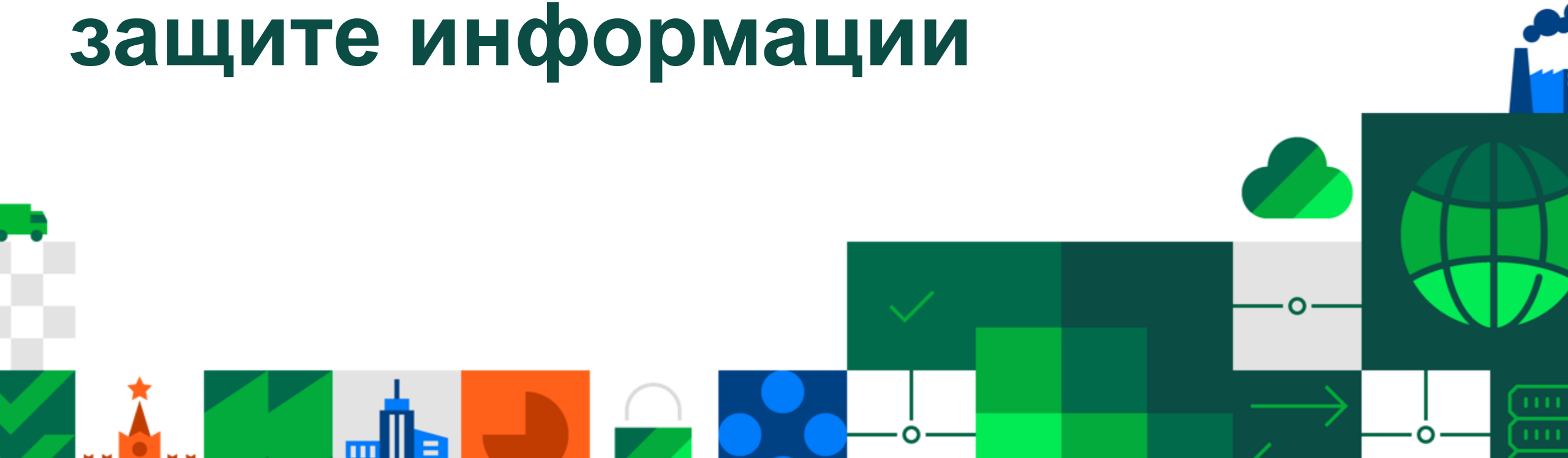
КОД безопасности

Комплексный подход к защите информации



КОД безопасности

О НАС

Российский разработчик средств защиты информации

Самый широкий портфель решений по ИБ

3 центра разработки – Москва, Санкт-Петербург, Пенза

Штат квалифицированных специалистов – 700 человек

Более 35 000 юридических лиц на территории РФ, использующих наши решения

Более 70-ти сертификатов ФСТЭК, ФСБ, МО на всю продуктовую линейку

КОД безопасности

ДОСКА ПОЧЕТА

Федеральное казначейство

РусГидро

КОД безопасности

Текущие проблемы ИБ

Все привыкли к иностранному ПО и железу – приходится переучиваться и менять привычки

- Иностранные ИТ и ИБ решения сильно шагнули вперед
- Приходится перестраивать инфраструктуру
- Приходится выделять новые бюджеты на новую инфраструктуру

КОД безопасности

Текущие проблемы ИБ

Из-за политической ситуации приходится менять подход к построению систем ИБ

- Раньше было тихо и спокойно
- Теперь всех атакуют
- Атакуют государственные информационные системы
- Взламывают крупные банки и предприятия
- Атакуют сервисы, к которым обыватели уже привыкли
- Взламывают объекты КИИ

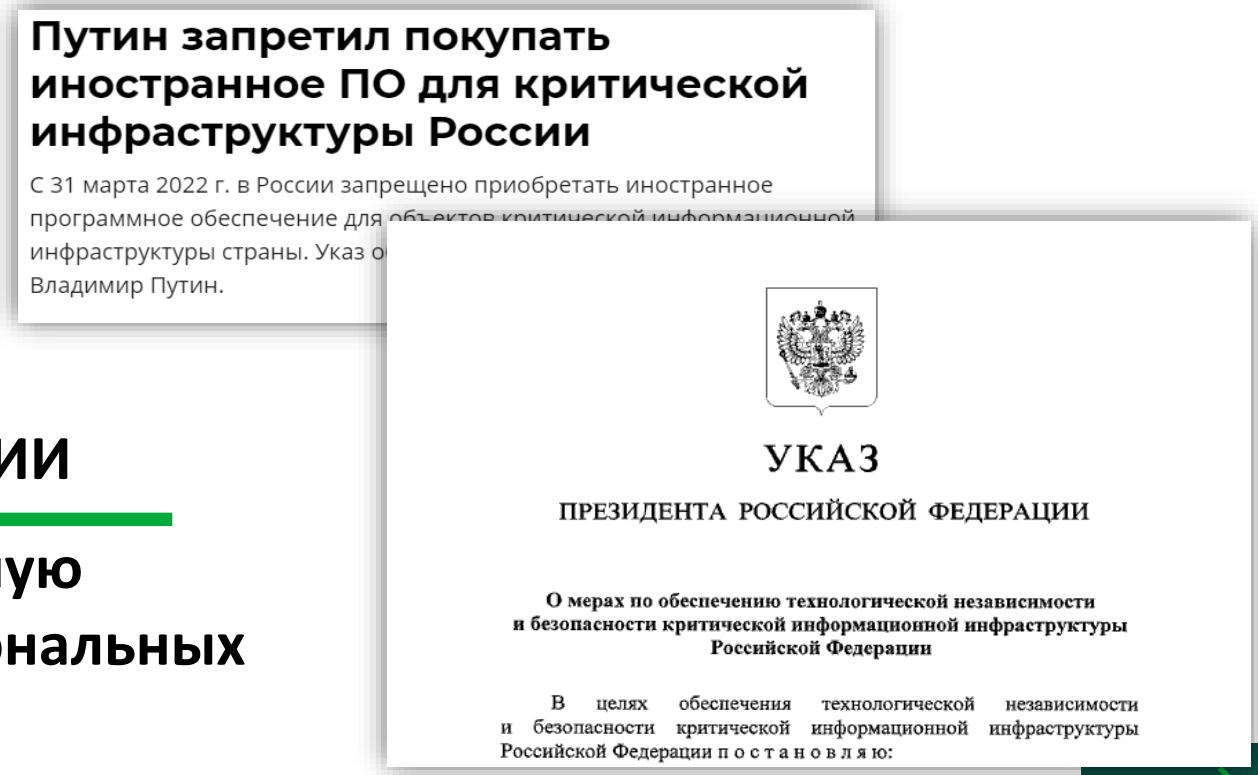
КОД безопасности

Текущие проблемы ИБ

Регуляторы заставляют более ответственно относиться к построению систем ИБ

Президент устанавливает уголовную ответственность за нарушения по теме ИБ в объектах КИИ

В правительстве обсуждают уголовную ответственность уже за утечку персональных данных



Путин запретил покупать иностранное ПО для критической инфраструктуры России

С 31 марта 2022 г. в России запрещено приобретать иностранное программное обеспечение для объектов критической информационной инфраструктуры страны. Указ о
Владимир Путин.

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации

В целях обеспечения технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации п о с т а н о в л я ю:

ВСЕ ЭТО НЕ ПРИВЫЧНО И БОЛЬНО!

КОД безопасности

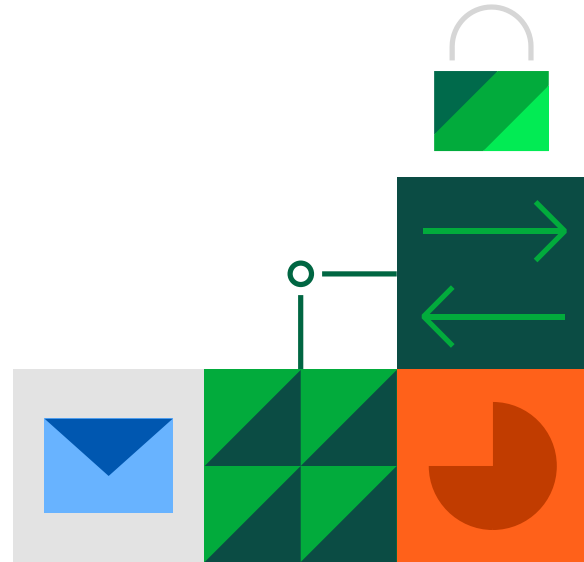
Текущие проблемы ИБ

Люди в экстремальных ситуациях делятся на два типа:

1. Пугаются, прячут голову в песок, и надеются, что ничего с ними не произойдет.
2. Быстро придумывают способы выхода из ситуации и не боятся принимать решения.

Так же и в нашей ситуации:

1. Можно по мелочи латать дыры в своих системах за минимальные бюджеты.
2. Можно быстро придумывать план перехода на новые рельсы, обосновывать бюджеты, и выполнять новые задачи.



КОД безопасности

Текущие проблемы ИБ

Как раньше, уже не будет никогда…

Теперь инфбез занимает важнейшую роль в развитии ИТ любой компании. А иначе компанию уничтожат…

КОД безопасности

Теперь про защиту инфраструктуры

- Есть рабочие станции – надо защищать
- Есть серверы – надо защищать
- Есть виртуализация – надо защищать
- Есть каналы связи – надо защищать
- Сеть смотрит в глобальный интернет – надо защищать

КОД безопасности

Что нужно для защиты информации?

- Аутентифицировать пользователей
- Контролировать пользователей
- Обеспечивать доступ
- Шифровать каналы связи
- Защищать сеть от внешних вторжений и ограничивать пользователей при выходе в интернет
- Обнаруживать и бороться с хакерскими атаками
- Обеспечивать анализ инцидентов ИБ
- Управлять всей инфраструктурой (АРМы, Сервера, Облака, трафик, доступ к данным и т.д.)

КОД безопасности

Что нужно для защиты информации?

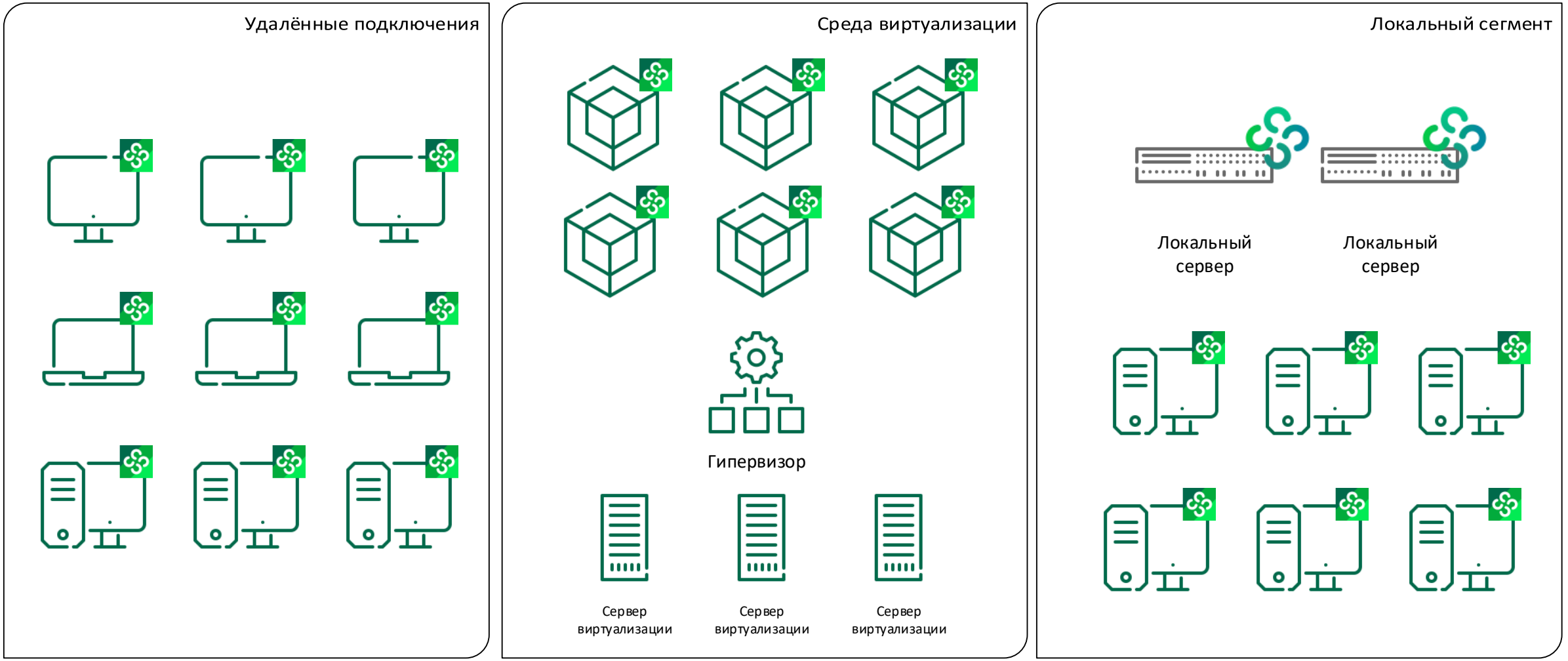
- Аутентифицировать пользователей
- Контролировать пользователей
- Обеспечивать доступ
- Шифровать каналы связи
- Защищать сеть от внешних вторжений и ограничивать пользователей при выходе в интернет
- Обнаруживать и бороться с хакерскими атаками
- Обеспечивать анализ инцидентов ИБ
- Управлять всей инфраструктурой (АРМы, Сервера, Облака, трафик, доступ к данным и т.д.)

КОД безопасности

Secret Net Studio / LSP

КОД безопасности

Secret Net Studio / LSP



КОД безопасности

Совместимость Secret Net LSP

ASTRA LINUX®

СЕРТИФИКАТ СОВМЕСТИМОСТИ

№ 11446/2023

Настоящим сертификатом ГК «Астра» (ООО «РусБИТех-Астра») подтверждает работоспособность и корректность совместного функционирования операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) и программного обеспечения

«Secret Net LSP» версии 1.12

компании «Код Безопасности» (ООО «Код Безопасности»).

Сертификат совместимости подготовлен на основании результатов совместных испытаний, проведённых компанией ООО «РусБИТех-Астра», представленных в документе протокола № 11446/2023 от 04.04.2023.

READY FOR ASTRA LINUX CERTIFICATE

Дата выдачи: 11.04.2023

Руководитель дивизиона внедрения и сопровождения ООО «РусБИТех-Астра» Богомолов Я. О.

Действие Сертификата на момент его предъявления можно проверить на сайте https://astralinux.ru/ready-for-astra/

РЕДСОФТ

КОД БЕЗОПАСНОСТИ

СЕРТИФИКАТ СОВМЕСТИМОСТИ

программного продукта «Средство защиты информации Secret Net LSP» версии 1.9, производства ООО «Код Безопасности»
и
программного продукта РЕД ОС 7.2 МУРОМ, производства ООО «РЕД СОФТ»

«29» апреля 2020 г. г. Москва

Настоящим сертификатом компании ООО «Код Безопасности» и ООО «РЕД СОФТ» подтверждают совместимость и корректность работы программного продукта «Средство защиты информации Secret Net LSP» версии 1.9 с операционной системой РЕД ОС 7.2 МУРОМ.

ООО «Код Безопасности» является производителем и правообладателем программного продукта «Средство защиты информации Secret Net LSP».

«Средство защиты информации Secret Net LSP» - сертифицированное средство защиты информации от несанкционированного доступа для операционных систем семейства Linux. Продукт обладает сертификатом ФСТЭК России (№2790 от 18.12.2012), соответствует требованиям руководящих документов по 5 классу защищенности СВТ и по 4 уровню контроля отсутствия НДВ. Может применяться в АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно.

ООО «РЕД СОФТ» является официальным производителем и правообладателем программного продукта РЕД ОС.

РЕД ОС – российская операционная система общего назначения семейства Linux для серверов и рабочих станций. Продукт обладает сертификатом ФСТЭК России (№4060 от 12.01.2019), что подтверждает его соответствие требованиям информационной безопасности и допускает его применение в государственных информационных системах и информационных системах персональных данных до 1 класса включительно. РЕД ОС зарегистрирована в Едином реестре российских программ для ЭВМ и баз данных Минкомсвязи России (№3751).

Настоящий сертификат выдан на основании испытаний, проведенных специалистами компаний ООО «Код Безопасности» и ООО «РЕД СОФТ».

Генеральный директор ООО «РЕД СОФТ» /М.В. Анисимов/

Генеральный директор ООО «Код Безопасности» /А.В. Голов/

КОД безопасности

base alt

СЕРТИФИКАТ СОВМЕСТИМОСТИ

СЗИ Secret Net LSP 1.12
и операционных систем Альт

27.04.2023 г. № 0071/23 г. Москва

Настоящим сертификатом компании ООО «Код Безопасности» и ООО «Базальт СПО» подтверждают совместимость и корректность работы СЗИ Secret Net LSP 1.12 производства компании ООО «Код Безопасности» и операционных систем (ОС) семейства «Альт» разработки компании ООО «Базальт СПО» на платформе **x86_64**.

Информация о совместимости дистрибутивов ОС «Альт» с СЗИ Secret Net LSP 1.12 приведена в таблице:

	Альт 8 СП (сертификат ФСТЭК России)	Альт Рабочая станция 9	Альт Сервер 9	Альт Рабочая станция 10	Альт Рабочая станция К 10	Альт Сервер 10
СЗИ Secret Net LSP 1.12	+	+	+	+	+	+

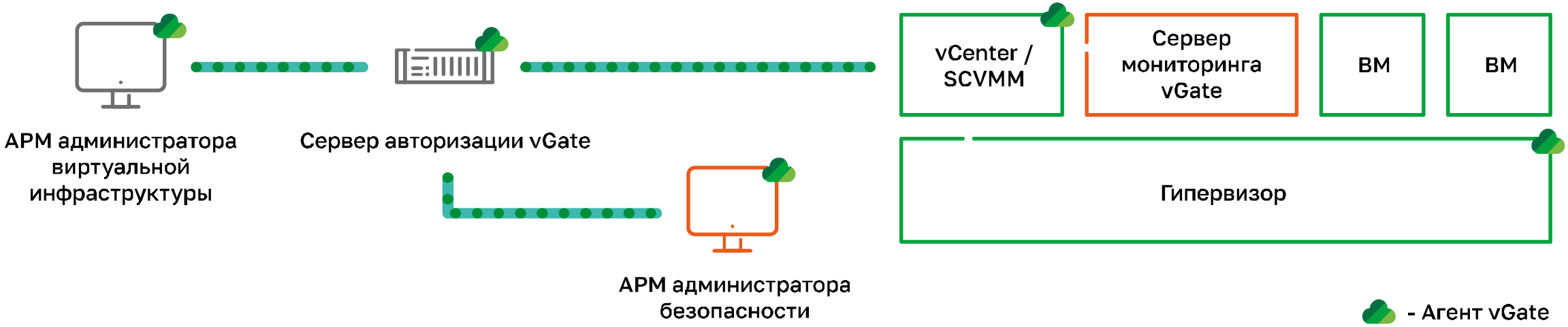
Настоящий сертификат оформлен по результатам тестовых испытаний, проведенных специалистами компаний ООО «Код Безопасности» и ООО «Базальт СПО». Результаты тестовых испытаний зафиксированы в двустороннем протоколе.

Технический директор ООО «Код Безопасности» _____ /Д.А. Зрячих

Генеральный директор ООО «Базальт СПО» _____ /С.И. Трандин

КОД безопасности

vGate 4.7



Защита настроек и виртуальных машин

Контроль целостности конфигурации виртуальных машин и доверенная загрузка

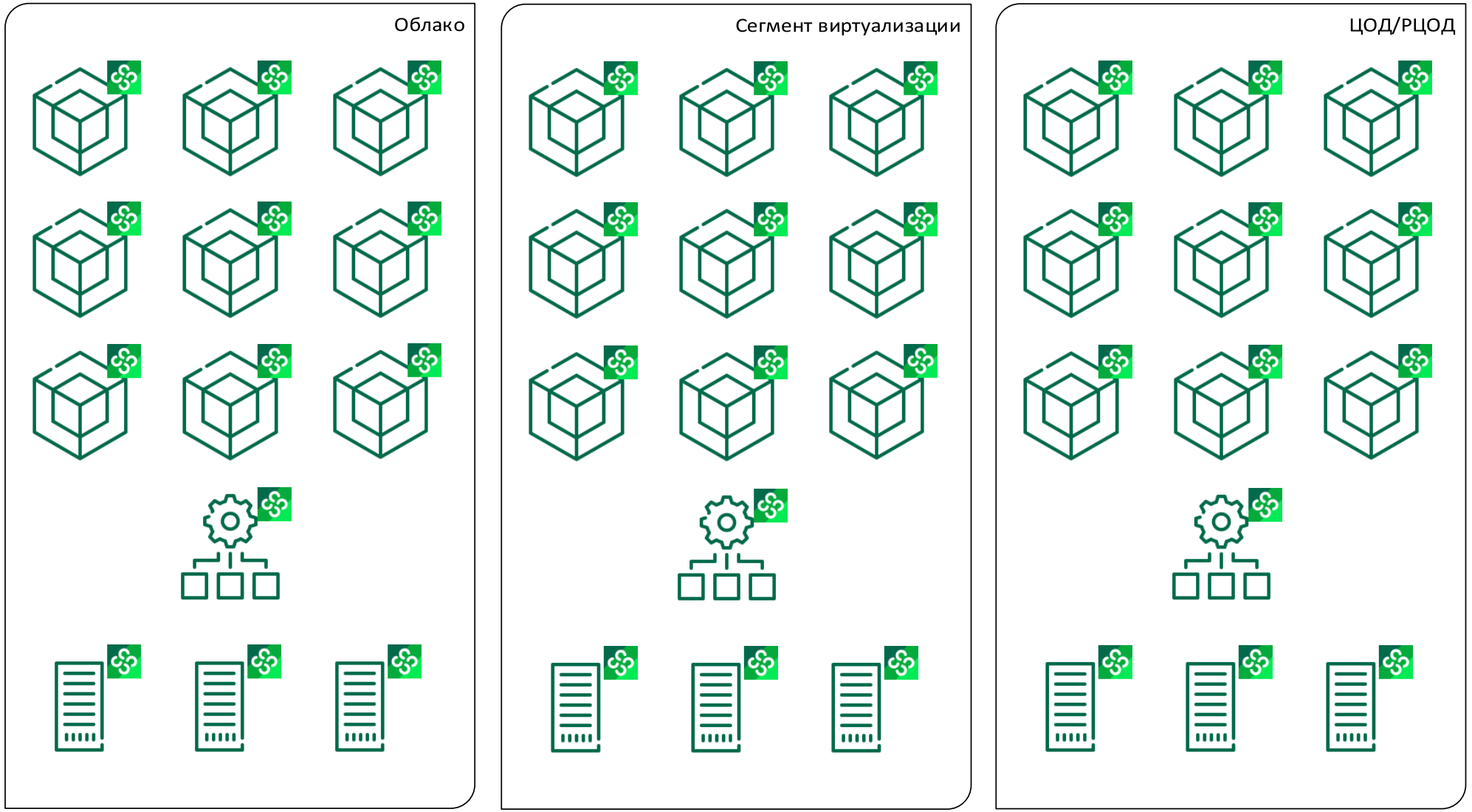
Контроль доступа администраторов ВИ к файлам виртуальных машин

Контроль целостности объектов внутри ВМ

Защита данных внутри ВМ

КОД безопасности

vGate 4.7



КОД безопасности

Континент 3 – СКЗИ

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

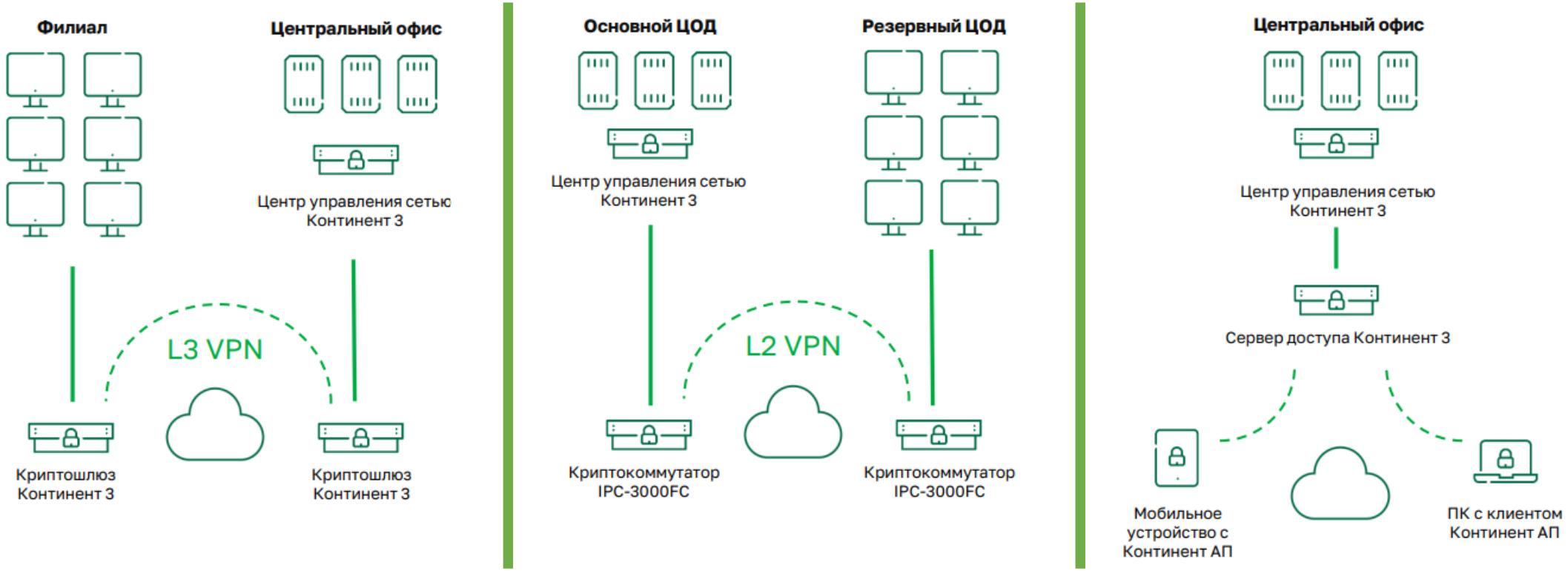
Аппаратно-программный комплекс, предназначенный для организации защищенного удаленного доступа с помощью VPN-клиента Континент АП.

СКЗИ Континент АП

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

КОД безопасности

Континент 3 – СКЗИ



КОД безопасности

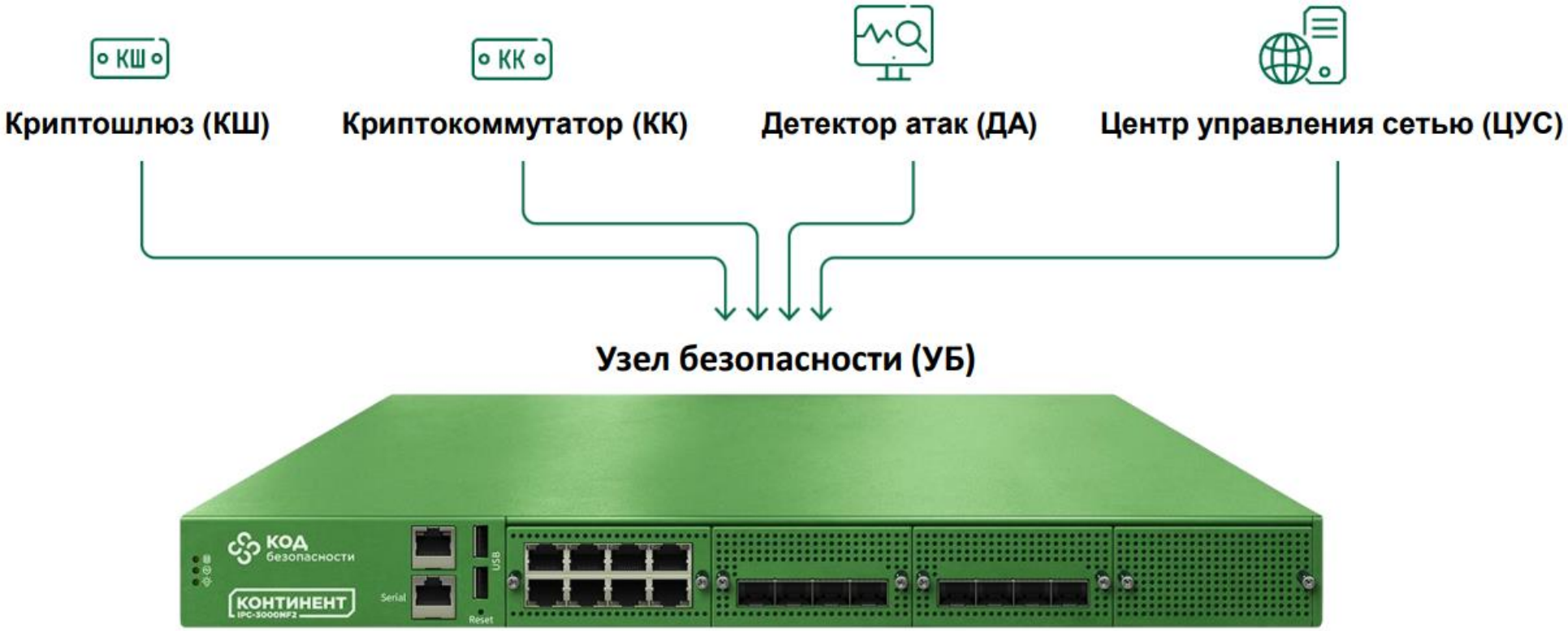
Континент 4 – UTM/NGFW

Сертифицирован ФСТЭК России:

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

КОД безопасности

Континент 4 – UTM/NGFW

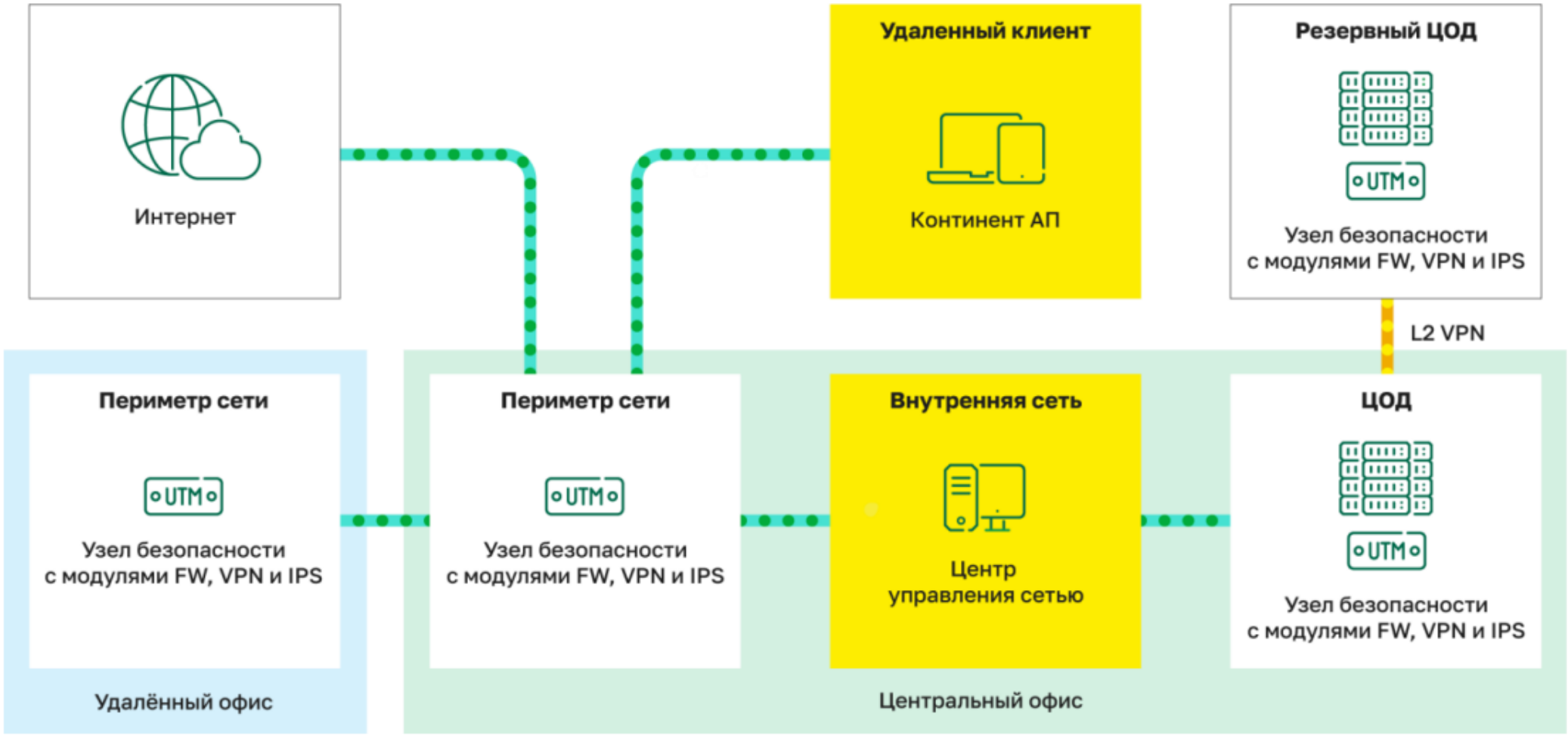


FW | IPS | App control | L2 VPN | L3 VPN | MGMT | Threat Intelligence | Log | URL Filtering | User Identity

Antivirus | GeoIP

КОД безопасности

Континент 4 – UTM/NGFW



КОД безопасности

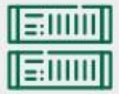
Континент 4 – UTM/NGFW

Безопасность

- Контроль сетевых приложений (4000 приложений)
- Система предотвращения вторжений
- Блокировка доступа к вредоносным сайтам
- SSL-инспектирование трафика
- Поведенческий анализ на основе машинного обучения
- Поддержка VPN ГОСТ

Управление

- Централизованное управление инфраструктурой из единой консоли
- Интеграция с LDAP
- Портал и агент аутентификации пользователей, SSO
- Гибкий интерфейс мониторинга
- Резервирование системы управления



Форм-фактор

- Многофункциональный узел безопасности (UTM)
- Высокопроизводительный межсетевой экран
- Система обнаружения вторжений (L2 IPS)
- Выделенная платформа управления

Сетевые технологии

- Динамическая маршрутизация
- Поддержка NAT
- Multi-WAN
- QoS
- Кластеризация узлов безопасности (переключение менее 1 секунды)

КОД безопасности

Континент 4 – UTM/NGFW

UTM

Интегрированный межсетевой экран

- Межсетевой экран
- Контроль приложений
- Поведенческий анализ
- Система обнаружения вторжений на сетевом уровне (L3)

NF2

Высокопроизводительный межсетевой экран

- Межсетевой экран с использованием технологии префиксных деревьев

L2 IPS

Детектор атак

- Система обнаружения вторжений на канальном уровне (L2)

КОД безопасности

Чем удобен Код Безопасности

Максимальное количество обязательных требований мы закрываем

Возможные конфликты систем между собой проще решать в рамках одного тикета в ТП

Легче адаптироваться к новым условиям жизни на рынке ИБ с меньшим количеством вендоров

КОД безопасности

Спасибо за внимание

С уважением, Сергей Мущенко
Руководитель отдела развития продаж компании «Код безопасности»
Тел.: +7 495 982 3020, доб. 889
Моб.: +7 916 119 6269
E-mail: s.mushchenko@securitycode.ru