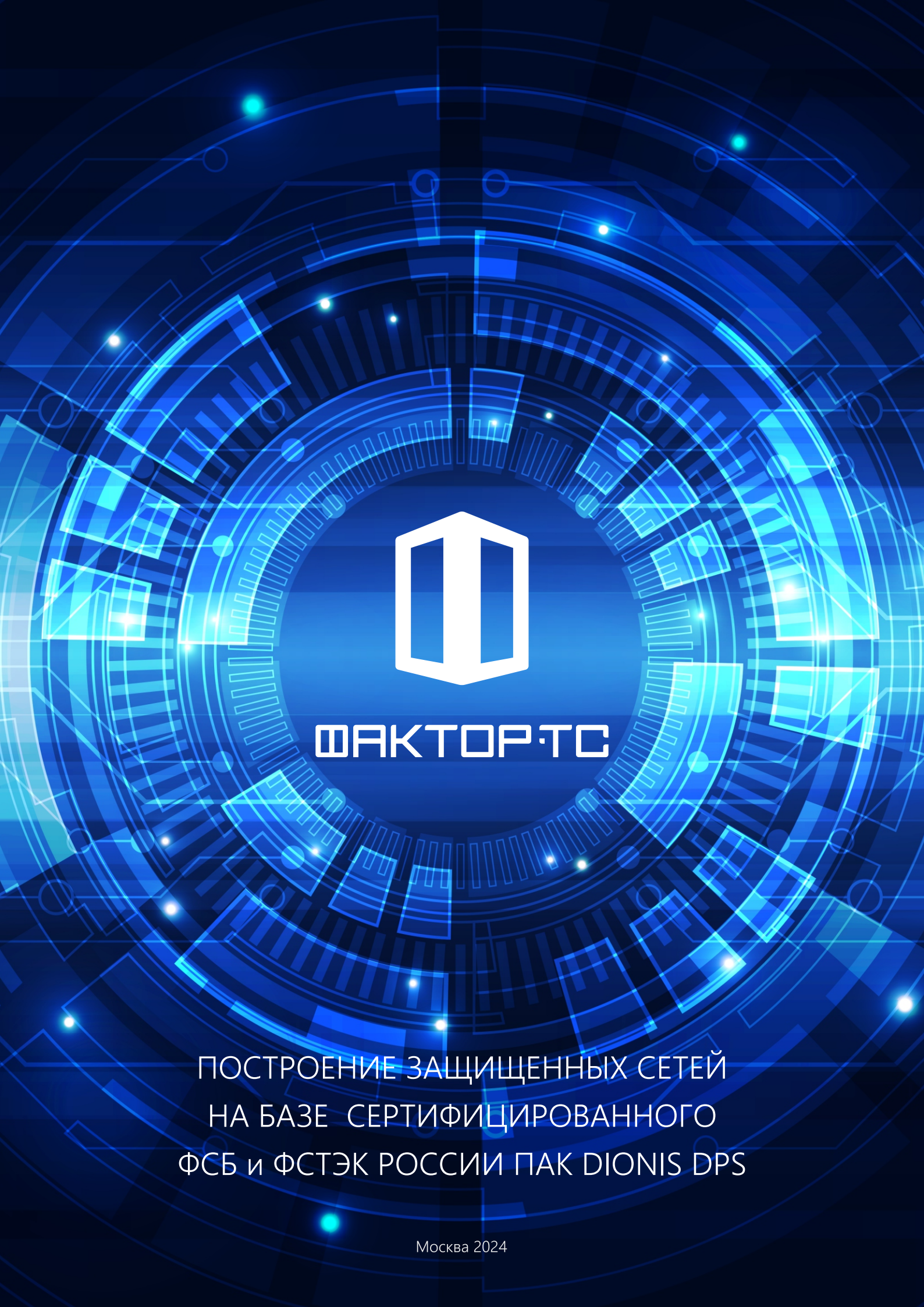
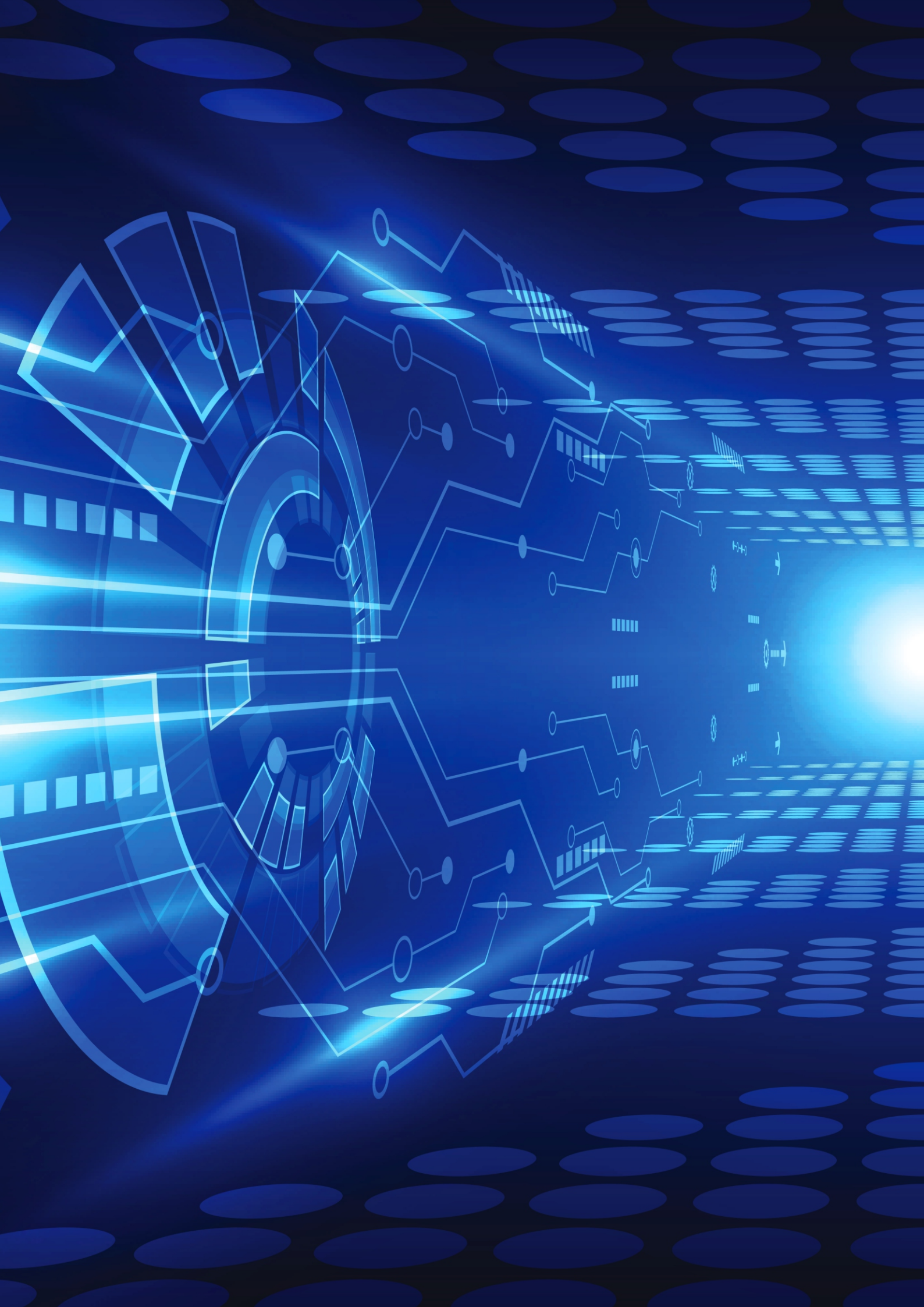
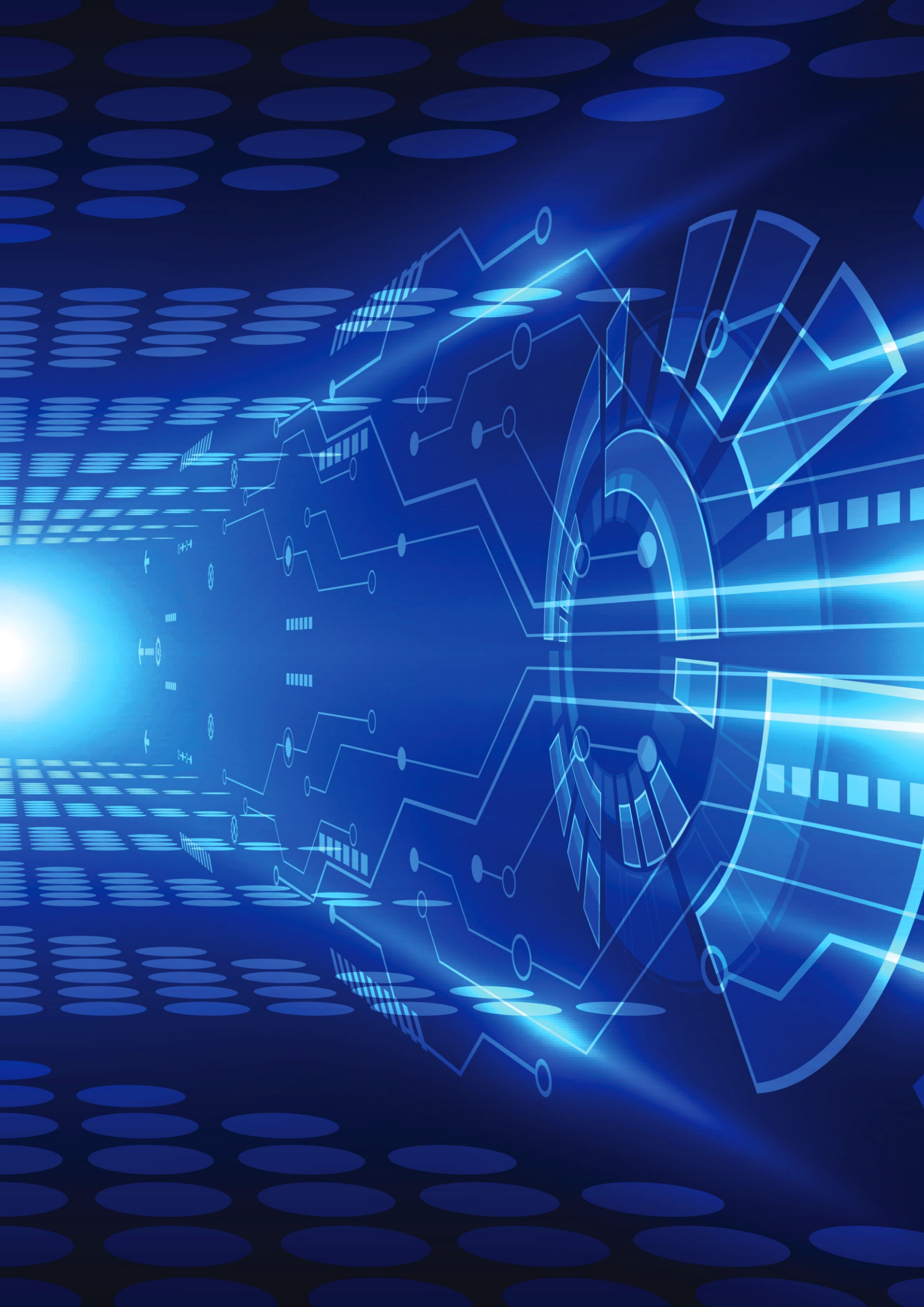


ПОСТРОЕНИЕ ЗАЩИЩЕННЫХ СЕТЕЙ НА БАЗЕ СЕРТИФИЦИРОВАННОГО ФСБ и ФСТЭК РОССИИ ПАК DIONIS DPS

Москва 2024





Архитектура защищенных сетей на базе Dionis DPS

Для защищенной передачи конфиденциальной информации через сети общего пользования в качестве пограничного устройства между защищаемыми локальными сетями и транспортной средой применяется ПАК Dionis DPS. В ПАК Dionis DPS реализованы алгоритмы шифрования в соответствии с государственными стандартами Российской Федерации.

ПАК Dionis DPS поддерживает два варианта VPN-туннелей, основное отличие которых состоит в том, что при их построении используются две разные схемы распределения ключей шифрования (симметричная и несимметричная).

Симметричная ключевая схема

Симметричная схема распределения ключей подразумевает использование отправителем и получателем для защиты информации симметричных ключей шифрования (ключей парно-выборочной связи). Стойкость основывается на сохранении в тайне симметричного ключа. Поэтому при использовании симметричной ключевой схемы требуются высоконадежные механизмы для распределения ключей.

В криптографических VPN-туннелях ПАК Dionis-DPS, которые используют симметричную ключевую схему, реализован ГОСТ 28147-89, ГОСТ Р 34.12-2015.

Симметричные ключи шифрования генерируются при помощи программы «Автоматизированное рабочее место генерации ключей» (АРМ ГК v.4) производства «Фактор-ТС».

Достоинства симметричной ключевой схемы

- Высокая скорость криптографической обработки.
- Простота реализации (за счет более простых операций).

Недостатки симметричной ключевой схемы

- Необходимо заранее планировать число абонентов.
- Требуется передача доверенным способом.

Рекомендации по применению

Криптографические VPN-туннели в ПАК Dionis-DPS на симметричных ключах шифрования эффективно использовать в любых сетях. Обеспечение непрерывности работы решается путем единовременной загрузки нескольких наборов ключей, каждый из которых используется ограниченное время (1 год). Такой механизм позволяет в момент обновления симметричных ключей посылать по защищенным каналам связи только команды на смену ключей без пересылки самих ключей. Это позволяет обеспечить автономность использования ПАК Dionis-DPS в течение нескольких лет.

Несимметричная ключевая схема

Несимметричная схема распределения ключей подразумевает использование в криптографических VPN-туннелях ПАК Dionis-DPS закрытые ключи и сертификаты X.509 (PKI - Public Key Infrastructure, инфраструктура открытых ключей). В этом случае в ПАК Dionis DPS применяются алгоритмы ГОСТ Р 34.12-2015, ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012, согласно спецификациям Технического комитета по стандартизации «Криптографическая защита информации» (ТК26).

Несимметричная ключевая схема – это такой способ распределения ключей, при котором для защиты канала связи между двумя абонентами оба абонента вырабатывают закрытый и открытый ключи. Закрытый хранится у его обладателя в тайне, а открытыми ключами абоненты обмениваются (о способе обмена далее). И только после этого с использованием определенного протокола на основе данных ключей получателем и отправителем формируется общий ключ шифрования (симметричный ключ).

Т. е. все участники информационного обмена обладают каждый своим открытым и закрытым ключом. Установление соединения (идентификация друг друга) происходит при использовании открытых и закрытых ключей, а после аутентификации и установления защищенного соединения между участниками на каждую передачу данных вырабатывается уникальный ключ шифрования, на котором и зашифровываются передаваемые данные.

Стойкость несимметричной схемы распределения ключей основана на сохранении в тайне закрытого ключа, математической сложности вычисления закрытого ключа по соответствующему открытому ключу и на обеспечении защиты открытого ключа от подмены злоумышленником в процессе его распространения по сети связи.

1. Взаимная аутентификация осуществляется на основе сертификатов X.509 v3 с использованием алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012

2. Выработка симметричного ключа для сеанса связи осуществляется с использованием алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, а шифрованием обеспечение целостности информации обеспечивается алгоритмом ГОСТ 34.12-2015

Архитектура открытых и закрытых ключей удобна для распределения ключей в системах с большим количеством географически удаленных друг от друга абонентов. Свой открытый ключ можно переслать любому адресату непосредственно перед установлением сеанса защищенной передачи данных. Для удобства можно разместить на открытом сетевом ресурсе открытые ключи всех участников защищенного обмена.

Но, несмотря на удобство эксплуатации такой инфраструктуры, появляется риск подмены открытых ключей. В случае для ЭП – это подделка подписи, а для шифрования – это возможность злоумышленника расшифровать сообщение, предназначенное легальному владельцу секретного ключа. Таким образом, возникает проблема доверия открытым ключам.

Для решения проблемы доверия к открытым ключам вводится третья сторона – Удостоверяющий центр. Удостоверяющий центр – сторона, чья честность неоспорима, а открытый ключ широко известен. Удостоверяющий центр организует выпуск сертификатов открытых ключей участников обмена информацией. При помощи открытого ключа Удостоверяющего центра все остальные участники информационного обмена проверяют подлинность сертификата открытого ключа любого участника.

Как было описано выше, открытый ключ может быть использован двумя способами:

1. Для проверки подписи владельца (аутентификация)
2. Для шифрования посылаемых ему данных (конфиденциальность)

Сертификат открытого ключа выдается Удостоверяющим центром (УЦ) и состоит из таких полей, как: открытый ключ владельца сертификата, срок действия, имя эмитента (удостоверяющего центра), имя владельца сертификата и самой важной части – цифровой подписи. Цифровая подпись удостоверяющего центра гарантирует подлинность сертификата пользователя. При формировании ЭП сертификата Удостоверяющий центр использует свой закрытый ключ. Для проверки подлинности сертификата пользователя (проверки ЭП УЦ) необходим сертификат (открытый ключ) удостоверяющего центра. Сертификат удостоверяющего центра для проверки ЭП всех получаемых пользователем сертификатов подписан самим удостоверяющим центром (самоподписанный сертификат) и носит название «корневой сертификат УЦ». Корневой сертификат должен быть доставлен каждому участнику обмена информацией доверенным образом, исключающим его подмену.

Для того чтобы Удостоверяющий центр выпустил сертификат на открытый ключ пользователя, пользователю необходимо отправить в удостоверяющий центр запрос на этот сертификат. Точный набор данных, включаемый в запрос, определяется регламентом удостоверяющего центра. В запрос обязательно включается имя пользователя, назначение запрашиваемого сертификата (ЭП или защищенный обмен), а также сам открытый ключ, на который создается сертификат, Таким образом, к моменту формирования запроса открытый ключ уже должен существовать. Для генерации запросов к УЦ на стороне удаленных пользователей используется программа МГК-3 производства ООО «Фактор-ТС». Электронная форма сертификата определяется стандартом X.509.

Каждый сертификат имеет ограниченный срок действия (1 год и 3 месяца, например). По истечении срока действия сертификат становится недействительным. По истечении срока действия сертификата удостоверяющего центра необходимо получить и установить в системе новый корневой сертификат УЦ. По истечении срока действия сертификата на открытый ключ пользователя необходимо сформировать запрос на новый сертификат.

Существует ряд причин, по которым действие сертификата бывает необходимо прекратить до окончания его срока действия.

Такими причинами могут быть:

1. Компрометация закрытого (секретного) ключа абонента
2. Замена сертификата в связи с изменениями реквизитов абонента

В случае прекращения срока действия сертификата Удостоверяющий центр отзывает соответствующий сертификат.

Если Удостоверяющий центр отзывает какой-либо сертификат, то он заносит его в список отозванных сертификатов (CRL – Certificate Revocation List). Все сертификаты, которые занесены в список отозванных сертификатов, – недействительны. Список сертификатов доводится до сведения всех пользователей. Перед началом любых действий с сертификатом какого-либо пользователя любой участник информационного обмена проверяет помимо подлинности сертификата еще и его отсутствие в списке отзыва сертификатов. Список отозванных сертификатов может находиться как локально, так и на специальном доступном для всех участников информационного обмена ресурсе. Владелец отозванного сертификата отправляет в удостоверяющий центр запрос на новый сертификат.

Преимущества:

- простота распределения ключевой информации в большой сети;
- удобные механизмы управления ключевой информацией

Недостатки:

- дополнительные затраты вычислительных ресурсов на выработку ключей на основе PKI

Рекомендации по применению

Несимметричная ключевая схема удобна в сетях с большим количеством стационарных серверов доступа и географически удаленных мобильных клиентов (от 200 и более), которые используют всевозможные физические среды доступа к сети и при этом активность таких абонентов носит скачкообразный характер.

ПРИМЕНЕНИЕ ПАК DIONIS DPS ДЛЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ СЕТЕЙ НА БАЗЕ СИММЕТРИЧНОЙ И НЕСИММЕТРИЧНОЙ КЛЮЧЕВЫХ СХЕМ

Организация защищенного доступа мобильных абонентов к ресурсам локальной сети по протоколу IPSec (ГОСТ). Класс защиты КС1, КС2, КС3

Решение имеет клиент-серверную архитектуру. В качестве сервера доступа выступает криптомаршрутизатор ПАК Dionis DPS, который ожидает подключений от удаленных клиентов. В качестве клиента выступает программное обеспечение DiSec производства компании «Фактор-ТС», которое устанавливается на различное клиентское оборудование (планшеты, ноутбуки, десктопы под управлением Windows 7, 8, 8.1,10, также разрабатывается клиент для ОС Linux). Защищенное соединение между клиентом и сервером устанавливается при помощи протокола IPSec (ГОСТ Р 34.12-2015,ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012). Услуги по предоставлению клиентам открытых и закрытых ключей выполняет удостоверяющий центр (УЦ) «Крипто-ПРО» или иной УЦ. Для генерации закрытых ключей и запросов к УЦ на выдачу сертификатов на стороне удаленных пользователей используется программное обеспечение «МГК-3» производства ООО «Фактор-ТС». Для хранения ключевой информации используется криптографический USB-токен (Rutoken, eToken), съемный USB-носитель и т. п. Реализуемый класс защиты КС1, КС2, КС3 (для классов КС2, КС3 дополнительно необходимо использовать сертифицированные ФСБ средства защиты (например, АПМДЗ). На рис. 1 изображена типовая схема реализации.

Необходимое оборудование и ПО	Назначение	Производитель
Криптомаршрутизатор ПАК Dionis DPS	Сервер доступа для абонентов	«Фактор-ТС»
Программное обеспечение DiSec	Подключение к серверу доступа	«Фактор-ТС»
Удостоверяющий центр (УЦ)	Управление инфраструктурой PKI	«Крипто-ПРО»
ПО оператора УЦ	Выпуск сертификатов по запросу	«Фактор-ТС»
ПО МГК (модуль генерации ключей)	Генерация запросов на сертификат	«Фактор-ТС»
Электронный токен («Рутокен»)	Хранение ключей и сертификатов	«Актив»
Планшет, ноутбук (Windows)	Установка ПО DiSec	Lenovo, Asus
Межсетевой экран (ФСБ МЭ3)	Защита УЦ от внешних угроз	
АПМДЗ (ФСБ) (для рабочих мест)	Для класса защищенности КС2, КС3	ПАК «Соболь» или аналог

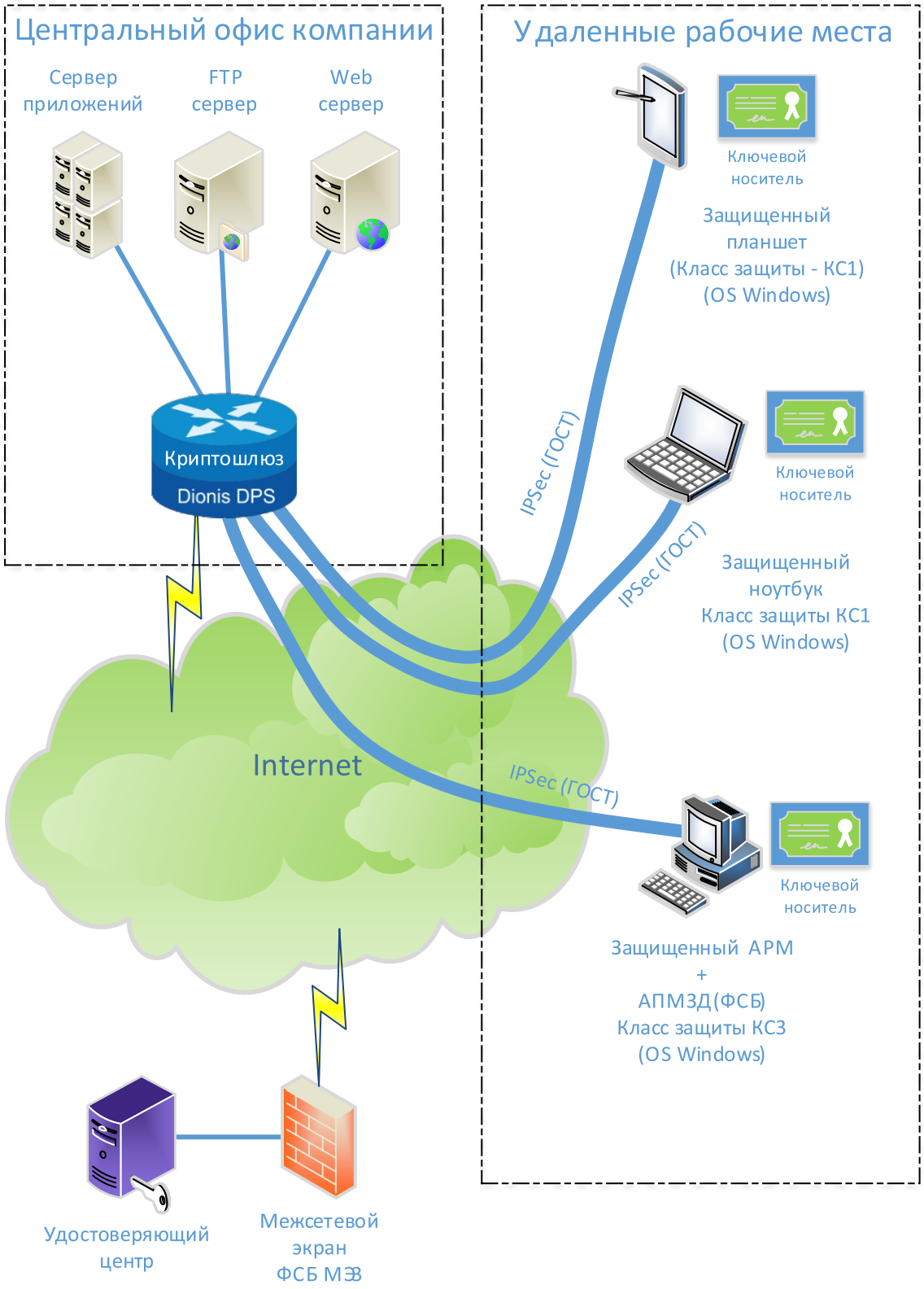


Рис. 1. Организация защищенного доступа мобильных абонентов к ресурсам локальной сети по протоколу IPSec (ГОСТ). Класс защиты КС1, КС2, КС3

Построение защищенной корпоративной сети на базе несимметричной ключевой схемы (PKI) с использованием протокола IPSec (ГОСТ). Класс защиты КС1, КС3

Решение имеет клиент-серверную архитектуру, такую же, как и в случае с организацией удаленного защищенного доступа мобильных абонентов (стр. 10), но при такой реализации в качестве клиентов центрального сервера доступа могут выступать сами ПАК Dionis DPS, за которыми находятся защищаемые ЛВС. ПАК Dionis DPS и клиентское ПО DiSec поддерживают технологию NAT Traversal, что позволяет всем подчиненным подразделениям и удаленным пользователям, кроме центрального узла, использовать динамические IP-адреса, получаемые по протоколу DHCP от провайдера. Услуги по предоставлению клиентам открытых и закрытых ключей выполняет удостоверяющий центр (УЦ) «Крипто-ПРО» или иной УЦ. Для генерации закрытых ключей и запросов к УЦ на выдачу сертификатов на стороне удаленных пользователей используется программное обеспечение «МГК-3» производства ООО «Фактор-ТС». Для хранения ключевой информации используется криптографический USB-токен (Rutoken, eToken), съемный USB-носитель и т. п. Реализуемый класс защиты КС2, КС3 (для класса КС3 на рабочих станциях необходимо дополнительно использовать сертифицированные ФСБ средства защиты, например АПМДЗ). На рис. 2 изображена типовая схема реализации.

Необходимое оборудование и ПО	Назначение	Производитель
Криптомаршрутизатор ПАК Dionis DPS	Сервер доступа для абонентов	«Фактор-ТС»
Криптомаршрутизатор ПАК Dionis DPS	Клиент сервера доступа и МЭ для ЛВС	«Фактор-ТС»
Программное обеспечение DiSec (клиент)	Подключение к серверу доступа	«Фактор-ТС»
Удостоверяющий центр (УЦ)	Управление инфраструктурой PKI	«Крипто-ПРО»
ПО МГК-4 (модуль генерации ключей)	Генерация запросов на сертификат	«Фактор-ТС»
ПО оператора УЦ	Выпуск сертификатов по запросу	«Крипто-ПРО»
Электронный токен («Рутокен»)	Хранение ключей и сертификатов	«Актив»
Планшет, ноутбук (ОС Windows)	Установка ПО DiSec	Lenovo, Asus
Межсетевой экран (ФСБ МЭ3)	Защита УЦ от внешних угроз	Любой
АПМДЗ (ФСБ) (для рабочих станций)	Для класса защищенности КС2, КС3	ПАК «Соболь» или аналог

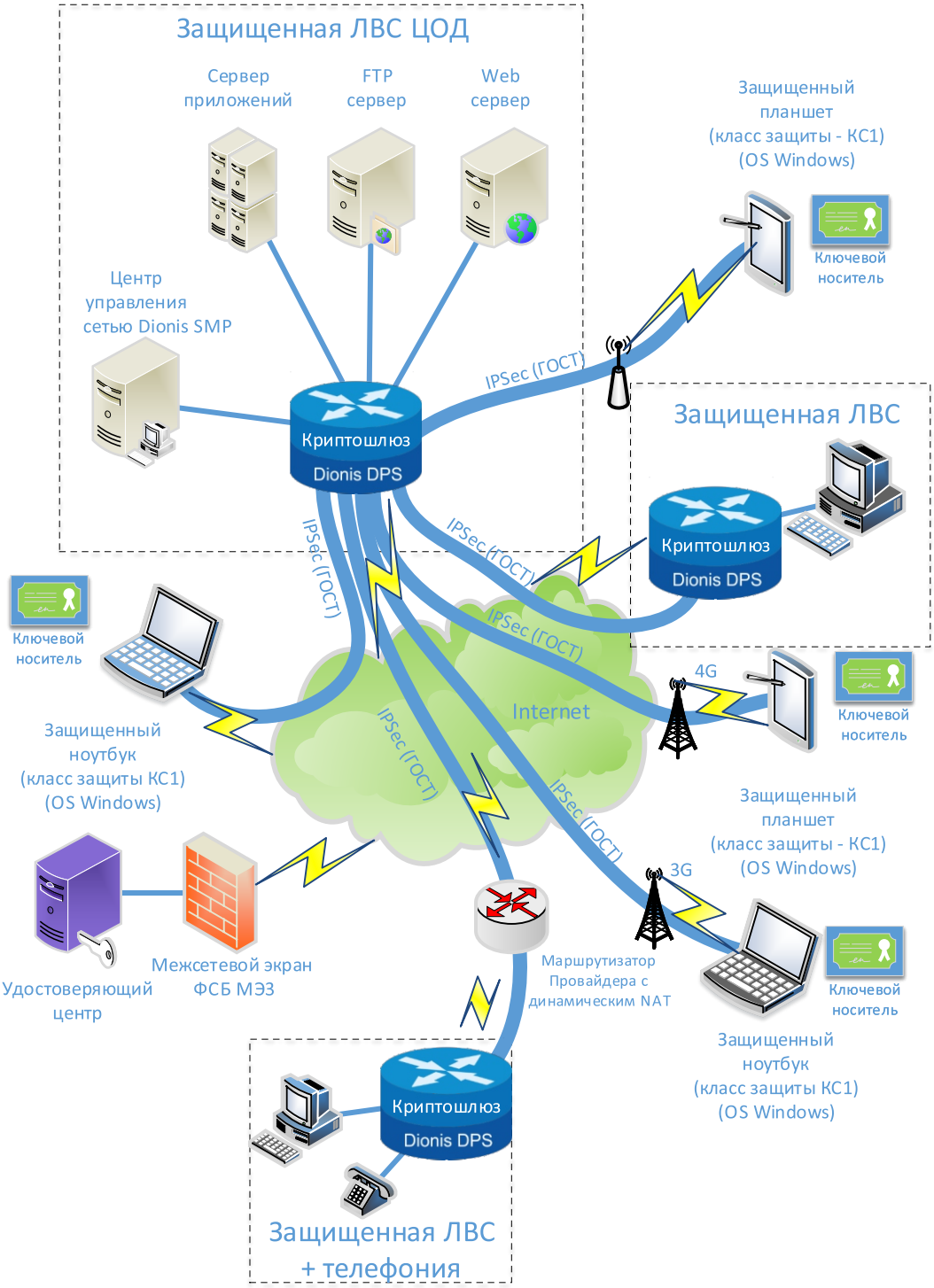


Рис. 2. Построение защищенной корпоративной сети на базе несимметричной ключевой схемы (PKI) с использованием протокола IPSec (ГОСТ). Класс защиты КС1, КС3

Организация корпоративного защищенного почтового обмена при помощи почтового клиента DioPost (КС1, КС2, КС3)

Программное обеспечение DioPost является почтовым клиентом, предназначенным для обмена как конфиденциальной почтовой корреспонденцией (с использованием криптографических средств защиты информации), так и открытой почтовой корреспонденцией (не защищенной криптографическими методами) между пользователями почтовых систем. Для организации обмена защищенной корреспонденцией используется несимметричная ключевая схема (PKI). Услуги по предоставлению клиентам открытых и закрытых ключей выполняет удостоверяющий центр (УЦ) «Крипто-ПРО» или иной УЦ. Для генерации закрытых ключей и запросов к УЦ на выдачу сертификатов на стороне удаленных пользователей используется программное обеспечение «МГК-3» производства ООО «Фактор-ТС». Для хранения ключевой информации используется криптографический USB-токен (Rutoken, eToken), съемный USB-носитель и т. п. Для обеспечения классов защиты КС2, КС3 необходимо дополнительно использовать сертифицированные ФСБ средства защиты на рабочих станциях с установленным ПО DioPost. На рис. 3 изображена типовая схема реализации защищенного обмена с использованием ПО DioPost.

Необходимое оборудование и ПО	Назначение	Производитель
Почтовый клиент DioPost	Защищенный почтовый обмен	«Фактор-ТС»
Почтовый сервер	Пересылка сообщений	Любой
ПО МГК-4 (модуль генерации ключей)	Генерация запросов на сертификат	«Фактор-ТС»
Удостоверяющий центр (УЦ)	Управление инфраструктурой PKI	«Крипто-ПРО»
ПО оператора УЦ	Выписка сертификатов по запросу	«Крипто-ПРО»
Электронный токен («Рутокен»)	Хранение ключей и сертификатов	«Актив»
Планшет, ноутбук (Windows)	Установка ПО DioPost	Lenovo, Asus
Межсетевой экран (ФСБ МЭ3)	Защита УЦ от внешних угроз	Любой
АПМДЗ (ФСБ) (для рабочих мест)	Для класса защищенности КС2, КС3	ПАК «Соболь» или аналог

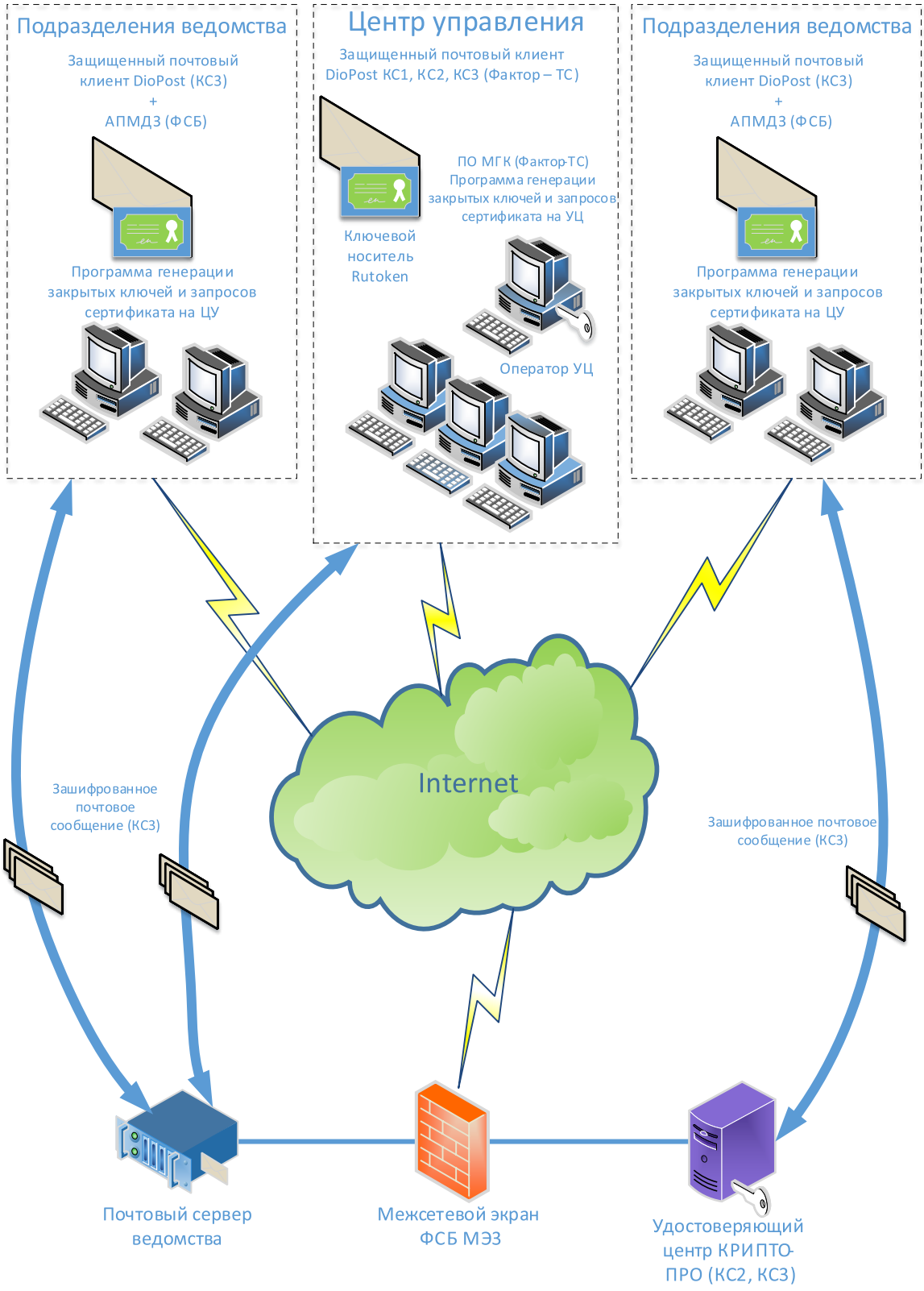


Рис. 3. Организация корпоративного защищенного почтового обмена при помощи почтового клиента DioPost (КС1, КС2, КС3)

Построение защищенной ведомственной сети с использованием симметричной ключевой схемы

Данное решение может быть построено по схеме «звезда» (такой вариант является частным примером, так как защищенная сеть может быть развернута и по принципу «каждый с каждым» или иным способом). Локальная вычислительная сеть (ЛВС) удаленного подразделения защищена межсетевым экраном ПАК Dionis DPS, который также является и криптомаршрутизатором. Каждый криптомаршрутизатор ПАК Dionis DPS удаленного подразделения связан одним криптографическим VPN-туннелем для защищенного обмена данными с центральным узлом, а также отдельным криптографическим туннелем (можно не использовать выделенный туннель для управления), через который проходит поток управления подчиненным узлом из центра управления сетью. Вся связь между удаленными криптомаршрутизаторами и защищаемыми ими ЛВС происходит через криптомаршрутизатор центрального узла. Симметричные ключи шифрования генерируются при помощи программы «Автоматизированное рабочее место генерации ключей» (АРМ ГК v.4) производства ООО «Фактор-ТС». Ключи записываются на USB-флеш-диски и доверенным способом доставляются на каждый узел. Возможно сгенерировать несколько ключей шифрования для каждого узла, чтобы единовременно загрузить их на узел и обеспечить автономность работы без необходимости физического доступа к узлу при плановой смене ключей шифрования. Плановую смену ключей можно выполнять при помощи центра управления сетью (Dionis SMP) по защищенному туннелю управления. По защищенному туннелю сами ключи шифрования не пересылаются; из Dionis SMP подается команда о замене старого ключа на новый, заранее загруженный при первом вводе ключей. На рис. 4 изображена типовая схема построения корпоративной сети с использованием симметричной ключевой схемы.

Необходимое оборудование и ПО	Назначение	Производитель
Криптомаршрутизатор ПАК Dionis DPS	Шифрование потока данных	«Фактор-ТС»
Центр управления сетью	Мониторинг и управление	«Фактор-ТС»
ПО АРМ ГК	Генерация ключей шифрования	«Фактор-ТС»
USB-флеш-диск	Хранение ключей шифрования	Любой

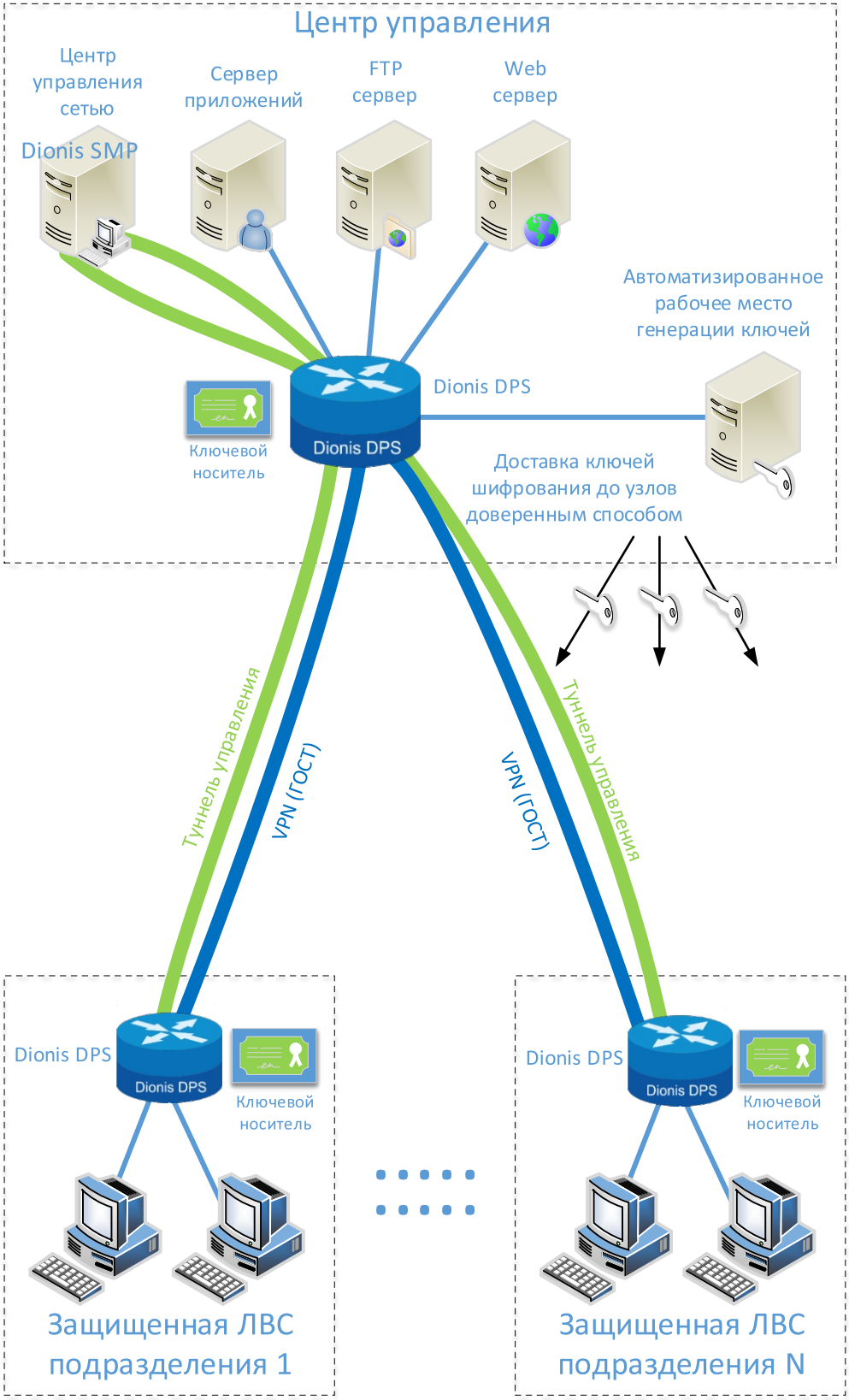


Рис. 4. Построение защищенной ведомственной сети с использованием симметричной ключевой схемы

Криптомаршрутизаторы для ЦОД. Создание защищенного канала связи (VPN ГОСТ 28147-89) со скоростью шифрования до 10 Гб/с

Данное решение позволяет организовать защищенный поток передачи данных (шифрование ГОСТ 28147-89) на скорости до 10 Гб/с при наличии нескольких каналов от разных провайдеров, не связанных между собой автономной системой. Для примера на рис. 5.1 приведена схема взаимодействия между основным центром обработки данных (ЦОД 1) и удаленным (ЦОД 2).

Изделия ПАК Dionis DPS используются в данной схеме не только как криптомаршрутизаторы (Dionis DPS 3 и Dionis DPS 4), но и как балансировщики нагрузки (Dionis DPS 1 и Dionis DPS 2). Задача балансировщика нагрузки — равномерно распределить трафик, поступающий из внутренней сети ЦОД, между криптомаршрутизаторами Dionis DPS 3 и Dionis DPS 4. Балансировщики Dionis DPS 1 и Dionis DPS 2 объединены в отказоустойчивый кластер (HA, High-Availability) и дублируют друг друга. Криптомаршрутизаторы Dionis DPS 3 и Dionis DPS 4 работают одновременно со скоростями шифрования равным 6 Гб/с (UDP 1500) каждый, что в сумме дает скорость шифрования свыше 10 Гб/с. Устройства Dionis DPS 3 и Dionis DPS 4 соединены с внешним каналом передачи данных через пограничные маршрутизаторы, которые также дублируют друг друга. В случае выхода из строя одного из криптомаршрутизаторов схема останется работоспособной, но общая производительность шифрования снизится до 6 Гб/с. Схема на стороне удаленного ЦОД 2 идентична схеме на стороне ЦОД 1. Криптографические туннели на симметричных ключах шифрования создаются между Dionis DPS 3 и Dionis DPS 4 и между Dionis DPS 6 и Dionis DPS 5 соответственно. Симметричные ключи шифрования генерируются при помощи программы «Автоматизированное рабочее место генерации ключей» (АРМ ГК v.4) производства ООО «Фактор-ТС». Ключи записываются на USB носитель и доверенным способом доставляются на каждый узел. На рис. 5.1 изображена типовая схема реализации высокоскоростного и отказоустойчивого взаимодействия между ЦОД.

Необходимое оборудование и ПО	Назначение	Производитель
Маршрутизатор Dionis DPS	Балансировка нагрузки	«Фактор-ТС»
Криптомаршрутизатор Dionis DPS	Шифрование потока данных	«Фактор-ТС»
Коммутатор (SFP+)	Коммутация оптоволокна	Любой
Пограничный маршрутизатор	Обеспечение доступа к внешней сети	Любой
ПО АРМ ГК	Генерация ключей шифрования	«Фактор-ТС»

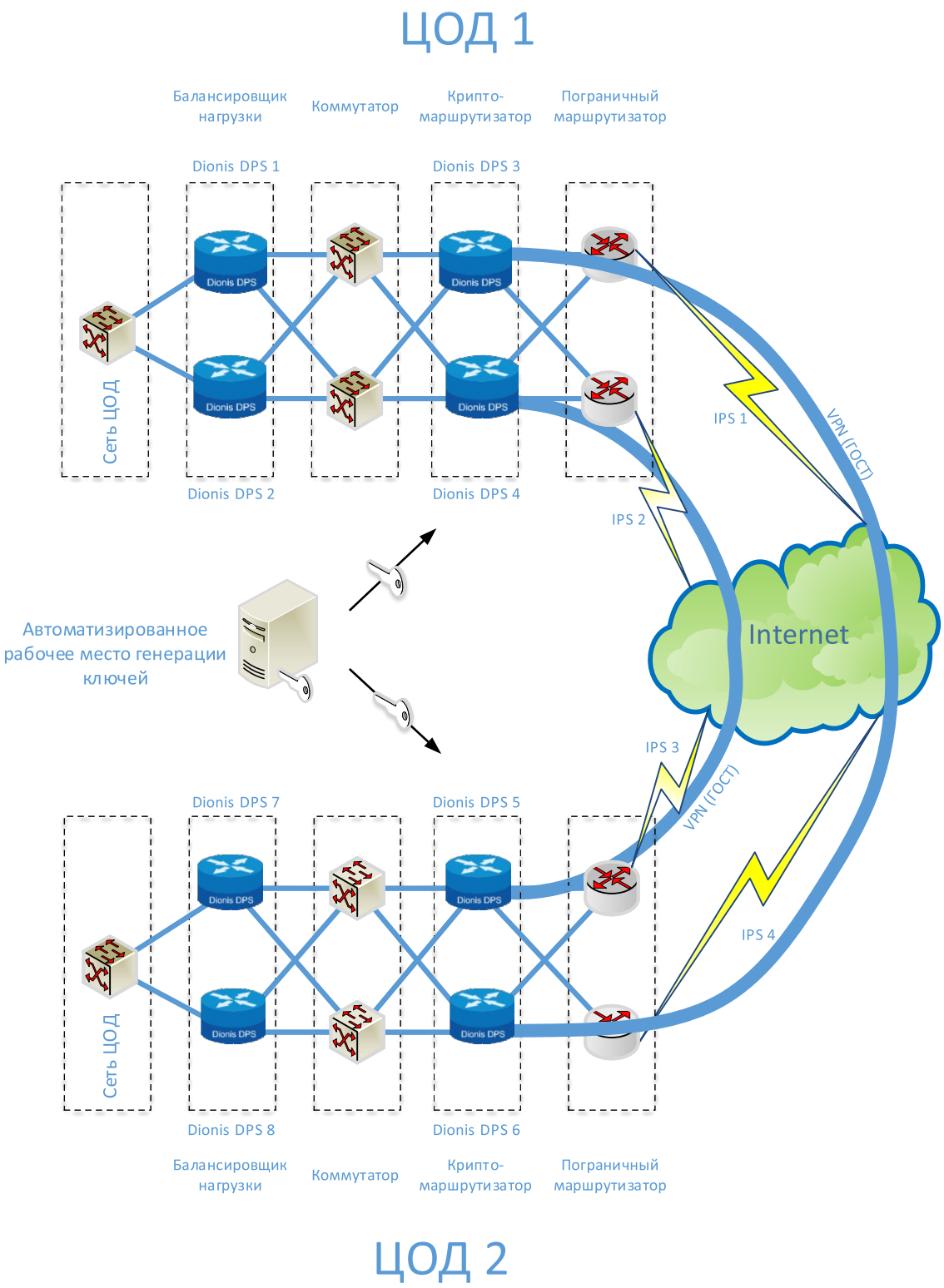


Рис. 5.1. Криптомаршрутизаторы для ЦОД. Создание защищенного канала связи (VPN ГОСТ 28147–89) со скоростью шифрования до 10 Гб/с при отсутствии автономной системы

Решение, изображенное на рис. 5.2, рекомендуется для использования при наличии автономной системы (AS) либо если есть планы по ее разворачиванию. Описанное решение позволяет организовать защищенный поток передачи данных с шифрованием по ГОСТ 28147-89 на скорости до 10 Гб/с.

Устройства Dionis DPS используются в данной схеме для решения двух задач: в качестве пограничных маршрутизаторов, принимающих анонсы BGP FullView от провайдеров, и в качестве криптошлюзов, объединенных в отказоустойчивый кластер (HA, High-Availability), для формирования зашифрованного соединения и обеспечения безопасности внутренних сетей ЦОД. Эти задачи специально разнесены по разным физическим устройствам для сохранения максимальной пропускной способности при пиковых нагрузках. При аварийном отключении одного из каналов связи стандартные механизмы работы протоколов BGP и OSPF приведут к автоматическому перераспределению трафика на рабочий канал, и таким образом препятствуют обрыву связи. То же самое произойдет и при выходе из строя одного из пограничных маршрутизаторов и/или коммутаторов. За счет использования отказоустойчивого кластера схема останется работоспособной даже при выходе из строя одного из криптошлюзов.
Симметричные ключи шифрования генерируются при помощи программы «Автоматизированное рабочее место генерации ключей» (АРМ ГК v.4) производства ООО «Фактор-ТС». Ключи записываются на USB-флеш-диски и доверенным способом доставляются на каждый узел, осуществляющий шифрование.

Необходимое оборудование и ПО	Назначение	Производитель
Маршрутизаторы Dionis DPS	BGP-маршрутизация	«Фактор-ТС»
Криптошлюзы Dionis DPS	Шифрование потока данных и защита периметра внутренних сетей (МЭ)	«Фактор-ТС»
Коммутаторы (SFP+)	Коммутация оптоволоконных каналов связи	Любой управляемый коммутатор 2-го уровня
ПО АРМ ГК	Генерация ключей шифрования	«Фактор-ТС»

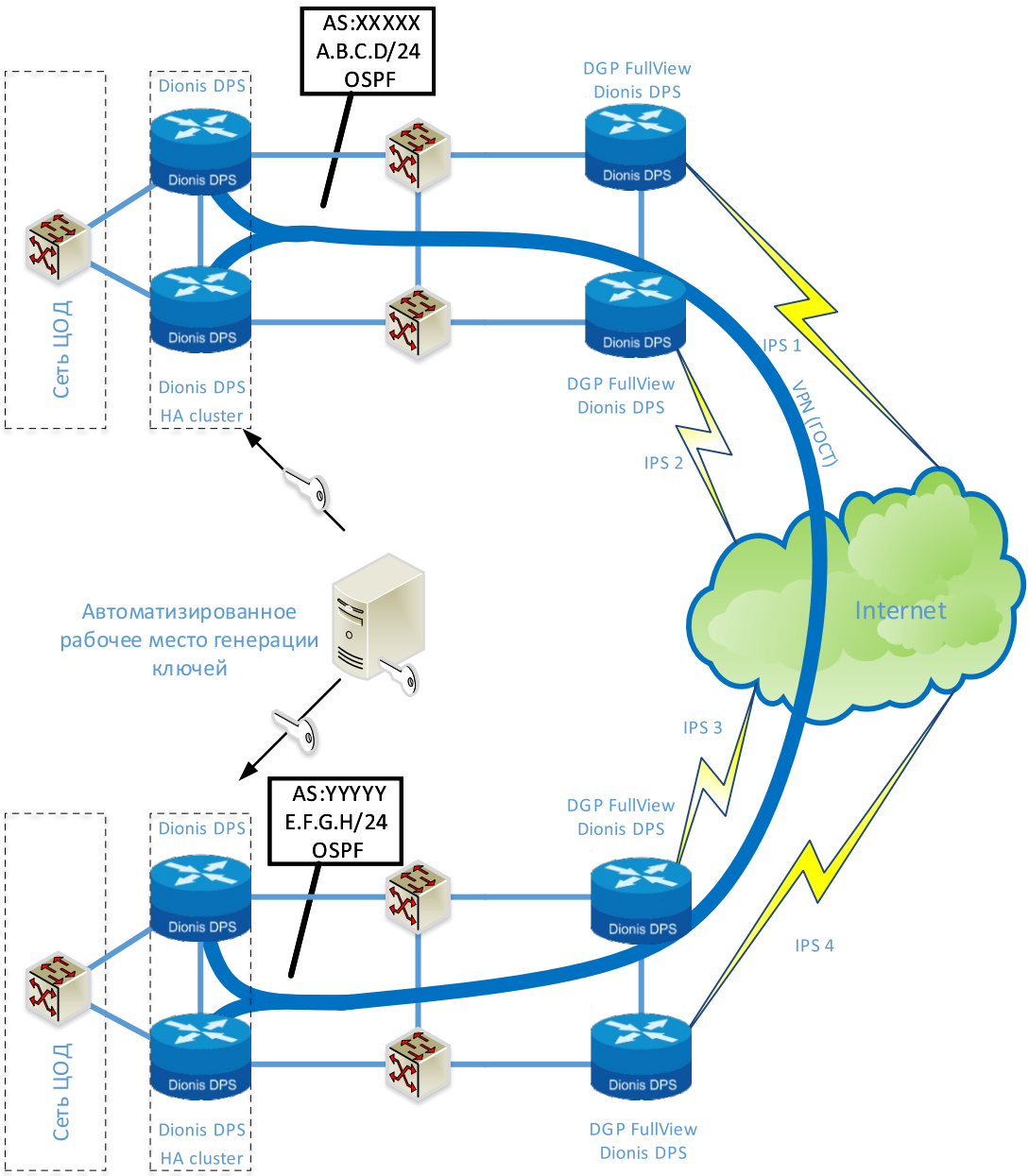


Рис. 5.2. Криптомаршрутизаторы для ЦОД. Создание защищенного канала связи (VPN ГОСТ 28147–89) со скоростью шифрования до 10 Гб/с при наличии автономной системы

Типовая схема построения географически распределенной сети ведомства с использованием симметричной и несимметричной ключевых схем (комбинированное решение)

Комбинированное решение использует симметричную и несимметричную ключевые схемы распределения ключей. Симметричная ключевая схема позволяет достигать сравнительно больших скоростей шифрования (приблизительно на 30 % больше по сравнению с несимметричной ключевой схемой распределения) и не требует разворачивания сложной инфраструктуры, поэтому для защиты магистральных каналов связи в крупной географически распределенной сети организации целесообразно использовать VPN-туннели с применением симметричной ключевой схемы распределения. Для построения подчиненных защищенных сетей целесообразно использовать несимметричную ключевую схему из-за разветвленности и постоянного роста этих сетей, а также из-за большого количества удаленных мобильных абонентов. При использовании несимметричной ключевой схемы возможно интегрировать программные и аппаратные решения компании «Фактор-ТС» в уже существующую инфраструктуру PKI с использованием существующих у заказчика удостоверяющих центров. Криптомаршрутизаторы крупных региональных центров находятся на границе двух ключевых схем и осуществляют перешифрование и перенаправление трафика из одного типа VPN-туннелей в другой. На рис. 6 изображена типовая схема реализации комбинирования ключевых схем.

Необходимое оборудование и ПО	Назначение	Производитель
Несимметричная ключевая схема		
Криптомаршрутизатор ПАК Dionis DPS	Сервер доступа для абонентов	«Фактор-ТС»
Криптомаршрутизатор ПАК Dionis DPS	Клиент сервера доступа и МЭ для ЛВС	«Фактор-ТС»
Программное обеспечение DiSec	Подключение к серверу доступа	«Фактор-ТС»
Удостоверяющий центр (УЦ)	Управление инфраструктурой PKI	«Крипто-ПРО»
ПО МГК (модуль генерации ключей)	Выпуск сертификатов по запросу	«Фактор-ТС»
ПО оператора УЦ	Генерация запросов на сертификат	«Крипто-ПРО»
Электронный токен («Рутокен»)	Хранение ключей и сертификатов	«Актив»
Планшет, ноутбук (Windows)	Установка ПО DiSec	Lenovo, Asus
Межсетевой экран (ФСБ МЭ3)	Защита УЦ от внешних угроз	Любой
АПМДЗ (ФСБ) (для рабочих мест)	Для класса защищенности КС2, КС3	ПАК «Соболь» или аналог
Симметричная ключевая схема		
Криптомаршрутизатор Dionis DPS	Шифрование потока данных	«Фактор-ТС»
Центр управления сетью	Мониторинг и управление	«Фактор-ТС»
ПО АРМ ГК	Генерация ключей шифрования	«Фактор-ТС»
USB-флеш-диск	Хранение ключей шифрования	Любой

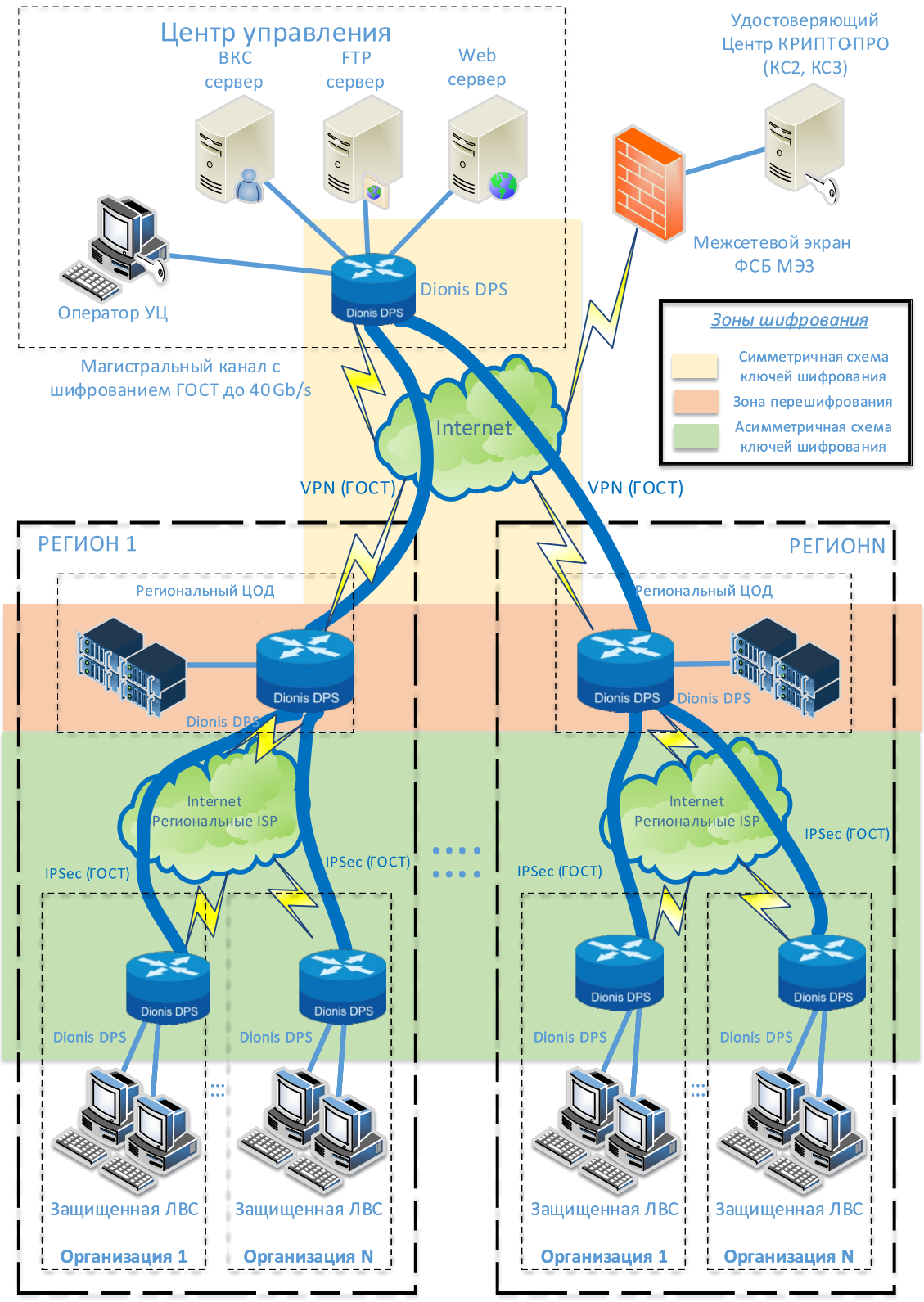


Рис. 6. Типовая схема построения географически распределенной сети ведомства с использованием симметричной и несимметричной ключевых схем

Объединение удаленных корпоративных ЛВС в единую защищенную телекоммуникационную сеть (L2 VPN)

Решение, изображенное на Рис. 7, позволяет объединить две территориально распределённые сети в единую сеть. Для этого в устройствах Dionis DPS настраивается шифрованное соединение канального уровня. Устройства обоих сетей будут взаимодействовать между собой, как если бы между ними было проложено прямое физическое соединение. К достоинствам L2 VPN можно отнести возможность применения любых протоколов 3-го уровня и выше (IPv4, IPv6, NetBIOS, SPX/IPX и т. п.) без необходимости согласования с провайдером и наличия у него соответствующего оборудования. Важно также и то, что применение L2 VPN хорошо сочетается с другими полезными технологиями 2-го уровня, например обеспечивающими быструю сходимость сети (RSTP и т. п.). Может работать за NAT.

Необходимое оборудование и ПО	Назначение	Производитель
Маршрутизаторы Dionis DPS	Организация L2 VPN	«Фактор-ТС»

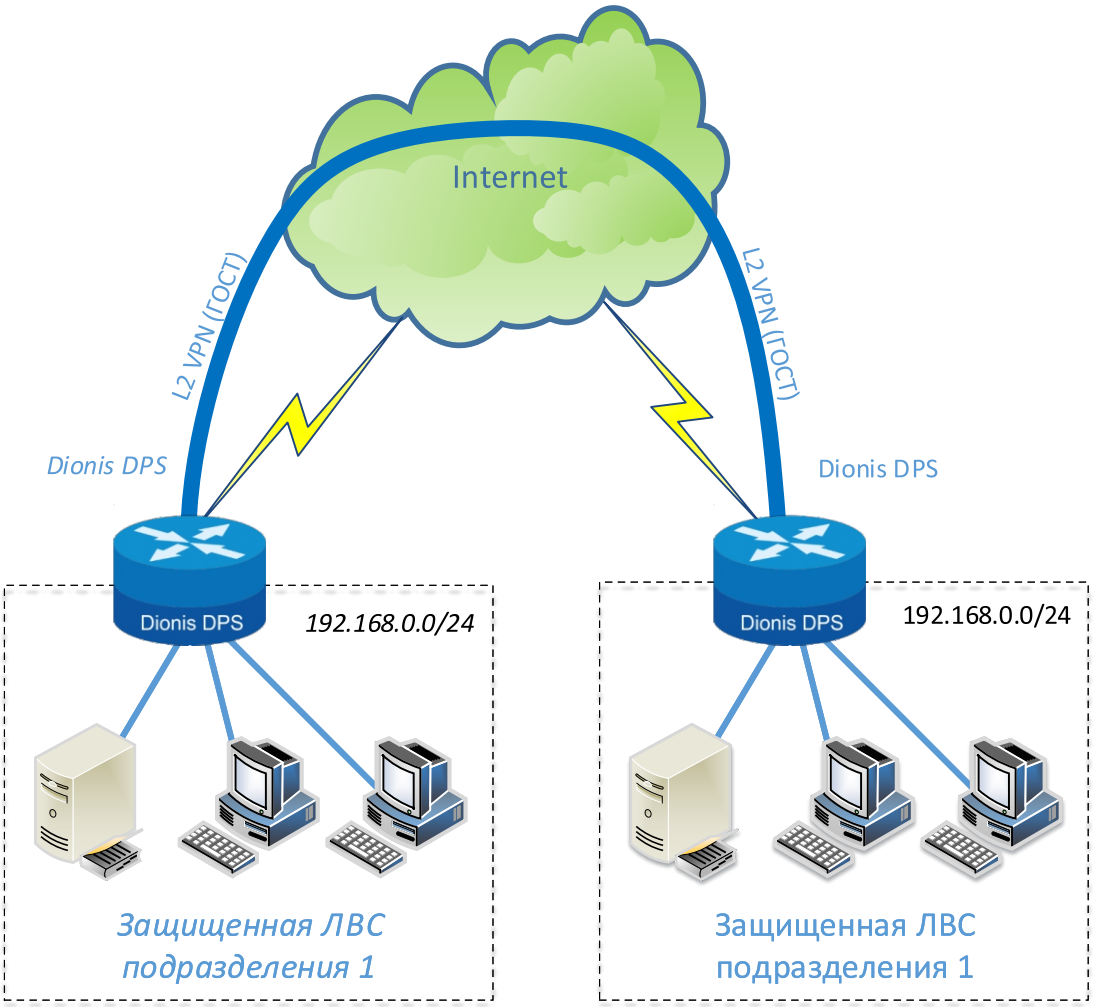


Рис. 7. Типовая схема объединения двух территориально разнесенных сетей с использованием L2 VPN с шифрованием по ГОСТ 28147-89

Защита корпоративной сети от сетевых угроз при помощи встроенного в ПАК Dionis DPS детектора атак (IPS/IDS). Создание единого центра управления политиками безопасности сети

На рис. 8 приведена типовая схема объединения сетей головного офиса и удаленных подразделений. Все ключевые задачи реализованы на устройствах Dionis DPS. Для организации безопасного объединения сетей используется шифрование по ГОСТ 28147-89. Высокая доступность серверов головного офиса достигается построением отказоустойчивого кластера, а защита от сетевых угроз достигается применением системы обнаружения вторжений IPS/IDS.

Устройства Dionis DPS используют технологию IPS — компонентные сигнатуры, которые позволяют распознавать и обеспечивать защиту как против известных, так и против неизвестных атак. В результате при атаках (реальных или потенциальных) данные устройства помогают значительно снизить влияние на такие важные аспекты, как полезная нагрузка, закрытая информация, а также предотвратить дальнейшее распространение компьютерных атак внутри защищаемой сети. База данных СОВ, включающая информацию о глобальных атаках и вторжениях, постоянно пополняется и обновляется через Интернет с серверов компании «Фактор-ТС». Эти сигнатуры, а также уникальные алгоритмы, применяемые в устройствах Dionis DPS, обеспечивают высокую точность обнаружения при минимальном количестве ошибочных срабатываний.

Управление детекторами атак происходит при помощи системы Dionis SMP, которая является ситуационным центром для сбора и анализа информации о сетевых атаках на все ЛВС организации.

Необходимое оборудование и ПО	Назначение	Производитель
Криптомаршрутизаторы Dionis DPS	Организация защищенных VPN	«Фактор-ТС»
Детектор атак Dionis DPS	Защита от сетевых атак	«Фактор-ТС»
Система Dionis SMP	Централизованное управление детекторами атак	«Фактор-ТС»

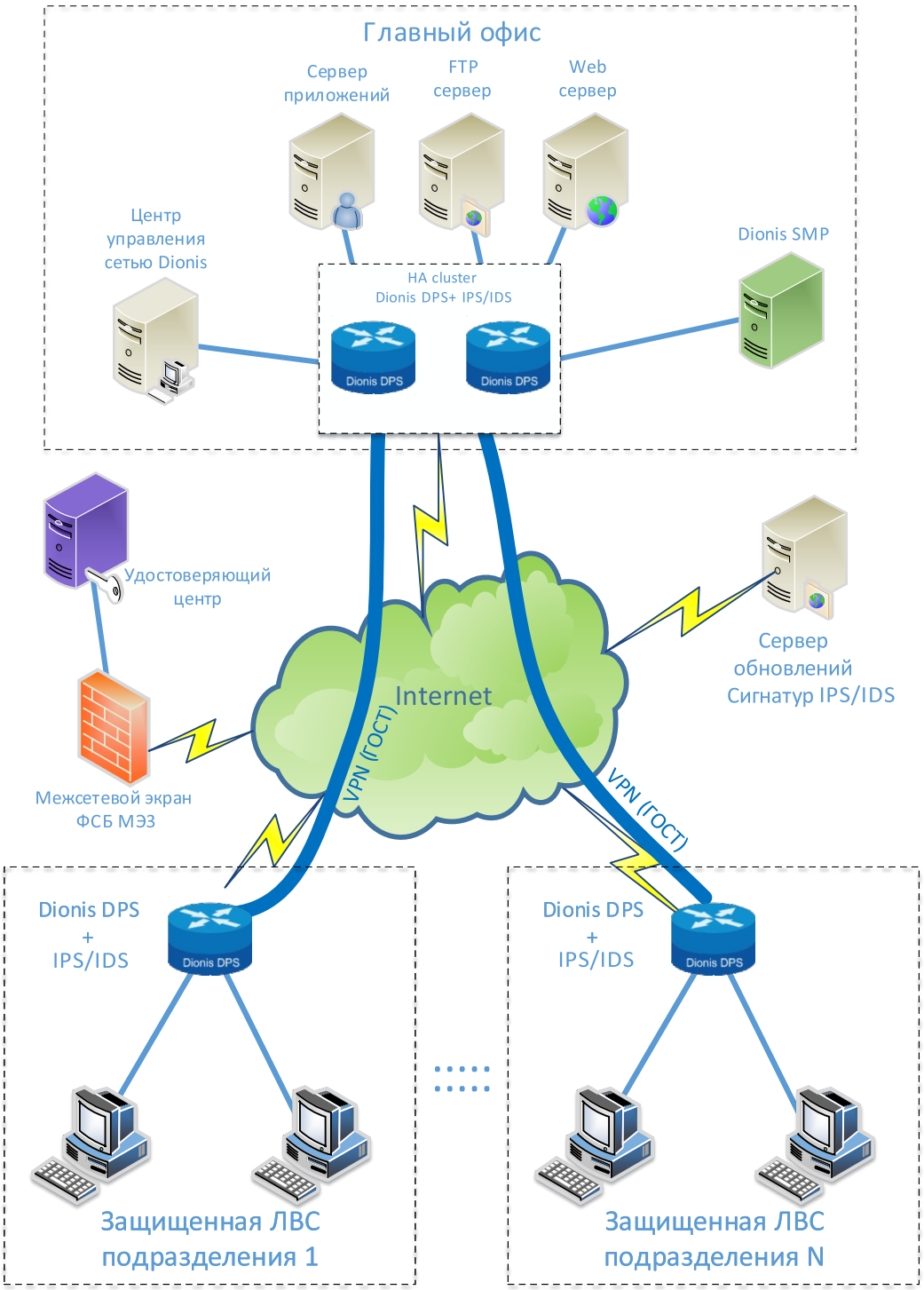


Рис. 8. Типовая схема объединения сетей главного офиса компании и территориально разнесенных подразделений с использованием отказоустойчивого кластера, VPN с шифрованием по ГОСТ 28147-89, детектором атак IPS/IDS

Москва, 1-й Магистральный пр-д,
дом 11, строение 1

dps.factor-ts.ru
sales@factor-ts.ru
+7 (495) 644 31 30