ViPNet Coordinator KB 4

Виталий Беличко

План вебинара

1. Введение
2. Модельный ряд
3. Функциональные возможности
4. Ключевая система
5. Особенности настройки и эксплуатации
6. Сертификация и планы развития

Классы СКЗИ

КС1	Атаки проводимые **за пределами КЗ**
КС2	Атаки проводимые **в пределах КЗ**
КС3	Атаки при **наличии физического доступа** к СВТ
КВ	Атаки, проводимые специалистами **в области разработки и анализа СКЗИ** (научно-исследовательские центры)
КА	Атаки, проводимые специалистами, **владеющими конструкторской документацией и аппаратным компонентам СКЗИ и СФ**

Приказ ФСБ России №378 от 10.07.2014

Применение СКЗИ класса КВ (ПДн)

Приказ **ФСБ России №378 от 10.07.2014** "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПД при их обработке в ИСПД с использованием СКЗИ информации, необходимых для выполнения установленных Правительством РФ требований к защите ПД для каждого из уровней защищенности»

СКЗИ класса КВ и выше применяются в случаях, когда для ИС **актуальны угрозы 2 типа** (наличие недокументированных возможностей в прикладном ПО, используемом в ИС)

Применение СКЗИ класса КВ (УЦ)

Приказ **ФСБ России №796** от 27.12.2011 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»

35. При подключении средств УЦ к информационно-телекоммуникационной сети, доступ к которой не ограничен определенным кругом лиц, указанные средства должны соответствовать требованиям к средствам УЦ класса **КВ2 или КА1**

Защита средств УЦ

1.6.3 Развертывание ПК ViPNet УЦ в корпоративной сети, связанной с ССОП

Если корпоративная сеть организации связана с сетью связи общего пользования, то взаимодействие между ПК ViPNet УЦ и пользователями УЦ может быть организовано либо по схеме №1 (рисунок 1, рисунок 2) с помощью съемных носителей, либо по каналам корпоративной сети через криптошлюз, сертифицированный по требованиям ФСБ России к СКЗИ класса КВ2 (рисунок 5, рисунок 6). В качестве такого криптошлюза может использоваться ПАК ViPNet Координатор-КВ2 или иные аналогичные продукты, сертифицированные ФСБ России по классу КВ.

При организации сетевого взаимодействия компонентов ПАК «КриптоПро УЦ 2.0» между собой в случае их размещения в разных контролируемых зонах, каналы связи (сети связи) между этими компонентами, в случае если данные каналы связи (сети связи) подключены к сетям передачи данных общего пользования (сети интернет), должны быть защищены с использованием СКЗИ, сертифицированных ФСБ России по классу не ниже КВ2, либо быть выделенными в соответствии с ФЗ «О связи» №126-ФЗ от 07.07.2003 года.

ПАК «ViPNet Координатор-КВ2»

- Два исполнения: КВ100 X2 и КВ1000 Q2
- Невысокая производительность
- Отсутствие кластера горячего резервирования

КВ1000 Q2

КВ100 X2


infotecs
ViPNet Coordinator KB 4

ViPNet Coordinator KB 4

- Соответствие требованиям СКЗИ класса КВ
- Высокая скорость шифрования до 4,5 Гбит/с
- Кластер горячего резервирования
- VPN канального уровня (L2overIP)
- Поддержка ViPNet Policy Manager
- Поддержка OSPF, vLan, QoS
- 2 новых исполнения

Функциональные возможности

VPN

- VPN-шлюз сетевого уровня (L3 VPN)
- VPN-шлюз канального уровня (L2OverIP VPN)
- Сервер IP-адресов
- Маскирование структуры трафика в UDP

МЕЖСЕТЕВОЙ ЭКРАН

- Межсетевой экран с контролем состояния сессий
- Раздельная фильтрация открытого и шифруемого IP-трафика
- NAT/PAT
- Антиспуфинг

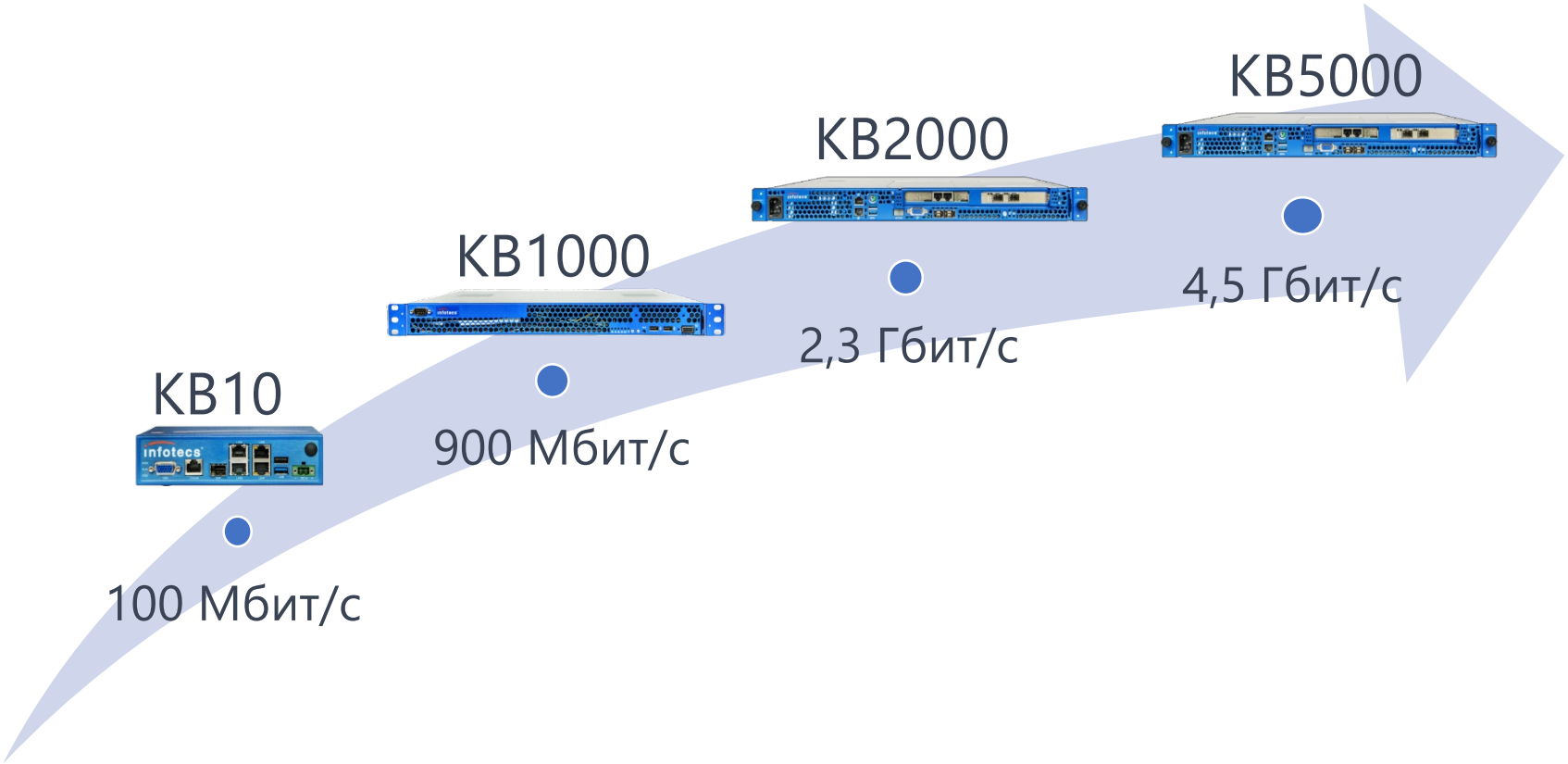
СЕРВИСНЫЕ ФУНКЦИИ

- DNS-сервер, NTP-сервер и SNMP-агент
- DHCP-сервер и DHCP-Relay
- Поддержка ИБП (UPS)
- Кластер горячего резервирования

СЕТЕВЫЕ ФУНКЦИИ

- Статическая маршрутизация
- Динамическая маршрутизация
- Поддержка VLAN (dot1q)
- Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)

Производительность КВ 4



Модельный ряд КВ 4

	КВ100	КВ1000	КВ2000	КВ5000
Форм-фактор	MiniPC	1U	1U	1U
L3 VPN	100 Мбит/с	900 Мбит/с	2,3 Гбит/с	4,5 Гбит/с
L2OverIP VPN	100 Мбит/с	840 Мбит/с	2 Гбит/с	3,4 Гбит/с
Максимальное количество туннелей	Не ограничено			
Сетевые интерфейсы (медные)	4x RJ45 1 Гбит/с			
Сетевые интерфейсы (оптические)	1 x SFP 1 Гбит/с	2x SFP 1 Гбит/с	4x SFP+ 10 Гбит/с	
Отказоустойчивый кластер	Нет	Да		

Дополнительные ТС

Устройство аутентификации:

- «Рутокен ЭЦП 2.0» либо «JaCarta ГОСТ»

Трансивер:

- Avago AFBR-5710PZ – KB100 N1/KB1000 Q6
- Avago AFBR-709SMZ – KB2000 Q4/KB5000 Q1

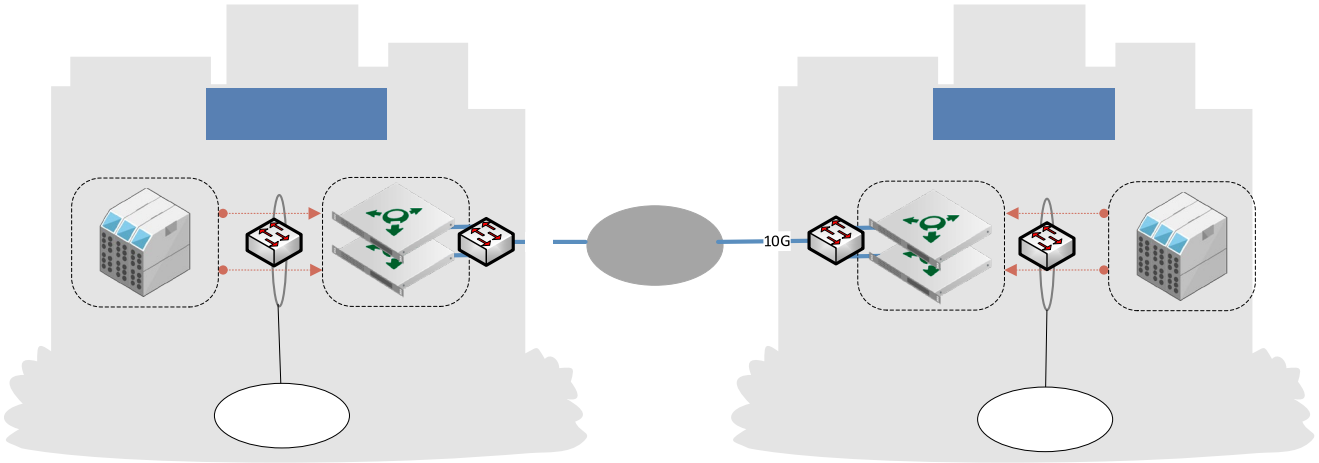
Оптический привод:

- Внешний USB DVD привод

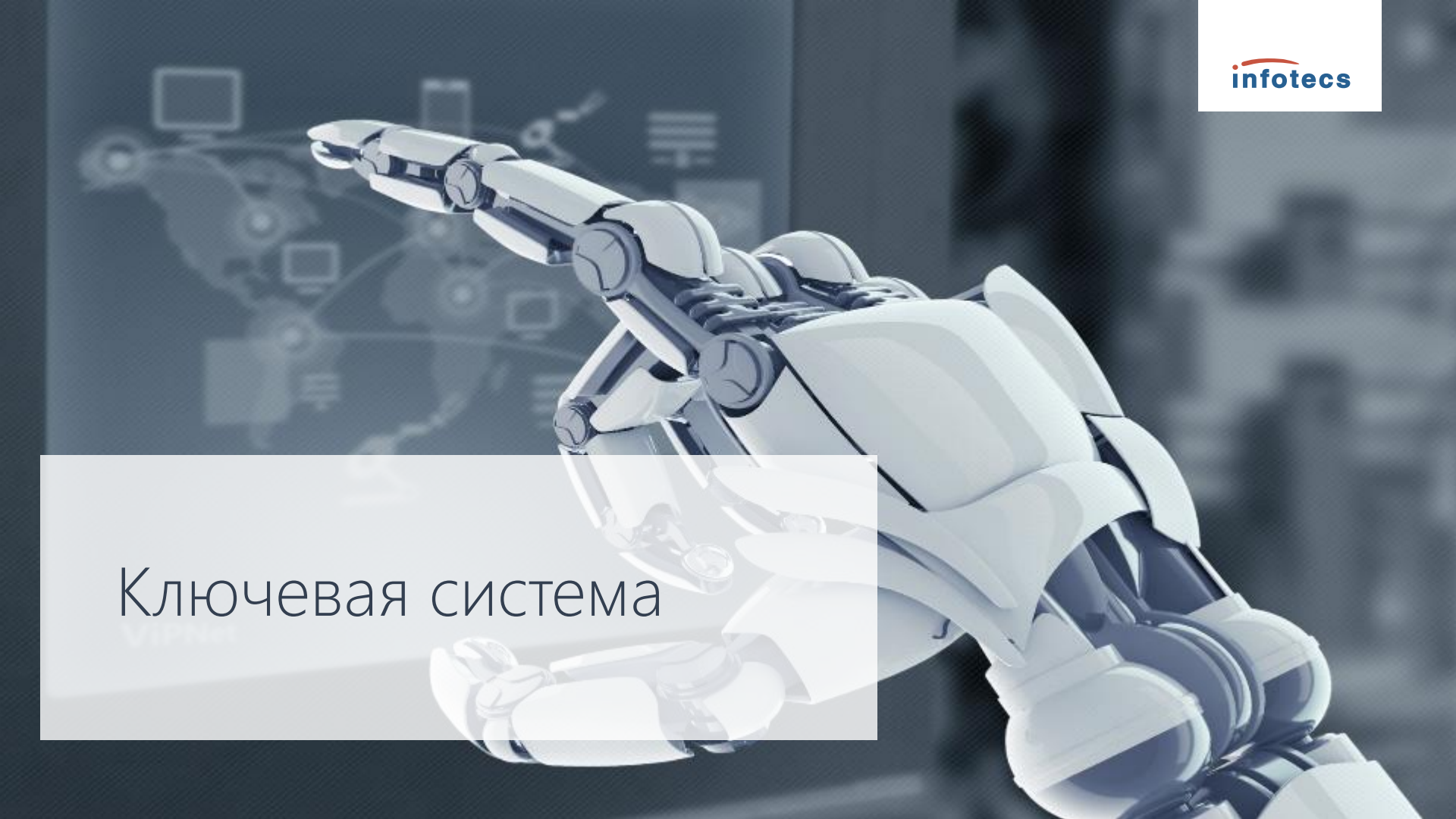
Защита каналов связи (L3 VPN)

- Защита периметра сети
- Объединение распределенных сетей
- Предотвращение НСД к информации

Защита каналов связи (L2overIP VPN)



- Защита канала между ЦОД и РЦОД
- Масштабируемость
- Отказоустойчивость



Ключевая система

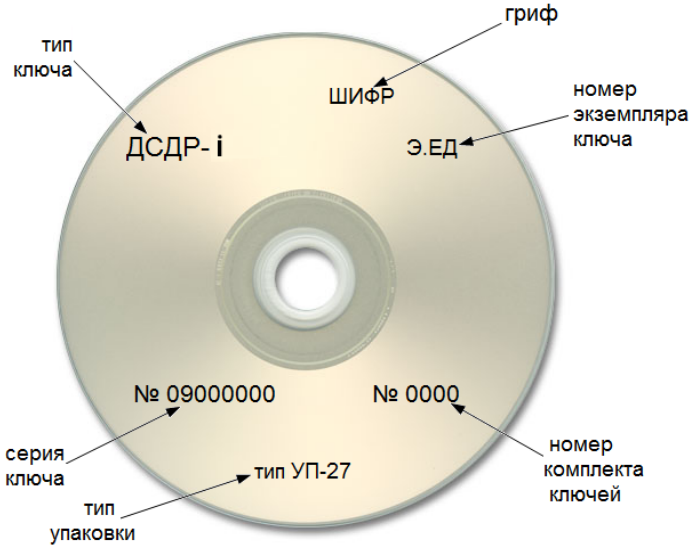
Ключевая система КВ 4

Ключевые блокноты ДСДР, изготавливаемые 8 Центром ФСБ России

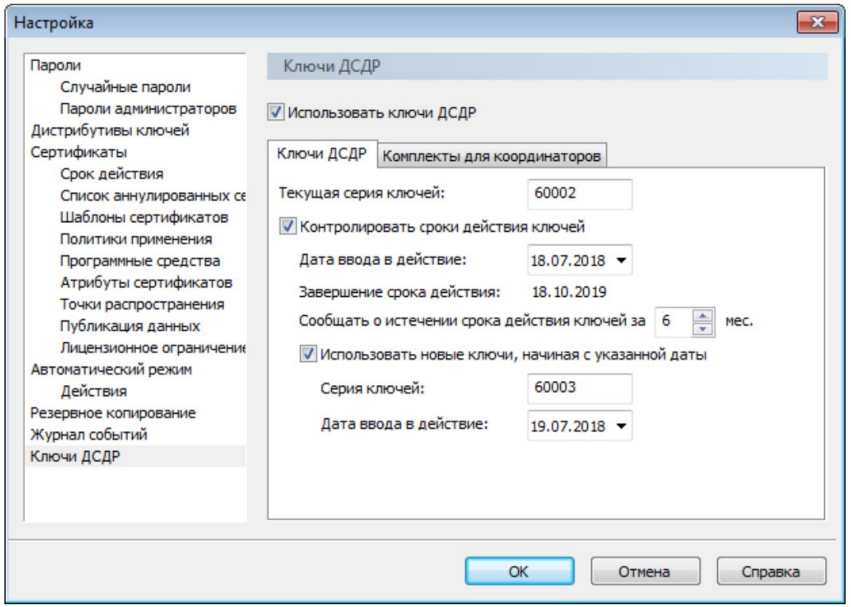
Ключевая информация, формируемая в ViPNet Administrator

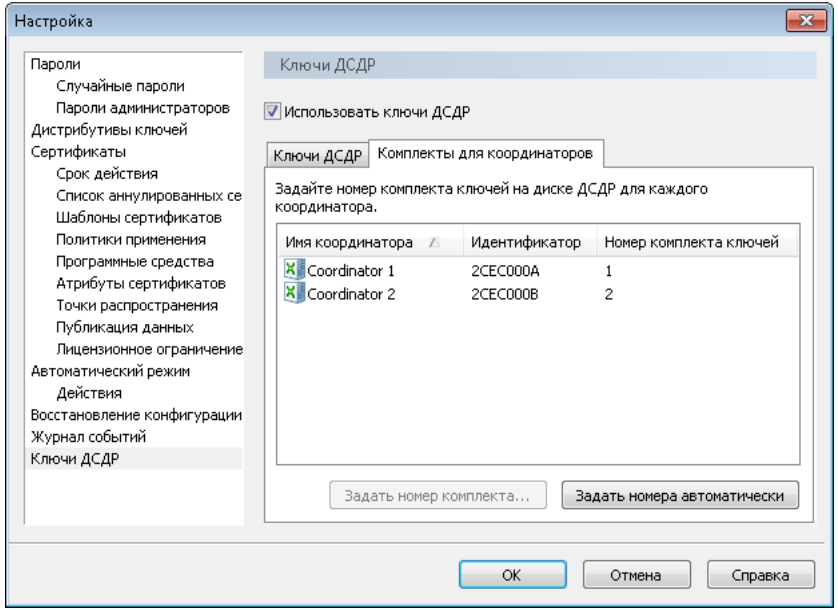
Ключевые блокноты ДСДР

- При заказе ДСДР необходимо заранее запланировать нужное шлюзов КВ в сети
- Размер серии ДСДР не может быть изменен во время действия ключей
- Рекомендуем заказывать комплект ключей с коэффициентом 2,5
- Допустимый срок эксплуатации серии ключей – 1 год и 3 месяца
- Для проведения плановой смены ключей необходимо предварительно заказать и получить новый ключевой блокнот

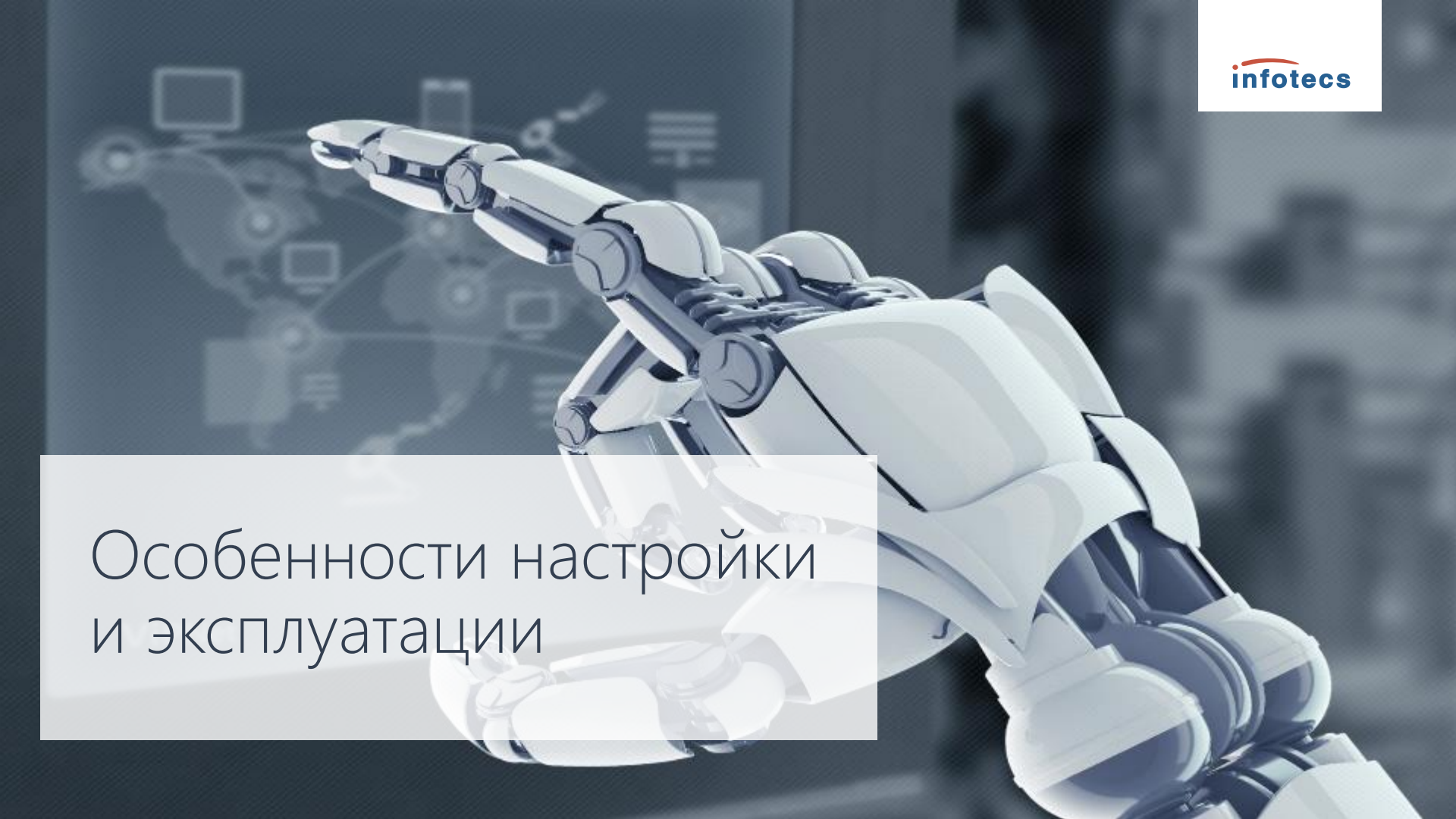


Регистрация ДСДР в ViPNet Administrator





Генерация и ввод ключей



Особенности настройки и эксплуатации

Функциональные ограничения

- Шлюзовой координатор (межсетевое взаимодействие)
- Подключение к внешней сети через «Координатор»
- Удаленное подключение через SSH или Web-UI
- Удаленное обновление ПО
- TCP-туннели
- Поддержка EtherChannel и изменение MTU
- Прокси-сервер и антивирус

Особенности эксплуатации

При истечении срока действия ключа ДСДР связь между КВ прервется

Необходимо использовать службу точного времени NTP и ИБП

Максимальная разница во времени между узлами КВ:
КВ100 – 236 с, КВ1000 – 51 с, КВ2000 – 19 с, КВ5000 – 10 с

Аутентификация пользователя по токену

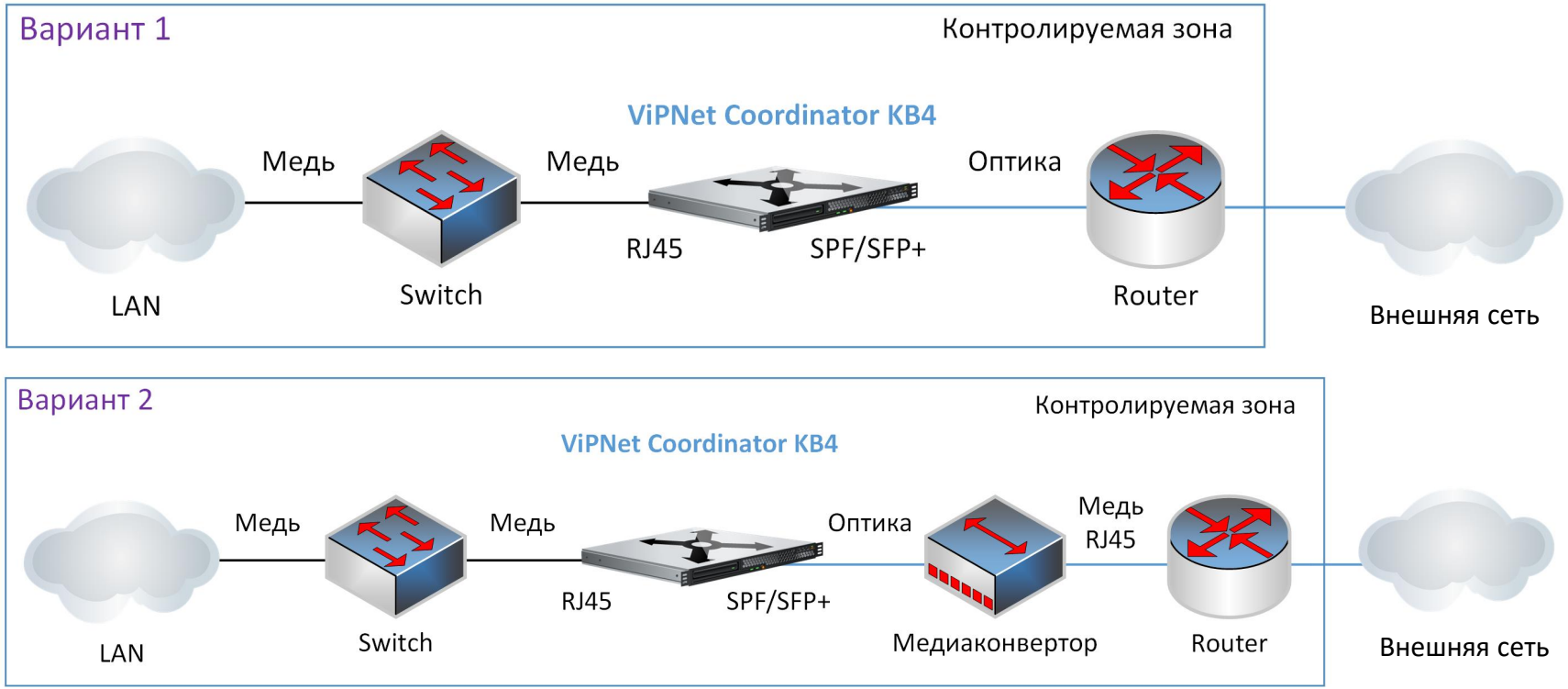
Локальная работа с ключами ДСДР (обновление/смена)

Подключение к внешней сети

Запрещается проводить прямое подключение ViPNet Coordinator KB 4 к каналам связи, выходящим за пределы контролируемой зоны

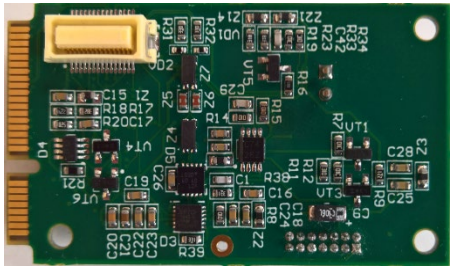
Подключение ViPNet Coordinator KB 4 к каналу связи, выходящему за пределы контролируемой зоны, должно осуществляться через фрагмент оптоволоконной сети, содержащей в своём составе коммутационное оборудование

Подключение к внешней сети



Защита от НСД

- Контроль вскрытия корпуса
- Экстренное стирание ключевой информации
- Контроль целостности ПО
- Контроль срока действия ключей ДСДР



Совместимость версий ПО

Управляющие компоненты:

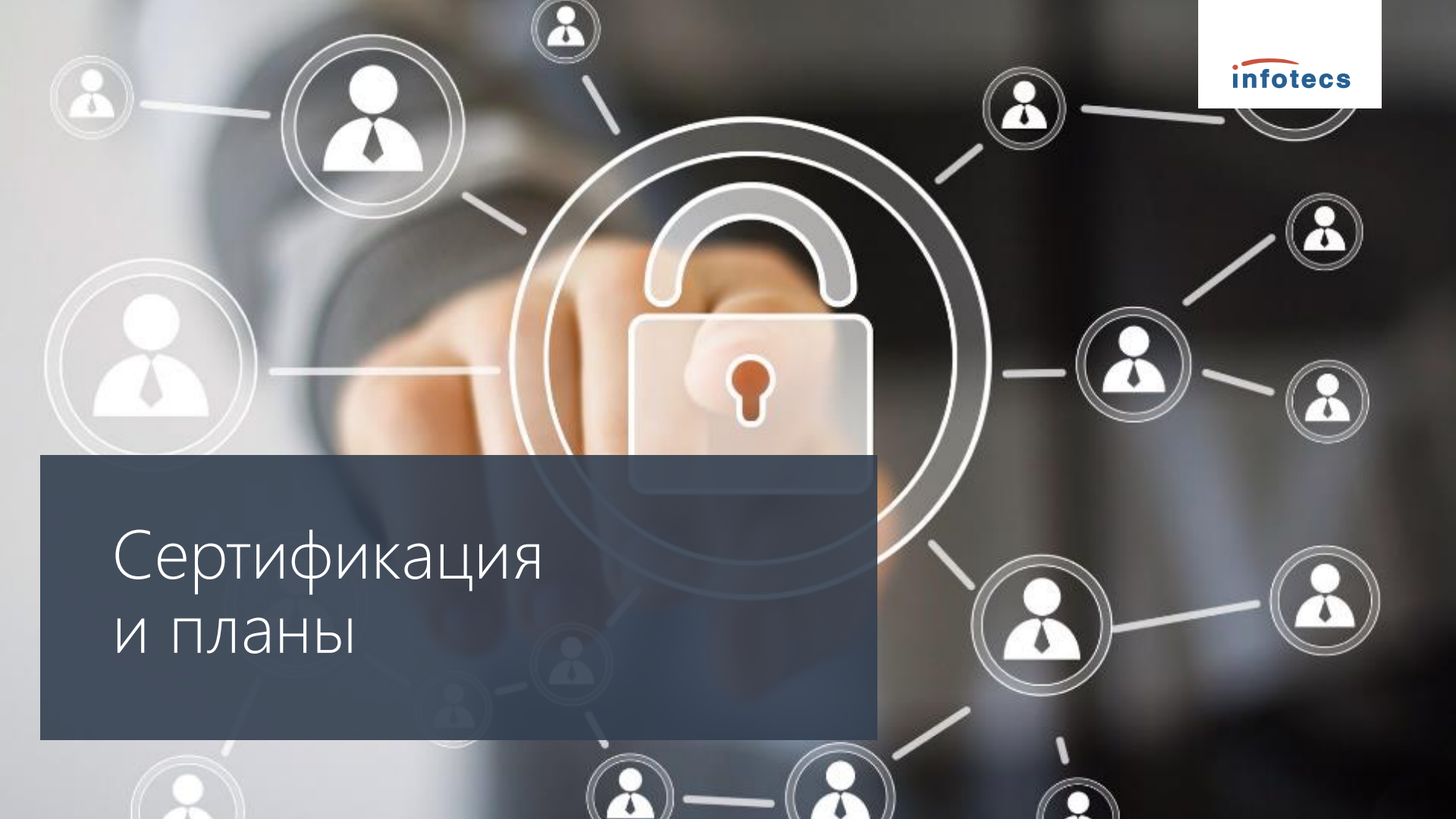
- ViPNet Administrator 4
- ViPNet Policy Manager 4
- ViPNet StateWatcher 4

Шлюзы безопасности:

- ViPNet Координатор-КВ2
- ViPNet Coordinator HW 4

VPN-клиенты:

- ViPNet Client 4



Сертификация и планы

Сертификация КВ4

ФСБ России на СКЗИ класса КВ:

- КВ1000: СФ/124-3678 от 12.04.2019 действителен до 12.04.2022
- КВ100, КВ2000, КВ5000 – в процессе сертификации

ФСБ России на МЭ 4 класса:

- В процессе сертификации (подписано положительное заключение)

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3678* от "*12*" *апреля* 2019 г.

Действителен до "*12*" *апреля* 2022 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»),
Обществу с ограниченной ответственностью «Линия защиты» (ООО «Лиза»).

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс **ViPNet Coordinator КВ 4** (исполнение ViPNet Coordinator КВ1000 на аппаратной платформе КВ1000 Q6) в комплектации согласно формуляру ФРКЕ.465614.001ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КВ и может использоваться для криптографической защиты (шифрование и имитозащита данных, передаваемых в IP-пакетах по сети связи общего пользования) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС»
сертификационных испытаний образца продукции № 781А-001001.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.465614.001ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.465614.001ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **А.М. Ивашко**

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 12 апреля 2019 г.

Первый заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России В.Н. Мартынов

Планы развития

- Переход на новый координатор (HW4.3.0)
  - Политики маршрутизации и проверка состояния шлюзов
  - Усовершенствованный механизм работы кластера горячего резервирования
  - Расширенная функциональность DHCP-сервера и DHCP-Relay
  - Поддержка EtherChannel и изменение значения MTU
- Удаленное управление по SSH
- Графический веб-интерфейс (webUI)
- Автоматическая смена серии ДСДР

Спасибо за внимание!

Vitaly.Belichko@infotecs.ru
Виталий Беличко