

VII Конференция «IT-Security Conference 2022»



s•terra

С-Терра Бел: Комплексный подход к защите информации

Сапрыкин А.М.
директор ООО «С-Терра Бел»,
член Оргкомитета международной конференции «Инфофорум»

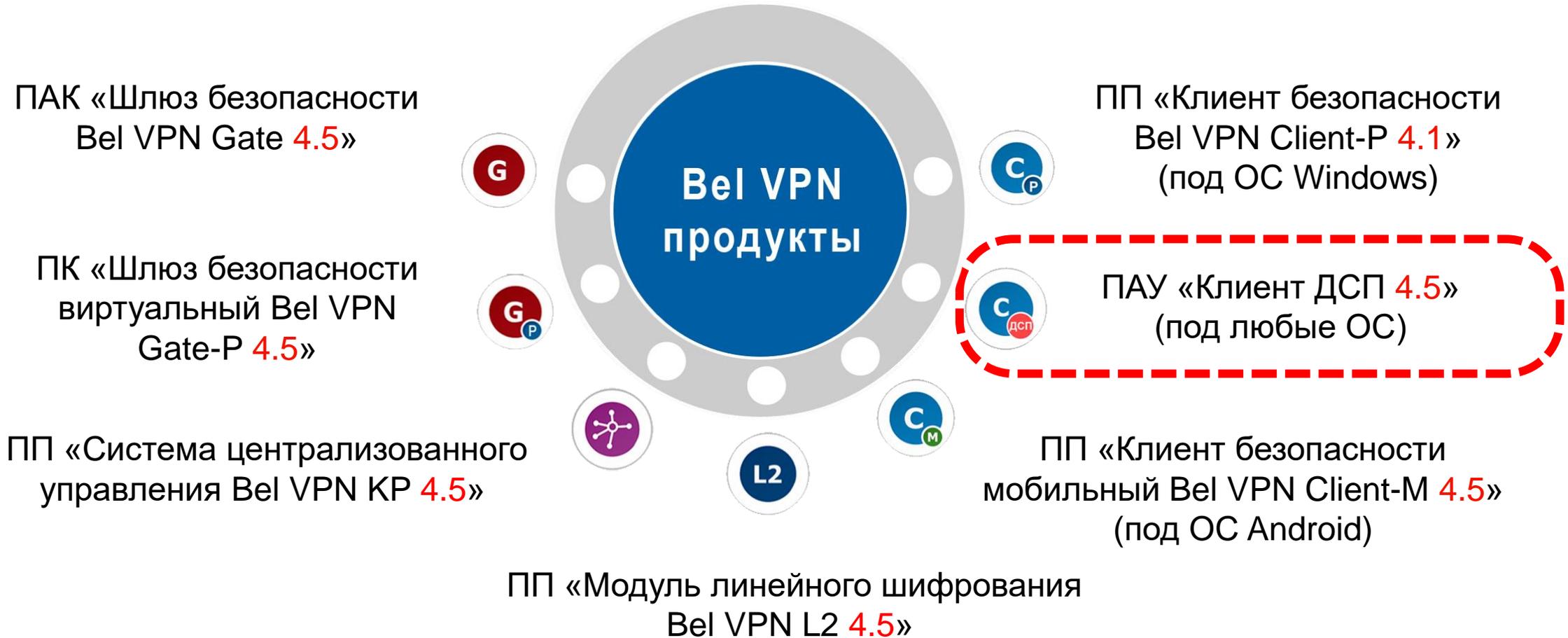
26.01.2022, Минск

Комплексный подход к защите информации

Bel VPN продукты компании С-Терра Бел позволяют обеспечить защиту в ИС любой сложности и защищенности, включая ИС классов 3-дсп и 4-дсп. Комплексный подход заключается:

- функционально полный набор Bel VPN продуктов
- наличие программно-аппаратных и программных продуктов
- масштабируемые по производительности (от 100 Мб/с до 15 Гб/с) и кол-ву туннелей шлюзы безопасности
- удаленный доступ для рабочих мест с практически всеми возможными ОС
- наличие отказоустойчивых (кластерных) решений и возможность балансировки
- наличие виртуальных решений с производительностью до 10 Гб/с
- наличие системы централизованного управления
- наличие модуля канального уровня
- работа с технологическими сертификатами ГосСУОК и «preshared key» (PSK)
- возможность маркировки и приоритезации трафика
- событийное протоколирование и мониторинг
- наличие сертифицированного межсетевого экрана
- процедура по обновлению пакетов ОС Debian GNU/Linux 9 (с репозитория на сайте)

Актуальные Bel VPN продукты (функционально полный набор)



Актуальные Bel VPN продукты (функционально полный набор)



комплекс программно-аппаратный **«Шлюз безопасности Bel VPN Gate 4.5»** – масштабируемый набор шлюзов, предназначен для защиты межсетевого обмена данных в территориально распределенных IP-сетях. Поставляется на аппаратных платформах производства РБ



программный комплекс **«Шлюз безопасности Bel VPN Gate-P 4.5»** по функциональности аналогичен ПАК, работает в виртуальных средах (VMware, ESXi, Citrix XenServer, Microsoft Hyper-V, KVM), а также на АП заказчика



программный продукт **«Клиент безопасности Bel VPN Client-P 4.1»** предназначен для защиты доступа удаленного пользователя к ведомственной сети, защищаемой шлюзом безопасности, работает со всеми версиями ОС Windows



программный продукт **«Клиент безопасности мобильный Bel VPN Client-M 4.5»** предназначен для защиты доступа удаленного пользователя к ведомственной сети, защищаемой шлюзом безопасности

Функционирует на мобильных устройствах (планшетах, смартфонах) со всеми версиями ОС Android

Актуальные Bel VPN продукты (функционально полный набор)



устройство программно-аппаратное **«Клиент ДСП 4.5»** предназначен для защиты доступа удаленного пользователя к ведомственным ИС классов 3-дсп, 4-дсп, а также рабочих мест, использующих нестандартные ОС (MacOS, Linux и т.п.) и находящихся в особых условиях



программный продукт **«Bel VPN KP 4.5»** предназначен для централизованного управления и мониторинга продуктами Bel VPN Gate 4.5 (входит в состав шлюза)/Client-P 4.1/Client-M 4.5 Функционирует под управлением ОС Windows Server



программный модуль **«Bel VPN L2 4.5»** предназначен для защиты сетевого трафика на канальном уровне (входит в состав шлюза)

Bel VPN продукты версии 4.5 **несовместимы** с иными СКЗИ других производителей. Разрыв соединения происходит на начальном этапе аутентификации продуктов.



Программный комплекс «Шлюз безопасности **Bel VPN Gate 4.5**»

Программный комплекс «Шлюз безопасности **Bel VPN Gate 4.5**» обеспечивает функциональность Bel VPN Gate в виртуальных средах (VMware ESXi, Citrix XenServer, Microsoft Hyper-V).

Производительность ПК **до 10 Гб/с** (ограничена возможностью виртуального интерфейса). В режиме MTU 1500 (макс.длина пакета) на практике (A1) была достигнута производительность **5,2 Гб/с**

- операционная система Debian 9
- новые возможности в cs_console:
 - настройка NHRP, VRRP, настройка получения адреса по DHCP, привязки локального сертификата и сертификата УЦ к криптокарте
 - просмотр информации об ISAKMP и IPsec соединениях, о криптоконтейнерах и сертификатах, о сетевых интерфейсах, состояния и статистики VRRP
- интеграция непосредственно в виртуальную инфраструктуру
- уведомления об окончании срока действия локального сертификата (и локальной лицензии)
- реализация сценариев обеспечения высокой доступности и отказоустойчивости
- оперативная адаптация к меняющимся задачам и требованиям сетевых приложений и инфраструктуры
- легкое сохранение или восстановление резервной копии
- эффективное использование вычислительных ресурсов
- экономия электроэнергии и места в стойке





Комплекс программно-аппаратный «Шлюз безопасности Bel VPN Gate 4.5»

Комплекс программно-аппаратный «Шлюз безопасности Bel VPN Gate 4.5» – масштабируемый набор шлюзов, предназначенся для защиты межсетевого обмена данных в территориально распределенных IP-сетях

- операционная система (Debian 9)
 - расширены пакеты драйверов
- новые возможности в cs_console
- более высокая производительность шифрования трафика
- сертифицированный межсетевой экран – по СТБ 34.101.73-2017 (пункты 7.3, 7.4)
- совместимость с Bel VPN продуктами версии 4.1
- используются **аппаратные платформы белорусского производства**



Все комплексы программно-аппаратные Bel VPN Gate 4.5 выполнены на аппаратных платформах белорусского производства (производительность до 15 Гб/с включительно – «Шлюз 15G»)



Аппаратные платформы белорусского производства

Все комплексы программно-аппаратные **Bel VPN Gate 4.5** выполнены на аппаратных платформах белорусского производства

	Целевое назначение	Количество туннелей шифрования (до)	Производительность	
			MTU 1500	MTU > 9000 (jumbo-frame)
Gate 100 Gate-P 100	Малые офисы	10	до 100 мбит/с до 250 мбит/с	
Gate 1000 Gate-P 1000		50	до 400 мбит/с до 1 Гбит/с	
Gate 3000 Gate-P 3000	Средние офисы	1000	до 1 Гбит/с до 2 Гбит/с	
Gate 7000 Gate-P 7000	Крупные офисы ЦОДы, СХД	неограниченно	до 6,6 Гбит/с до 5,2 Гбит/с	до 15 Гбит/с до 9,7 Гбит/с

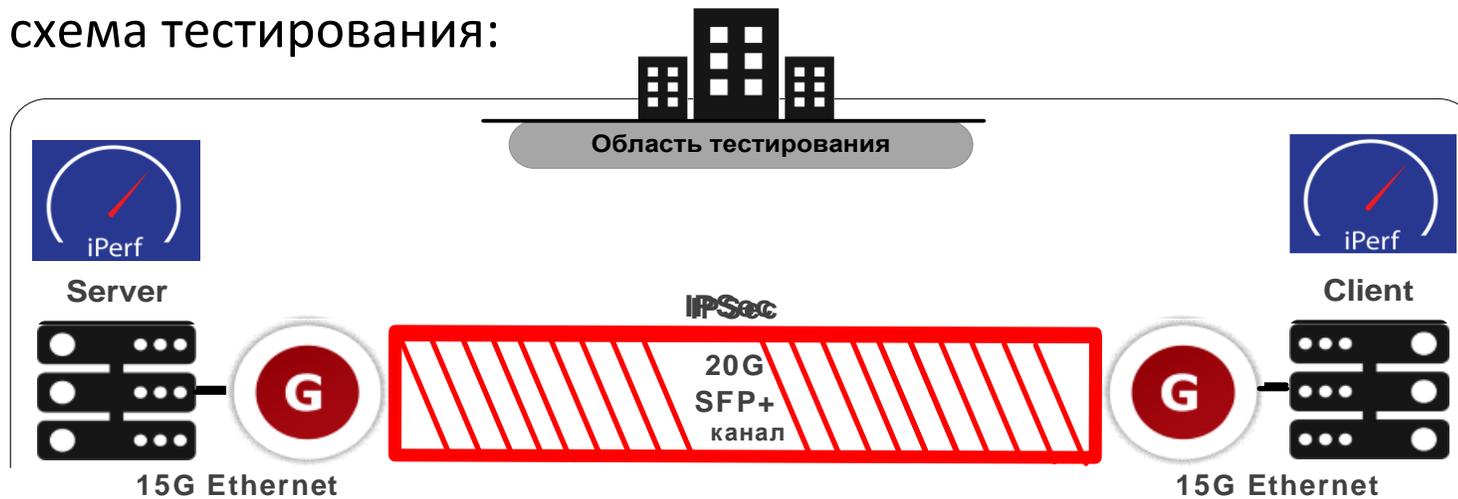


15

Гбит/с

Производительность до 15 Гбит/с

- аппаратная платформа белорусского производства
- схема тестирования:



QR-CODE – узнать подробности



Параметры защищенного соединения:

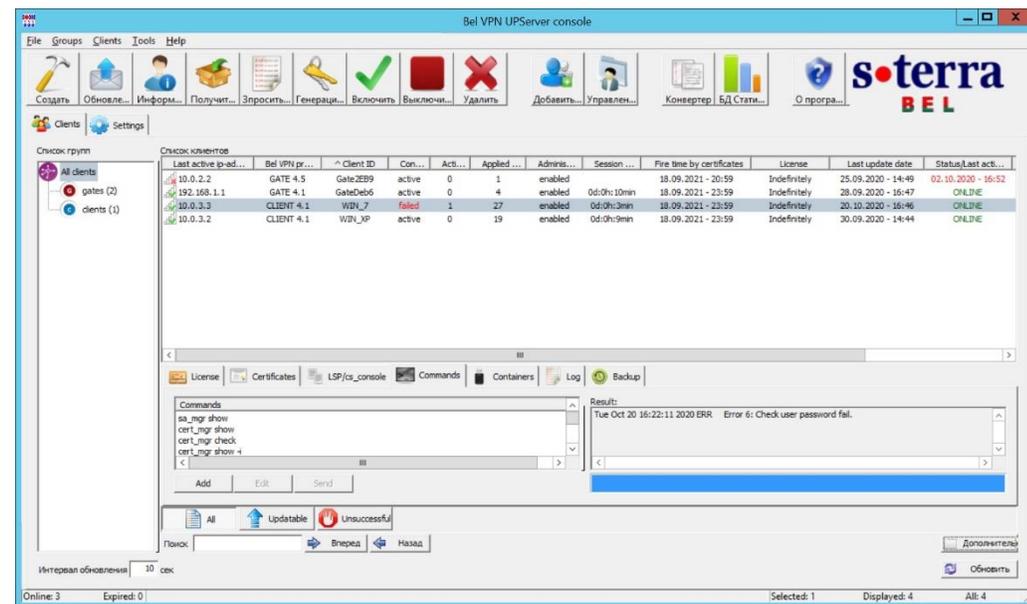
- алгоритм шифрования – СТБ 34.101.31-2011 (раздел 6.4 – режим гаммирования с обратной связью)
- алгоритм контроля целостности – СТБ 34.101.31-2011 (раздел 6.6 – выработка имитовставки)

4.5
version

ПП «Система централизованного управления Bel VPN KP 4.5»

Усовершенствованный программный продукт «Система централизованного управления Bel VPN KP 4.5» предназначен для централизованного управления Bel VPN продуктами

- обновлен пользовательский интерфейс
- в работу продукта встроена система проверки целостности файлов и автоматического устранения ошибок при их наличии
- быстрое отслеживание состояния Bel VPN продуктов
- встроены дополнительный контроль, анализ и сбор данных при добавлении Bel VPN продуктов в панель управления
- увеличена производительность обмена данными и обновления Bel VPN продуктов
- совместимость с Bel VPN продуктами версии 4.1

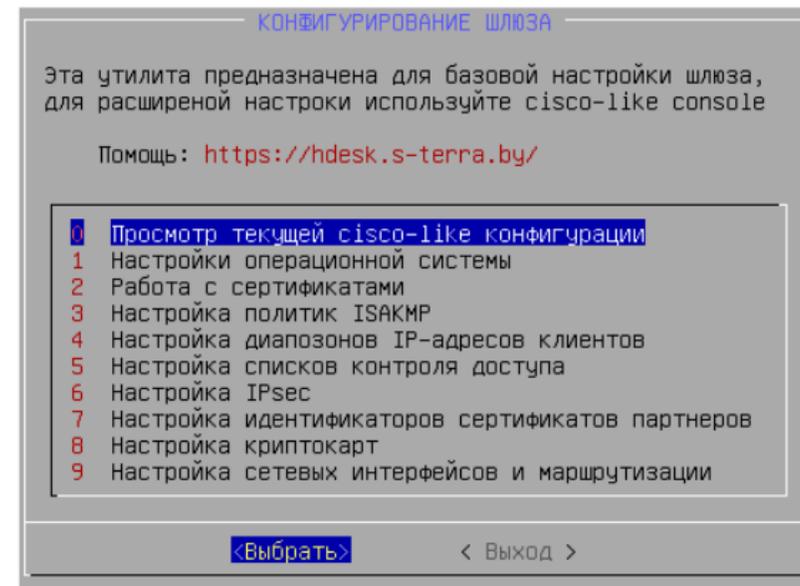




Программный продукт «**Конфигуратор Bel VPN**» представляет собой псевдографический интерфейс взаимодействия пользователя с ПАК (ПК) «Шлюз безопасности Bel VPN Gate 4.5» (далее – шлюз). Предназначен для проведения первоначальной настройки шлюза, а также для внесения изменений в настройки впоследствии

- предоставляется **бесплатно**
- легкая установка на комплексы программный и программно-аппаратный «Шлюз безопасности Bel VPN Gate 4.5»
- быстрая и удобная настройка СКЗИ
- прозрачность используемого кода (написан на bash-скрипте)
- возможность использования через SSH, COM-порт, посредством локального подключения

QR-CODE – *узнать подробности:*





Обновление ОС Debian GNU/Linux 9 для ПАК (ПК) «Шлюз безопасности Bel VPN Gate 4.5»

Обновление пакетов ОС Debian GNU/Linux 9, которая входит в состав поставки СКЗИ для закрытия уязвимостей, устранения проблем с совместимостью, оптимизации работы и ее производительности

- обновления предоставляются **бесплатно**
- формирование файла-архива для загрузки на СКЗИ Off-line
- распространение и обновление через репозиторий ООО «С-Терра Бел» on-line
- возможность настройки автоматического обновления
- все пакеты обновления проходят тщательное тестирование перед передачей их пользователям

QR-CODE – репозиторий для обновления:



Репозиторий для обновления ПАК(ПК) «Шлюз безопасности Bel VPN Gate 4.5»

Возможны следующие варианты обновления:

Вариант 1 - шлюз безопасности имеет доступ к сети Интернет

- добавьте ключ репозитория С-Терра Бел в список доверенных ключей:
`gpg --no-check-certificate -o - 'https://updates.s-terra.by/s-terra.gpg' | apt-key add -`
[Скопировать](#)
- установите репозиторий С-Терра как единственный источник обновлений:
`echo 'deb http://updates.s-terra.by/stretch /' > /etc/apt/sources.list`
[Скопировать](#)
- обновите список пакетов доступных в репозитории:
`apt update`
[Скопировать](#)
- запустите обновление пакетов:
`apt upgrade -y`
[Скопировать](#)

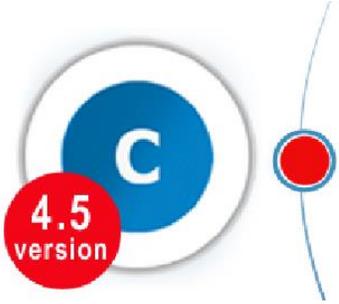
Вариант 2 - шлюз безопасности не имеет доступа к сети Интернет

- скачать архив с пакетами обновления и загрузить его на шлюз:
[Скачать](#)
- распакуйте архив:
`tar xf Update-*.tar.gz`
[Скопировать](#)
- запустите обновление пакетов:
`./update.sh`
[Скопировать](#)

ПП Клиент безопасности Bel VPN Client-M 4.5

под ОС Android

Сертификат
от 07.07.2020



Программный продукт «Клиент безопасности мобильный **Bel VPN Client-M 4.5**» предназначен для защиты доступа удаленного пользователя к ведомственной сети, защищаемой шлюзом безопасности

- новый пользовательский интерфейс
- анимация процессов подключения и работы
- поддержка новых версий Android
- возможность использования нескольких тем (для экономии заряда аккумулятора)
- дополнительная сигнализация о процессах работы СКЗИ
- упрощенная настройка устройства
- обновление сертификатов через Email, Viber, Skype и т.д.
- контроль срока действия сертификатов
- биометрическая аутентификация
- совместимость с Bel VPN продуктами версии 4.1

QR-CODE на презентацию продукта





ПАУ «Клиент ДСП 4.5» предназначается для защиты удаленного доступа в ИС классов 3-дсп, 4-дсп (приказ ОАЦ № 66 от 20.02.2020г.):

- класс 3-дсп – информационные системы, в которых обрабатывается служебная информация ограниченного распространения и которые подключены к открытым каналам передачи данных
- класс 4-дсп – информационные системы, в которых обрабатывается служебная информация ограниченного распространения и которые не имеют подключений к открытым каналам передачи данных

Возможно также использование ПАУ «Клиент ДСП 4.5» в защищенных ИС иных классов:

- требующих повышенный уровень безопасности, в частности, в платежных терминалах, банкоматах, инфокиосках и других
- использующих на рабочих местах любые нестандартные операционные системы (**Linux, MacOS, Astra Linux и другие**)



USB-C Power In /Slave



Dual Gbps Ethernet Ports

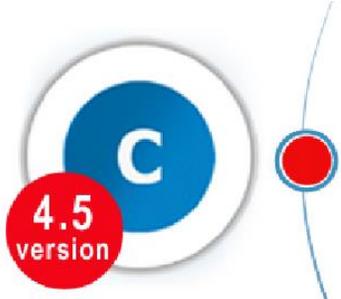


1GB DDR4 RAM

В ПАУ «Клиент ДСП 4.5» используется аппаратная платформа со следующими параметрами :

- размеры: 62 x 60 x 27.5 (мм)
- вес: 115 г
- USB питание DC 5V/2A (возможно от сети)
- ОЗУ 1 Гб DDR4
- 3 x (2 x 10/100/1000 Ethernet + 1 x USB Ethernet)





ПП «Клиент безопасности **Bel VPN Client 4.5**» под ОС Windows и Linux

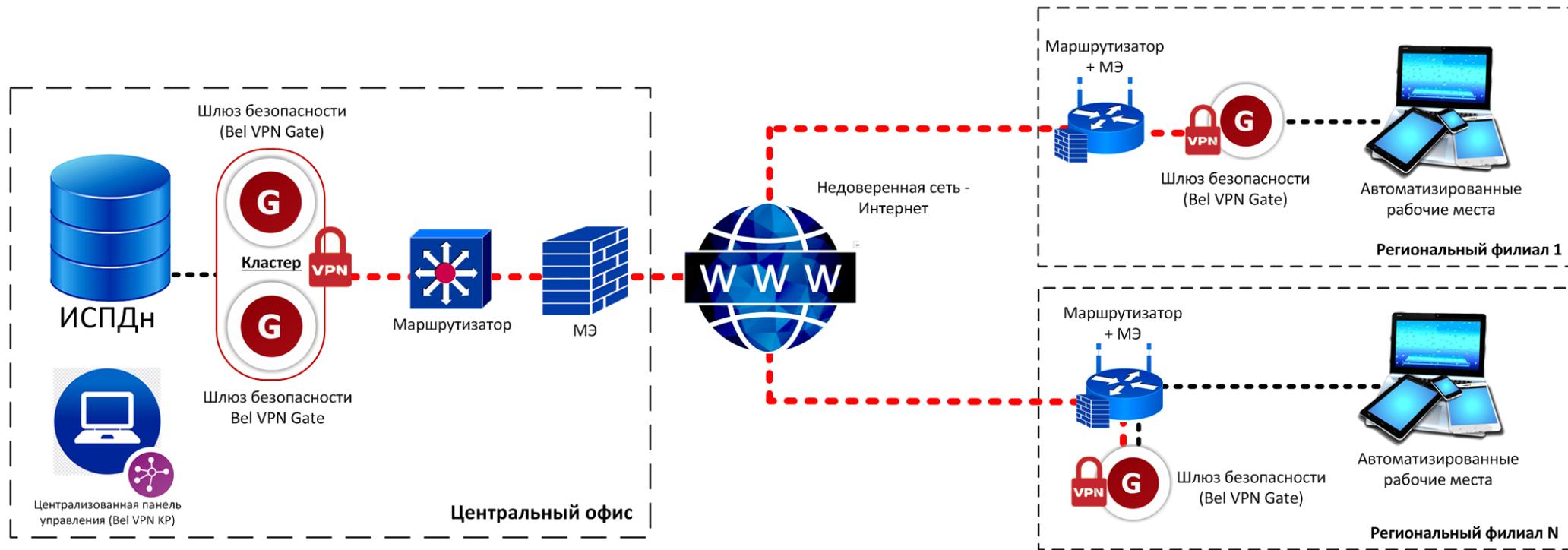


Программный продукт «Клиент безопасности **Bel VPN Client 4.5**» предназначен для защиты доступа удаленного пользователя к ведомственной сети, защищаемой шлюзом безопасности

- варианты установки Bel VPN Client 4.5 :
 - на ОС Windows (совместимость со всеми версиями)
 - на ОС семейства Linux
- поддержка консольного режима и режима GUI
- новый пользовательский (GUI) интерфейс
- проработанный механизм аутентификации
- упрощенная настройка клиента безопасности
- совместимость с Bel VPN продуктами версии 4.1



Решение для территориально распределенной защищенной ИС

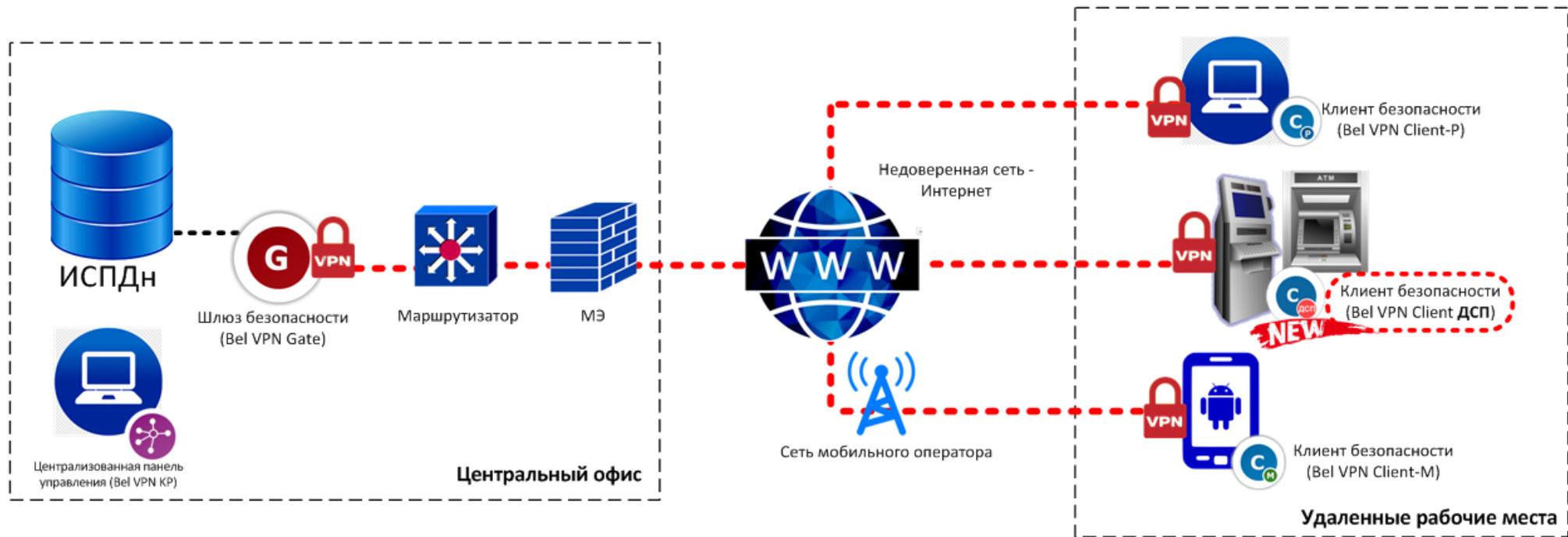


Пример 1. Территориально распределённая защищенная ИС с ПДн

Задача: организация состоит из центрального офиса, где находится БД, и филиалов. Связь осуществляется через недоверенную сеть - Интернет

Решение: в центральном офисе два производительных шлюза объединены в отказоустойчивый VRRP кластер. Используется система централизованного управления. Менее производительные шлюзы – в филиалах

Решение для удаленного доступа к ресурсам защищенной ИС №1

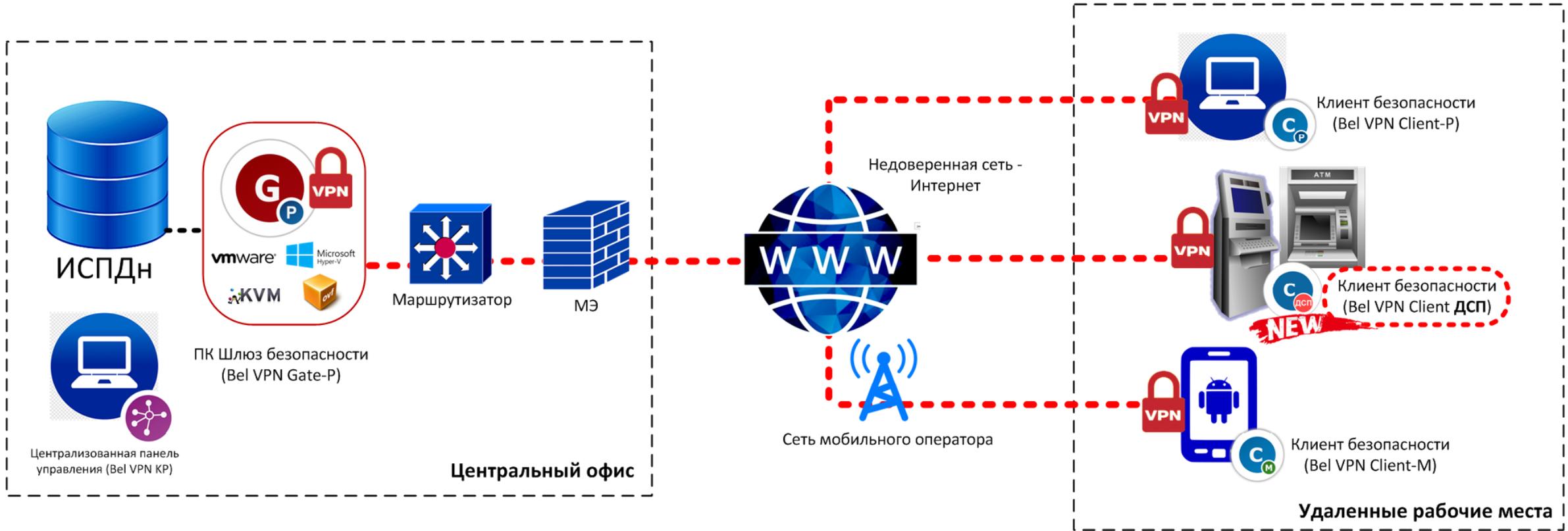


Пример 2. Удаленный доступ к ресурсам защищенной ИС с ПДн

Задача: в центральном офисе развернута БД, к которой необходим доступ сотрудникам, работающим удаленно. Сотрудники используют PC и ноутбуки с Windows, планшеты и смартфоны с Android, рабочие станции с MacOS, Linux.

Решение: в центральном офисе используется один шлюз. Для удобства также используется система ЦУ. На PC, ноутбуках, смартфонах используются: Клиент-P (Windows), Клиент-M (Android), Клиент-ДСП (MacOS, Linux)

Решение для удаленного доступа к ресурсам защищенной ИС №2



Пример 3. Удаленный доступ к ресурсам защищенной ИС с ПДн (виртуальное исполнение)

Техническая поддержка

□ Стандартная:

- дистанционно – телефон/e-mail/портал технической поддержки;
- обработка запросов по схеме 9/5 (с 9 до 18 в рабочие дни).

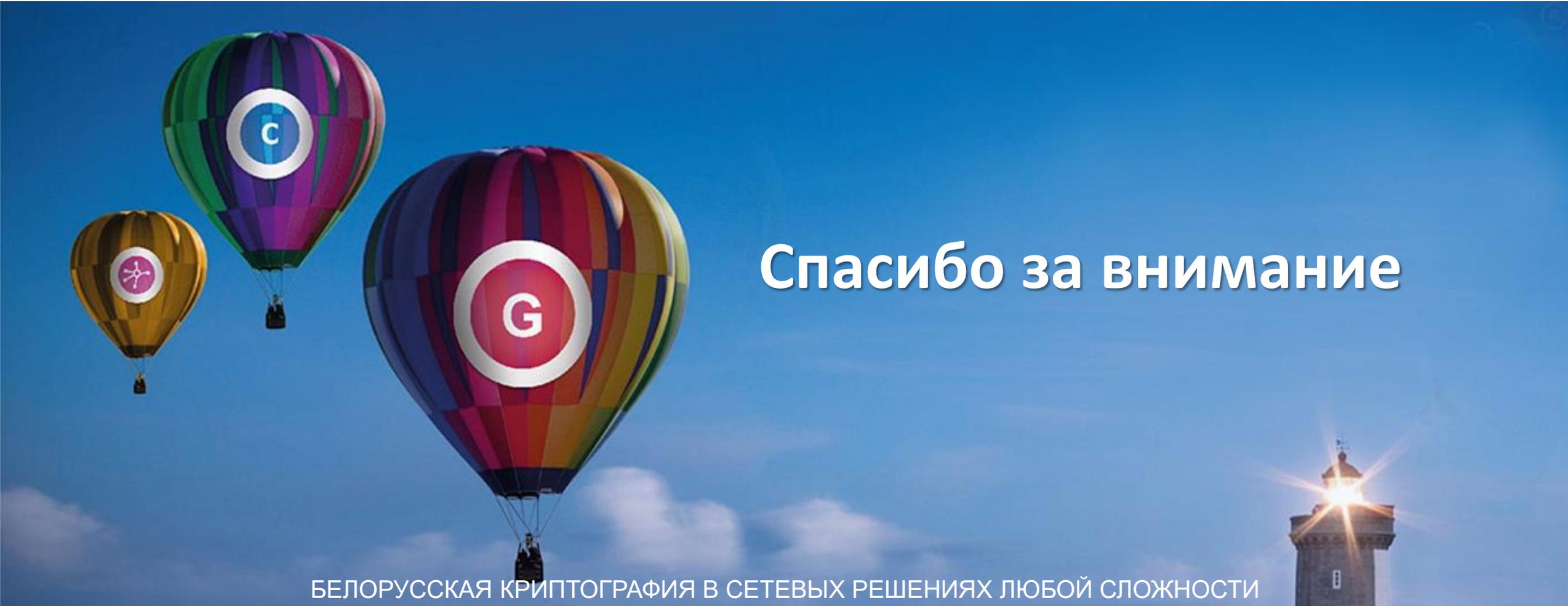
Время реакции:

- ✓ на запросы с уровнем важности «критичный» и «высокий» - **2 часа**;
- ✓ на запросы с уровнем важности «средний» - **1 день**;
- ✓ на запросы с уровнем важности «низкий» - **1 день**.

- бесплатно первый год;
- предоставление подменного оборудования на время диагностики и ремонта;
- бесплатное предоставление обновлений на ПО (в рамках одной версии);
- скидка на модернизацию СКЗИ при выпуске сертифицированных новых версии Bel VPN продуктов.

□ Расширенная:

- выезд инженера на площадку Заказчика;
- время на реакцию и устранение неисправностей - по согласованию с Заказчиком;
- совместное оказание ТП с партнерами, оказывающими Заказчику услуги по обслуживанию сетевого оборудования (первая линия).



Спасибо за внимание

БЕЛОРУССКАЯ КРИПТОГРАФИЯ В СЕТЕВЫХ РЕШЕНИЯХ ЛЮБОЙ СЛОЖНОСТИ

220012, г.Минск, ул. Чернышевского, д. 10А

+375 (17) 280 60 00

info@s-terra.by, www.s-terra.by

s•terra