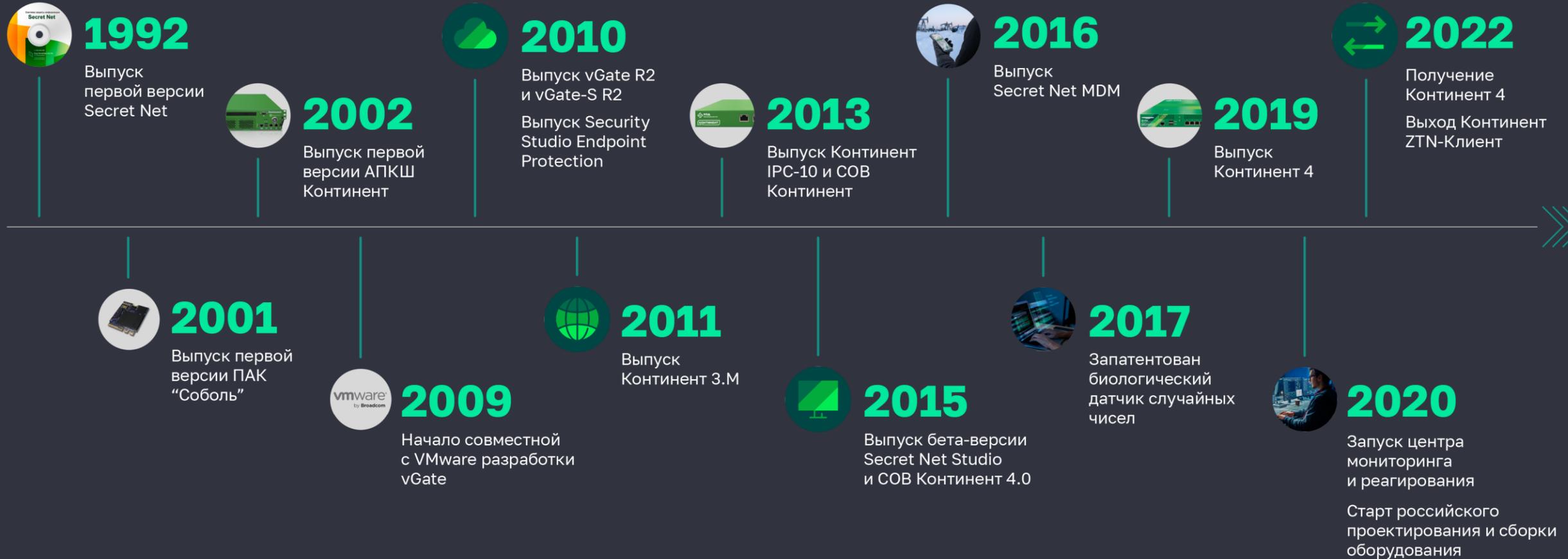


# Код Безопасности

## Защита без границ



# История компании



# Код Безопасности в цифрах



30 лет

Защищаем крупнейшие  
ИТ-инфраструктуры

1200+

Официальных партнеров

50000+

Организаций защищены нашими  
продуктами

50+

Разработанных СЗИ и СКЗИ

60+

Лицензии и сертификаты ФСТЭК, ФСБ,  
Минобороны России

800+

Квалифицированных  
специалистов

# Код Безопасности в цифрах



Членство в профильных общественных организациях и ассоциациях: АРПП «Отечественный софт», «Ассоциация защиты информации» (АЗИ), АПКИТ



3 центра разработки в России (Москва, Санкт-Петербург, Пенза), представительства в Республике Беларусь (Минск) и ОАЭ (Дубай)



Продукция охватывает все уровни инфраструктурной безопасности



Российский разработчик программных и аппаратных средств защиты информации

# Наши клиенты



## Государственные организации



Федеральное  
казначейство  
России



Федеральная  
налоговая служба  
России



Министерство юстиции  
Российской Федерации



Федеральная  
таможенная служба  
России



Центральная  
избирательная комиссия  
Российской Федерации



Федеральный фонд  
обязательного  
медицинского  
страхования

## Телекоммуникационные компании



ПАО  
«Ростелеком»



ПАО  
«МГТС»



ГК «АКАДО  
Телеком»



АО  
«Воентелеком»

# Наши клиенты



## Финансовые организации



Банк России  
Центральный банк  
Российской Федерации



ПАО «Сбербанк»



ГК «Внешэкономбанк»



Банк «ВТБ»  
(ПАО)



АО «Российские  
космические системы»



Ростех  
ГК «Ростех»



ПАО «Московский  
кредитный банк»



ПАО  
«Промсвязьбанк»



АО  
«АЛЬФА-БАНК»



АО  
«Газпромбанк»



ПАО «ГМК  
„Норильский никель“»

## Предприятия ТЭК



ГК  
«Росатом»



ПАО  
«Газпром»



ПАО  
«Россети»

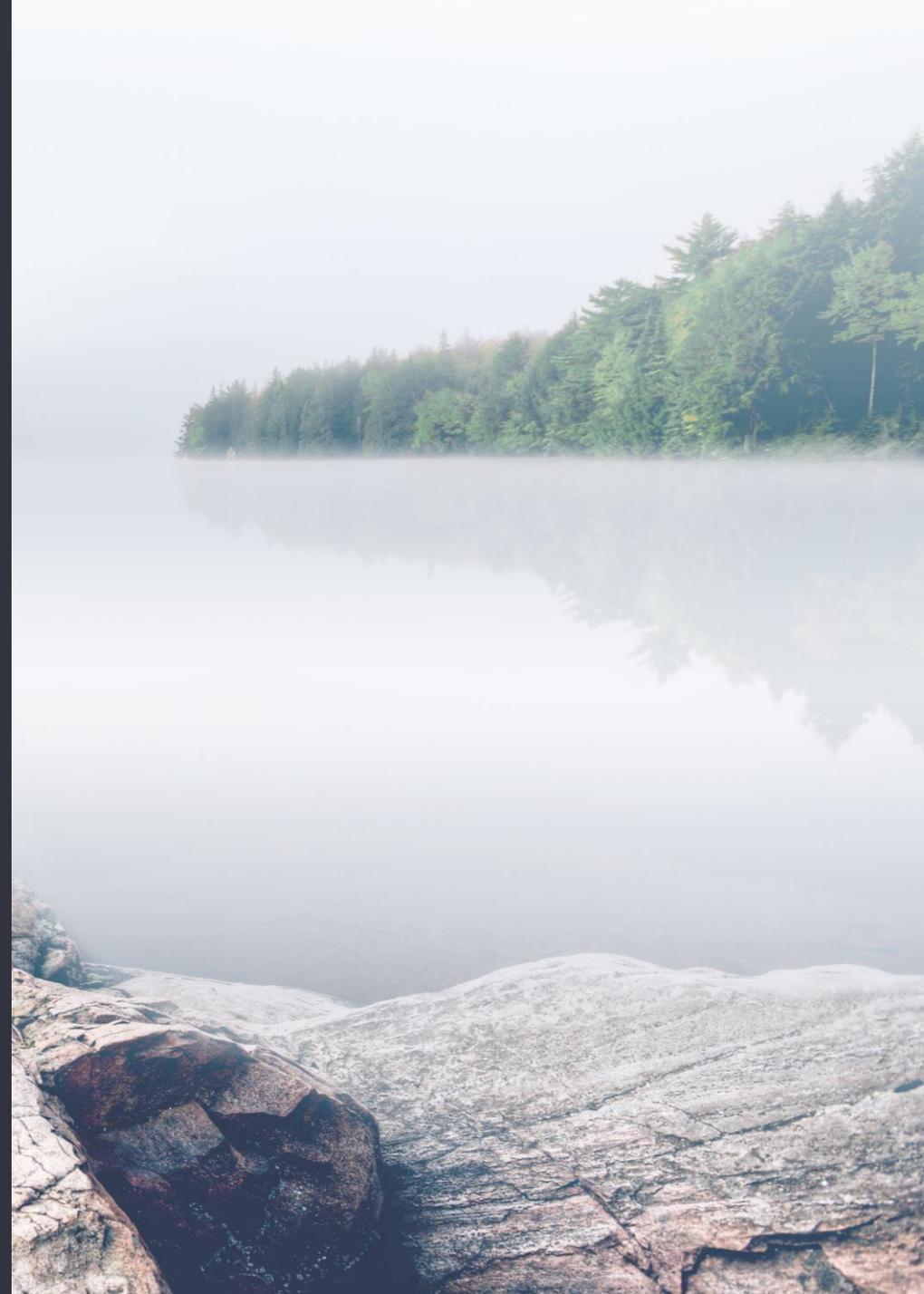


ПАО «НК  
„Роснефть“»



ПАО «АК  
„Транснефть“»

# Краткий обзор продуктов



# Комплексный подход к защите



## Единая архитектура безопасности

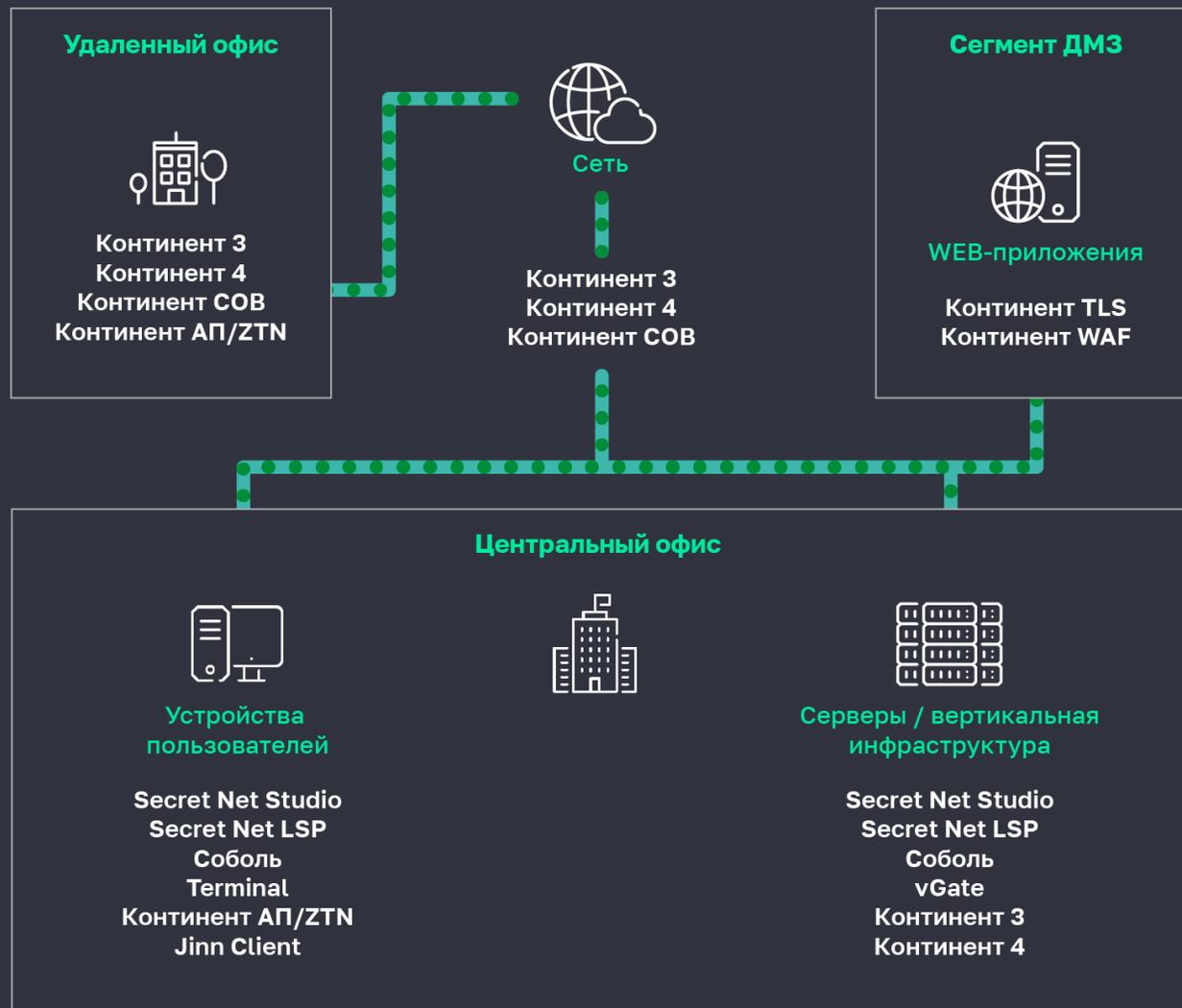
Компания «Код Безопасности» разрабатывает несколько линеек продуктов, объединенных общим архитектурным замыслом и ориентированных на обеспечение безопасности различных компонентов информационной системы. Такой подход позволяет нашим заказчикам поэтапно развивать систему обеспечения информационной безопасности, добавляя новые элементы, расширяющие область действия уже внедренных средств защиты.

## Централизованное управление и мониторинг

Все продукты «Кода Безопасности» обеспечивают централизованное управление политиками безопасности, мониторинг состояния средств защиты и оперативное оповещение о нештатных ситуациях. Дополнительно обеспечивается возможность интеграции с SIEM-системами.

## Гарантированная совместимость продуктов

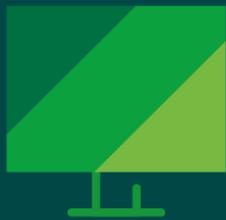
Все продукты «Кода Безопасности» совместимы между собой и обеспечивают корректное функционирование и взаимодействие различных звеньев комплексной системы защиты. При использовании нескольких продуктов «Кода Безопасности» заказчику доступны дополнительные механизмы управления безопасностью, упрощающие настройку и применение продуктов.



# Соболь

Электронный замок

Сертифицированный аппаратно-программный  
модуль доверенной загрузки (АПМДЗ)





## Преимущества:

- Контроль целостности системного реестра Windows, аппаратной конфигурации компьютера и файлов до загрузки операционной системы.
- Простота установки, настройки и администрирования.
- Обеспечение запрета загрузки операционной системы со съемных носителей (USB, FDD, DVD/CD-ROM, LPT, SCSI-порты и др.)

## Предназначен для решения следующих задач:

- Интеграция с СЗИ Secret Net Studio и Secret Net LSP.
- Возможность программной инициализации без вскрытия системного блока.
- Аппаратный датчик случайных чисел.
- Защита конфиденциальной информации и гостайны в соответствии с требованиями нормативных документов.

# Secret Net Studio

Средство защиты данных и контроля безопасности  
конечных точек





## Преимущества:

- Сокращение издержек на администрирование СЗИ и обучение персонала
- Высокая масштабируемость, поддержка распределенных инфраструктур
- Быстрая централизованная настройка защиты в соответствии с требованиями законодательства РФ
- Централизованное управление клиентами Secret Net LSP на платформе Linux

## Предназначен для решения следующих задач:

- Защита конфиденциальной информации.
- Защита от проникновения и несанкционированных действий злоумышленника внутри системы.
- Защита объектов критической информационной инфраструктуры (КИИ).
- Выполнение требований и рекомендаций по защите конечных точек.

# Возможности продукта



# vGate

---

Средство защиты жизненного цикла виртуальных машин микросегментации сетей





## Преимущества:

- Автоматическое приведение инфраструктуры в соответствие с отраслевыми стандартами и требованиями безопасности
- Мониторинг событий безопасности виртуальной инфраструктуры
- Поддержка зарубежных и российских платформ виртуализации – VMware vSphere, Microsoft Hyper-V, Скала-Р
- Безагентный межсетевой экран уровня гипервизора

## Предназначен для решения следующих задач:

- Защита виртуальных машин от несанкционированного копирования, клонирования, уничтожения.
- Защита от специфических угроз, характерных для виртуальных сред.
- Контроль привилегированных пользователей.
- Микросегментация инфраструктуры.
- Мониторинг событий безопасности и расследование инцидентов ИБ.
- Автоматизация compliance и best practice.

# Континент 4

Универсальное устройство для всесторонней защиты  
сети (UTM) корпоративного уровня  
с поддержкой алгоритмов ГОСТ





## Функции:

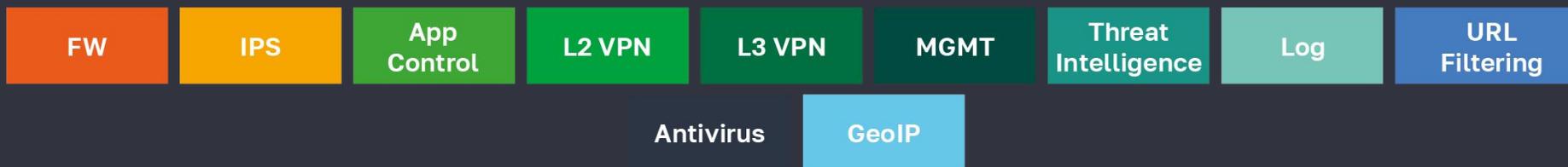
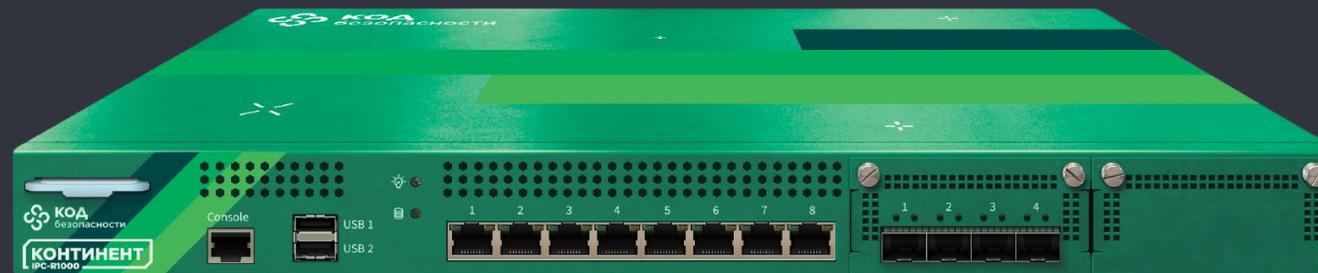
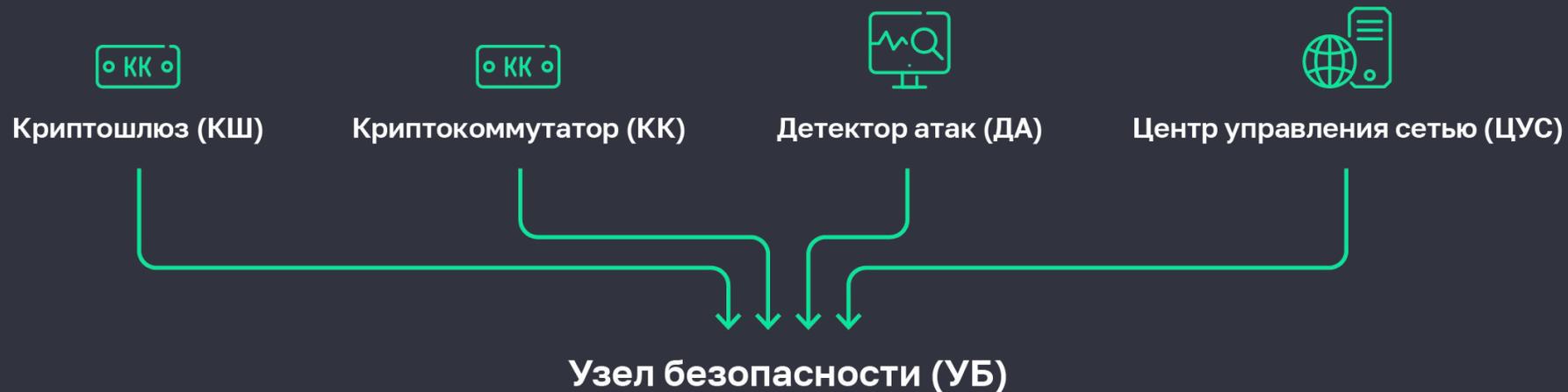
- Централизованное управление
- Эргономика
- Защита от вторжений и вредоносного ПО
- Масштабируемость и отказоустойчивость
- VPN и удаленный доступ
- Расшифровка трафика
- Сетевые функции



## Сценарии использования:

- В датацентре организации
- На периметре организации
- В геораспределенной инфраструктуре
- Для малого и среднего бизнеса
- Защита технологических сетей

# Компоненты узла безопасности



# CryptoPod

Гарнитура с криптографической защитой





## Преимущества:

- Шифрование связи на уровне каналов передачи данных в режиме реального времени
- Защита от перехвата и несанкционированной расшифровки трафика
- Защита от нежелательных звонков
- Конфиденциальность хранения данных о пользователях системы

## Система CryptoPod:

- Гарнитура сопряжена с идентифицированным устройством
- Во время звонка на мобильное приложение поступает уже зашифрованный на гарнитуре трафик, который не может быть расшифрован в приложении
- Сервер помогает установить сообщение на гарнитурах, далее гарнитуры связываются и обмениваются трафиком напрямую, сохраняя конфиденциальность информации даже от приложения



# CryptoPod. Технические характеристики



Мобильные ОС :  
IOS 12 и выше  
Android 9.0 и выше

Сопряжение по Bluetooth 2.0 или выше

Прием/передача на частоте 2400-2483,5 МГц

Время работы гарнитуры (в режиме ожидания): 20 часов  
Время работы гарнитуры (в режиме разговора): 4 часа

# Проектный подход Кода Безопасности за рубежом



# Наши принципы



1

Соответствие российским  
и международным стандартам

2

Мы всегда рядом:  
наша ТП ответит на все  
вопросы

3

Поддержка цифрового  
суверенитета дружественных  
стран

4

Открытость технологий,  
знаний, опыта

5

Единая экосистема  
безопасности

# Международное сотрудничество



## Принципы международного сотрудничества:

- Экспорт технологий в дружественные страны
- Создание альянсов.
- Создание национальных стандартов.

~\$67 МЛРД\*

Объем рынка информационной безопасности стран БРИКС+ к 2029 году

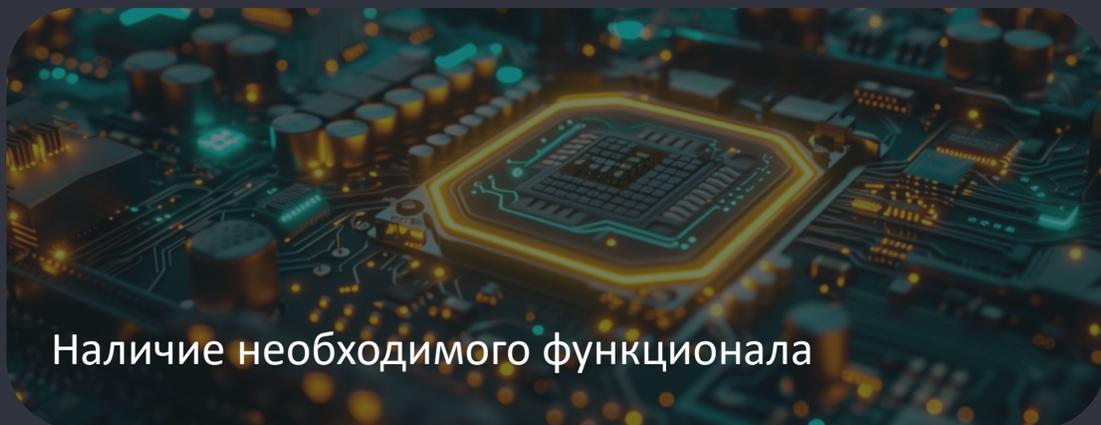
\* - по экспертным оценкам

## Ключевые тенденции и вызовы в области защиты КИИ в мире:

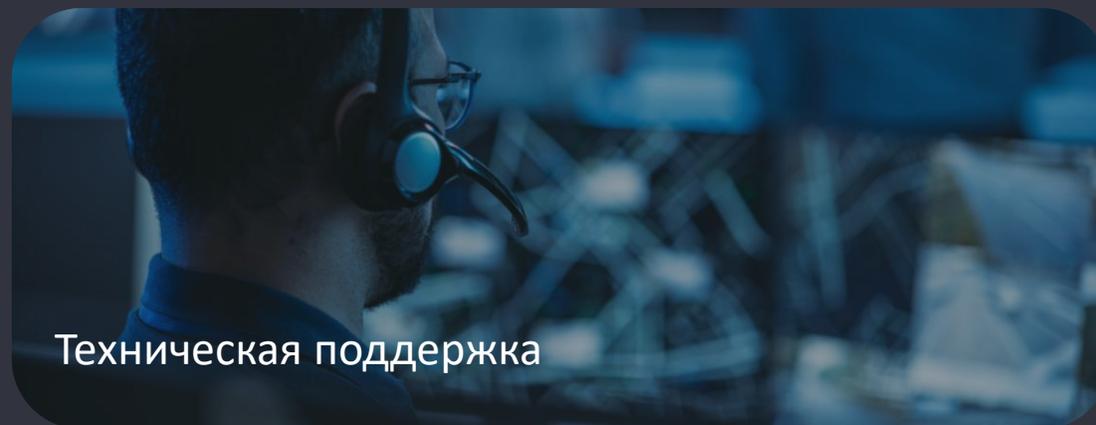
- Отказ от вендерной зависимости производителей оборудования и ПО из США и создание собственных суверенных решений в области защиты КИИ.
- Массовое применение искусственного интеллекта и интернета вещей.
- Использование хакерских атак на государственном уровне как оружия против экономик суверенных государств.
- Сохранение санкционного давления и методов нерыночной конкуренции в среднесрочной перспективе.



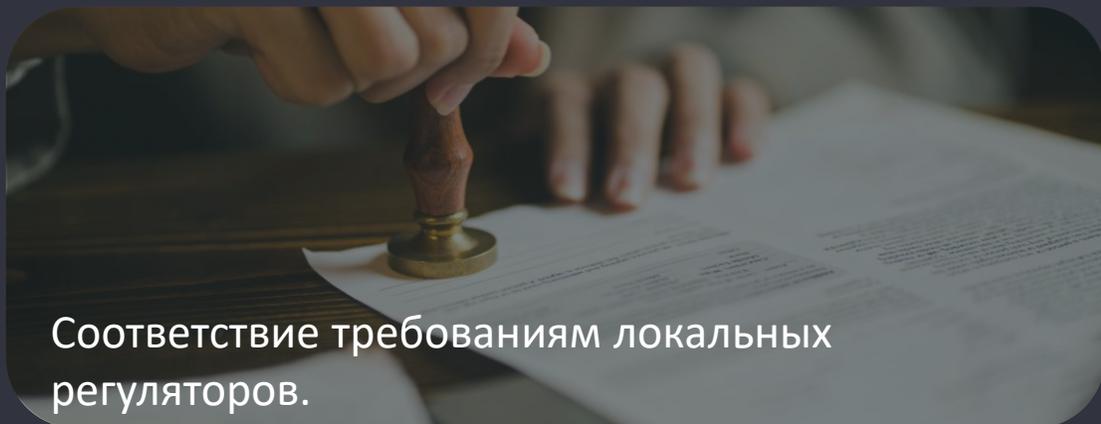
# На что обращать внимание?



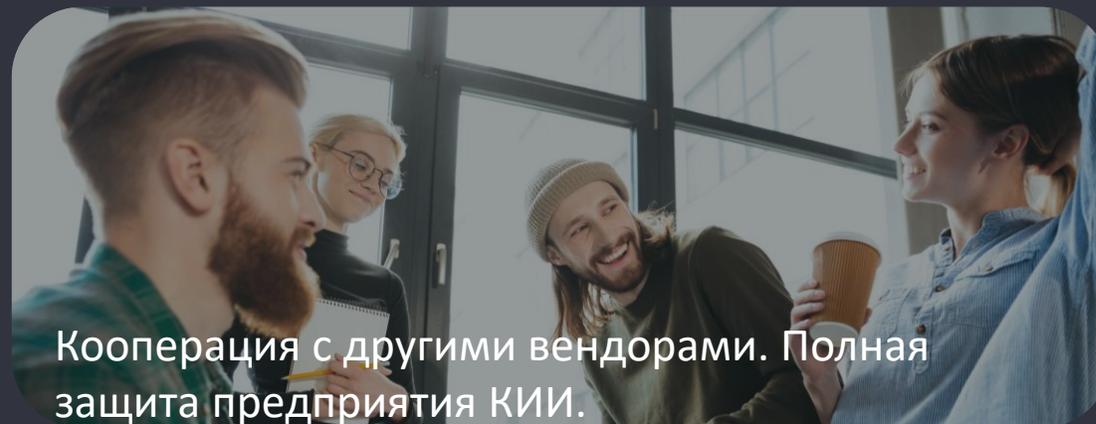
Наличие необходимого функционала



Техническая поддержка

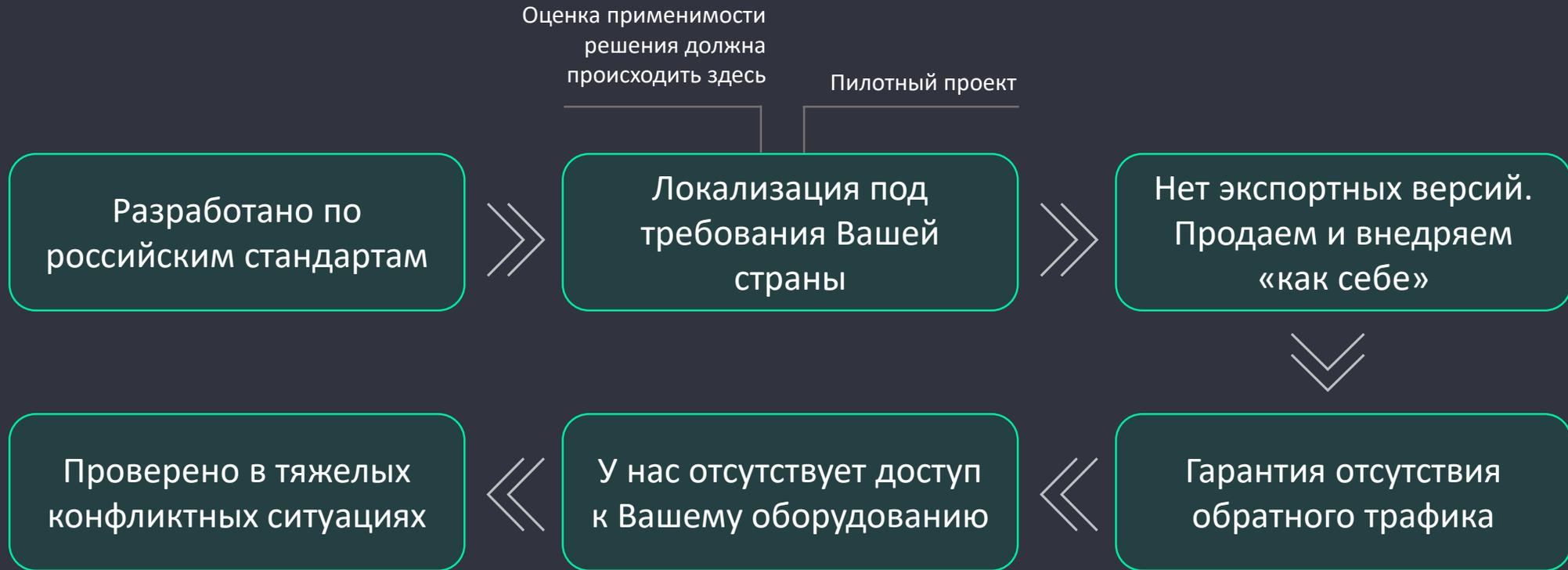


Соответствие требованиям локальных регуляторов.



Кооперация с другими вендорами. Полная защита предприятия КИИ.

# Основа доверия нашим продуктам





# КОД безопасности

[www.securitycode.net](http://www.securitycode.net)  
[export@securitycode.ru](mailto:export@securitycode.ru)