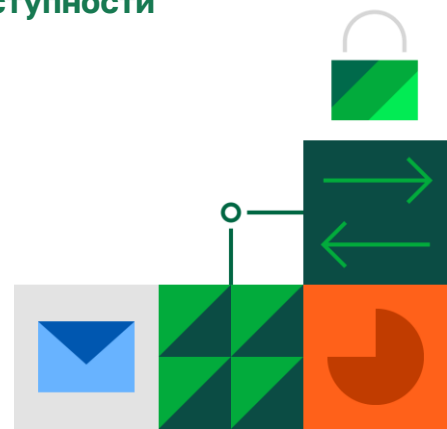
Резервирование каналов связи

Поддержка IPv6 для WAN

Поддержка Multicast-маршрутизации

Поддержка VLAN

Работа в режиме кластера высокой доступности





## Криптошлюз

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче на сетевом уровне

## Маршрутизация трафика

- Статическая
- Динамическая
  - RIP
  - OSPF
  - BGP

## Поддержка NAT

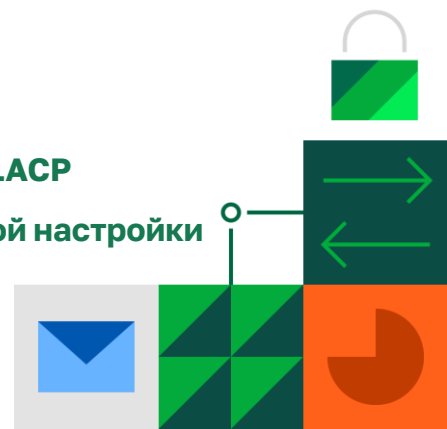
- Source NAT
- Destination NAT

## Возможность работы КШ за NAT

## Доступ к сети за несколькими КШ

## Агрегация интерфейсов по протоколу LACP

## Встроенный DHCP-сервер с поддержкой настройки provisioning server и DHCP-relay





## Криптокоммутатор

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче на канальном уровне

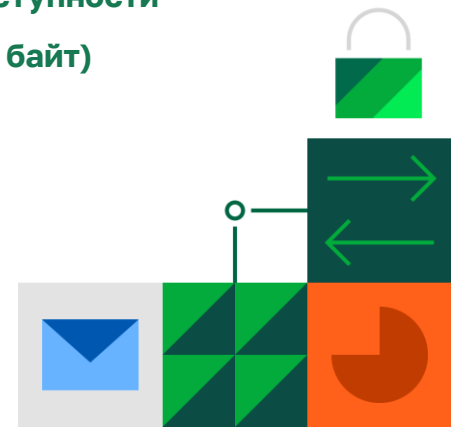
**Шифрование данных в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью**

**Алгоритм имитозащиты данных – ГОСТ 28147–89 в режиме выработки имитовставки**

**Работа в едином адресном пространстве**

**Работа в режиме кластера высокой доступности**

**Поддержка Jumbo-frame (MTU до 9000 байт)**





## Криптокоммутатор

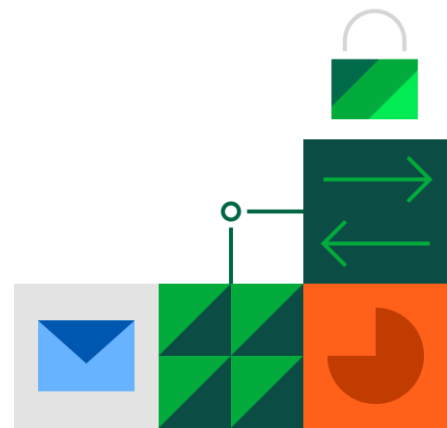
Аппаратно-программный комплекс,  
предназначенный для криптографической  
защиты трафика при его передаче на  
канальном уровне

Туннелирование MPLS-трафика

512 портов виртуального коммутатора

Линейное увеличение производительности

Классификация трафика по ToS





## Детектор атак

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

**Регулярное обновление сигнатур (базы решающих правил, БРП)**

**Сочетание сигнатурного и эвристического методов анализа трафика**

**Поддержка протоколов различных уровней**

- Транспортного уровня
- Сетевого уровня
- Сеансового уровня
- Прикладного уровня

**Автоматическое получение данных от ДА и создание правил блокировки трафика на КШ, работающих под управлением одного ЦУС**





## Сервер доступа    Континент АП

Аппаратно-программный комплекс и клиентское ПО, установленное на персональное устройство, предназначенные для криптографической защиты передаваемого трафика

**Клиентские приложения для всех популярных платформ**

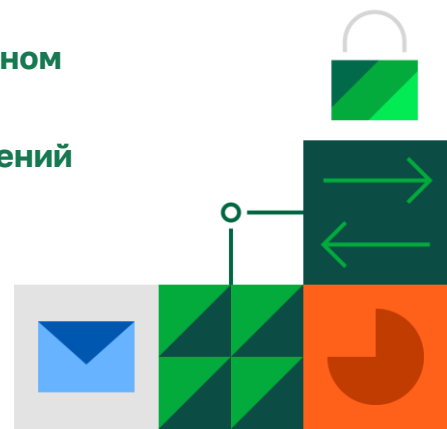
**Поддержка Сервером доступа аутентификации по сертификатам ГОСТ 2012 (TK26)**

**Поддержка различных ключевых носителей**

**Возможность установки VPN-соединения до регистрации пользователя в ОС**

**Объединённый TLS и VPN клиенты в одном инсталляторе**

**Режим запрета незащищенных соединений**



## Формфактор

Семейство специализированных аппаратных платформ для построения защищённого VPN-канала

## Производительность шифрования

20 Гбит/с  
40 Гбит/с

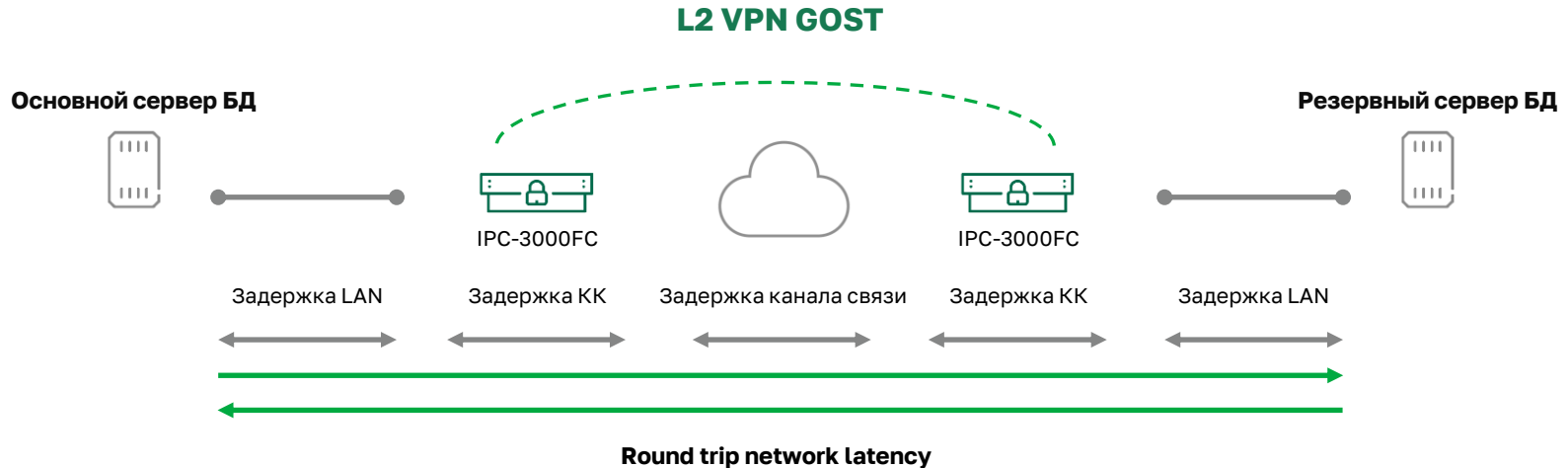
## Особенности

Минимизация задержек при передаче трафика  
На обычной платформе показатель задержки минимум в два раза больше, а чаще всего – на порядок

## Модельный ряд

IPC-3000FC  
IPC-3000FC-N  
IPC-3000FC-40G





## Round trip network latency

время затраченное на передачу пакета плюс время до получения пакета-подтверждения.

## Он состоит из:

- задержка криптокоммутатора
- задержка локальной сети
- задержка канала связи

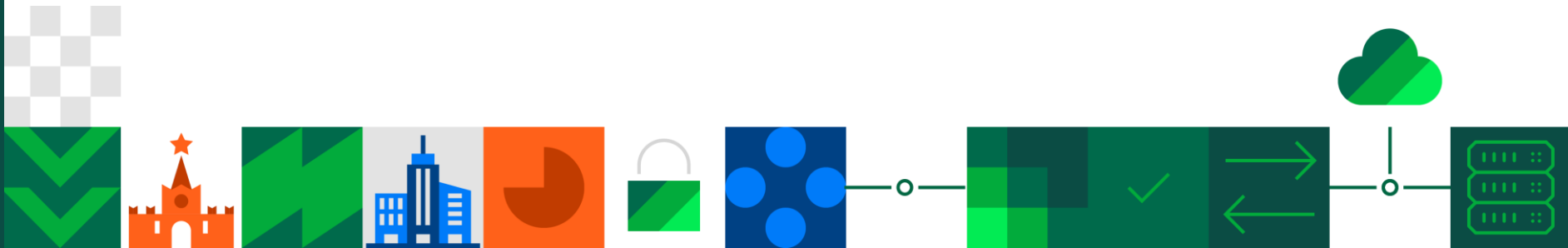
**Задержка криптокоммутатора должна минимально влиять на общую задержку передачи данных**





# О компании

---





### «Крупнейшие производители высокотехнологичного оборудования»



«Эксперт РА»



«Коммерсант»

### «Крупнейшие разработчики ПО»



«Эксперт РА»



«Коммерсант»

### «Крупнейшие ИТ-компании России»



«Коммерсант»



«TAdviser»

- ✓ Более **20 лет** на страже безопасности крупнейших предприятий России
- ✓ **9 лицензий** ФСТЭК, ФСБ и Минобороны России
- ✓ **3 центра разработки:** Москва, Санкт-Петербург, Пенза
- ✓ Более **400 квалифицированных специалистов R&D**, имеющих уникальные компетенции
- ✓ Более **50 разработанных СЗИ и СКЗИ**
- ✓ Более **60 сертификатов** соответствия
- ✓ Обеспечена безопасность **1 200 000 компьютеров** в **32 000 организаций**
- ✓ Партнерская сеть компании насчитывает более **1000 авторизованных партнеров**

## 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»



ФГУП «Почта России»



ГК «АКАДО Телеком»



АО «Воентелеком»

## Финансовые организации:



ПАО «Сбербанк»



Центральный банк Российской Федерации



ГК «Внешэкономбанк»



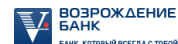
АО «Газпромбанк»



АО «Страховая группа МСК»



ПАО «VTB24»



ПАО «Банк «Возрождение»

## Промышленные предприятия:



ГК «Ростех»



АО «Российские космические системы»



ПАО «ГМК «Норильский никель»



ГКНПЦ им. М.В. Хруничева

## Предприятия ТЭК:



Государственная корпорация по атомной энергии «Росатом»



ПАО «Газпром»



ПАО «АК «Транснефть»



ПАО «НК «Роснефть»



# КОД безопасности

info@securitycode.ru  
www.securitycode.ru

