Приложение №1 к извещению

Техническое задание

№ п/п	Наименование	Характеристика	Описание
1	Передача права на использование ПО ViPNet Prime (Update Administrator)	Вид лицензии	Простая (неисключительная)
		Способ предоставления	Экземпляр на материальном носителе
		Срок действия лицензии	Бессрочно
		Количество	1 шт.
		Функциональные требования	Требования к управлению VPN-сетью ПК управления VPN-сетью должен обеспечивать: управление структурой защищенной виртуальной сети (VPN); регистрацию сетевых узлов (далее – СУ) и пользователей VPN-сети; задание связей между объектами (СУ, пользователи, группы пользователей) VPN-сети; контроль перечня лицензий на ПК и ПАК защищенной виртуальной сети (VPN); возможность интеграции с Active Directory; настройки доменной аутентификации с помощью служб федераций AD FS; ведение журнала событий; многопользовательский доступ администраторов с ролевой моделью доступа; аутентификацию администраторов по паролю или сертификатам и аудит их действий; разграничение полномочий администраторов; централизованное управление настройками СУ VPN-сети и политиками доступа пользователей к функциям узлов VPN-сети; управление конфигурациями и справочниками узлов и пользователей VPN-сети; рассылку узлам и пользователям VPN-сети обновлений справочников, ключевой информации и программного обеспечения; аудит обновления справочно-ключевой информации на узлах VPN-сети; разделение VPN-сети на изолированные части – организации, к которым может быть предоставлен отдельный доступ; формирование наборов справочно-ключевой информации для первичной инициализации СУ VPN-сети, а также управление обновлением ключевой информации для узлов и пользователей VPN-сети; настройка сложности паролей пользователей и администраторов сетевых узлов; создание профилей DNS для сетевых узлов.
		Требования к поддерживаемым	ПК управления VPN-сетью должен функционировать под управлением операционных

		операционным системам	систем: Astra Linux Special Edition «Смоленск» 1.7.5; Astra Linux Special Edition «Воронеж» 1.7.5; Ubuntu 22.04 LTS; Ubuntu 20.04 LTS. ПК управления VPN-сетью должен поддерживать работу в следующих виртуальных средах: VMware vSphere 6.7; VMware Workstation Pro 15.x, 16.x; Proxmox 7.4, 8.2; ПК СВ «Брест» 3.2; zVirt 4.1.
		Требования к сертификации	ПК управления VPN-сетью должен соответствовать Требованиям ФСБ России к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1, КС2, КС3, требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27.12.2011 №796, установленным для классов КС1, КС2, КС3.
		Требования к поставке	Лицензия на бумажном носителе – 1 шт.
2	Сертифицированный дистрибутив программного обеспечения ПО ViPNet Prime	Способ предоставления	Экземпляр на материальном носителе
		Совместимость	Полная совместимость с ПО ViPNet Prime
		Количество	1 шт.
		Состав поставки	CD-диск с дистрибутивом программного обеспечения. Техническая и эксплуатационная документация в электронном виде. Формуляр с серийным номером. Электронную копию сертификата соответствия ФСБ.
3	Передача права на использование ПО ViPNet PKI Client 2.x Базовая лицензия	Вид лицензии	Простая (неисключительная)
		Способ предоставления	Экземпляр на материальном носителе
		Срок действия лицензии	Бессрочно
		Количество	2 шт.
		Функциональные требования	PKI-клиент должен обеспечивать: - создание ключа ЭП и ключа проверки ЭП, создание ЭП и проверку ЭП в соответствии с ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018) «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»; - хэширование данных в соответствии с ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.11-2012

			«Информационная технология. Криптографическая защита информации. Функция хэширования»; - шифрование (зашифрование и расшифрование) данных в соответствии с алгоритмами ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Информационная технология. Криптографическая защита информации. Блочные шифры» («Магма», «Кузнечик»), и ГОСТ Р 34.13-2015 (ГОСТ 34.12-2018) «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»; - организацию защищенного TLS-соединения в соответствии с алгоритмами ГОСТ Р 34.10-2012, ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик» и ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018); - поддержку следующих форматов ЭП: • PKCS #7 (CMS) в соответствии с RFC 5652, RFC 4490; • XMLDSig; • усовершенствованная подпись CAdES в соответствии с «CMS Advanced Electronic Signatures», ETSI TS 101 733 V1.8.3; • XAdES в соответствии с «XML Advanced Electronic Signatures», ETSI TS 101 903 V1.3.2; • WS-Security; - поддержку работы с облачными сервисами ЭП; - поддержку внешних устройств для подключения к туннелируемым ресурсам; - добавление меток времени при формировании ЭП в соответствии с RFC 3161; - обращение к сервису проверки статуса сертификата (OCSP-серверу) и проверки статуса сертификата в соответствии с RFC 6960.
		Требования к сертификации	PKI-клиент должен соответствовать: - требованиям ФСБ России к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1, КС2, КС3, требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для классов КС1, КС2, КС3.
4	Установочный комплект ПО ViPNet PKI Client 2.x (Исполнения:1-6) сертификационными документами	Способ предоставления	Экземпляр на материальном носителе
		Количество	1 шт.
		Состав поставки	CD-диск с дистрибутивом программного обеспечения. Техническая и эксплуатационная документация в электронном виде. Формуляр с серийным номером. Электронная копия сертификата соответствия ФСБ.

5	Лицензия на операционную систему специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64, уровень защищенности «Максимальный» («Смоленск»), РУСБ.10015-01 (ФСТЭК), способ передачи диск, для рабочей станции, на срок действия исключительного права, с включенными обновлениями Тип 1 на 12 мес.	Способ предоставления	Экземпляр на материальном носителе, Лицензия в электронном виде в личном кабинета Заказчика
		Количество АРМ на которых можно установить ПО	1 шт.
		Срок действия лицензии	Бессрочно
		Требования к встроенному комплексу средств защиты информации операционной системы	Операционная система должна обеспечивать встроенными сертифицированными средствами: идентификацию и аутентификацию пользователей; управление средствами аутентификации; управление учетными записями пользователей, разграничение полномочий и назначение прав пользователям; реализацию дискреционного и мандатного разграничения доступа; возможность указания параметров настройки комплекса средств защиты во время создания пользователя; возможность создания среды выполнения контейнеров, обеспечения работы с ними и поддержкой изоляции процессов, выполняемых в контейнерах; возможность маркировки документов при выводе на печать; управление доступом к защищаемым ресурсам БД на основе иерархических и не иерархических меток доступа; реализацию мандатного управления доступом к почтовым сообщениям, а также автоматическую маркировку создаваемых пользователем почтовых сообщений. В составе операционной системы должна быть реализована возможность защиты аутентификационной информации с использованием функции хэширования. В составе операционной системы должно быть ядро, поддерживаемое Центром исследования безопасности системного программного обеспечения ИСП РАН. В составе операционной системы должна быть реализована возможность внедрения в сетевые пакеты протоколов IPv4 и IPv6 классификационных меток в соответствии с ГОСТ Р 58256-2018 для обеспечения: организации сетевого взаимодействия прикладных процессов на основе их классификационных меток; фильтрации сетевого трафика на основе классификационных меток. Операционная система должна иметь графическое средство настройки ограничений пользователя по запуску программ в изолированном окружении с использованием механизма пространств имён и фильтрации системных вызовов,

			обеспечивающих: ограничение прав пользователя на запуск приложений ядром системы; ограничение прав пользователя средствами графического интерфейса; разрешение запуска только тех программных компонентов, которые явно разрешены администратором безопасности. Обеспечение запрета запуска (исполнения) пользователем созданных самостоятельно (с использованием текстовых редакторов или непосредственно в командной строке) программ с использованием интерпретируемых языков программирования. В составе операционной системы должны быть графические средства настройки защиты машинных носителей, обеспечивающие: идентификацию устройств и сопоставление пользователя с устройством; управление доступом субъектов доступа к устройствам методами мандатного и дискреционного управления доступом; задание правил управления доступом, разрешающих или запрещающих доступ субъектов доступа к устройствам, а также определяющих разрешенные типы доступа, в том числе с использованием атрибутов безопасности; учет носителей информации и контроль использования интерфейсов ввода и вывода. Операционная система должна включать в свой состав программное обеспечение, реализующее задачи аудита и журналирования (регистрации) событий безопасности. Регистрация событий безопасности должна выполняться с учётом требований ГОСТ Р 59548-2022. Операционная система должна включать в состав графические средства настройки контроля целостности: контроль целостности дистрибутива; контроль объектов файловой системы; контроль целостности исполняемых файлов. Операционная система должна обеспечивать возможность блокировки: запуска исполняемых файлов, включая EXE и загрузки библиотек, в том числе DLL, .NET 7/8, целостность которых нарушена; открытия файлов, в том числе пустых, и самораспаковывающихся 7Z архивов, установленных на контроль, при нарушении их целостности. В составе операционной системы должна быть реализована возможность ограничения полномочий пользователей по использованию консолей. В операционной системе должна быть реализована возможность очистки и ограничения работы с

			оперативной памятью. Должны быть обеспечены работы по устранению уязвимостей и включению информации об уязвимостях программного обеспечения операционной системы в банк данных угроз безопасности информации ФСТЭК России (https://bdu.fstec.ru/vul). Механизмами безопасности операционной системы должна быть обеспечена защита системных и привилегированных процессов от несанкционированного доступа и управления (исключение возможности повышения привилегий пользователей и управления привилегированными процессами в случае использования дефектов, уязвимостей в программном обеспечении информационной системы). Операционная система должна обеспечивать запрет операций записи в системные каталоги и файлы (программы, файлы конфигурации), а также установки программного обеспечения, запуска и остановки системных процессов операционной системы, вне зависимости от изменения пользователем своих привилегий в текущем сеансе работы. Операционная система должна предоставлять средство настройки профиля системы со следующими возможностями: настройка комплекса средств защиты в соответствии с требованиями о защите информации, предъявляемыми к определенному классу защищенности информационных систем, при помощи графического интерфейса; импорт и экспорт настроек комплекса средств защиты системы. Операционная система должна иметь графические средства для работы со сторонними устройствами аутентификации - токенами, обеспечивающие следующие возможности: двухфакторная авторизация; вход и разблокировка сессии по токену; блокировка сессии при извлечении токена.
		Требования к функциональным возможностям операционной системы	Операционная система должна быть предназначена для функционирования на средствах вычислительной техники с аппаратной платформой x86-64, включая процессоры Intel не ниже 10-го поколения. Операционная система должна поддерживать работу на ядре Linux версии не ниже 6.1 с возможностью обновления до новых версий ядра (в соответствии с документацией на продукт). Операционная система должна обеспечивать функционал в графическом исполнении: наличие графических средств создания, настройки и управления несколькими репозиториями используемого программного обеспечения со следующим функционалом:

			проверка зависимостей пакетной базы; автоматическая публикация в сети по протоколам http и ftp; выбор конкретных репозиториев, из которых будет произведено обновление пакетов; наличие средств подключения к операционной системе по протоколу RDP, со следующими возможностями по умолчанию: вход в сессию локально, а затем подключение к этой сессии удаленно с автоматической блокировкой доступа к сессии локально и возможностью одновременной работы локально в графической сессии из-под другого пользователя; вход в сессию удаленно, а затем подключение к этой сессии локально при входе в систему с автоматическим отключением удаленного клиента; проброс нескольких смарт-карт или токенов (eToken, Рутокен, JaCarta) с возможностью их одновременного использования на сервере и клиенте. наличие графической утилиты управления драйверами nvidia, intel, amd с возможностью выбора драйверов и возможностью восстановления драйверов при неудачной загрузке операционной системы; наличие графических средств настройки выделяемых ресурсов памяти пользователям (квоты); наличие графического инструмента для просмотра и редактирования значения переменных окружения (просматривать текущие переменные, изменять значение и описание переменных, удалять и объявлять переменные); наличие графических средств настройки и изменения ориентации экрана в ручном или автоматическом режиме, с возможностью калибровки поворота, а также задания ориентации по умолчанию; наличие графического инструмента управления регистрацией событий, включающего в себя управление сервисом системных событий, настройку ротации событий и настройку параметров сбора системных событий, наличие графического средства просмотра системных событий; наличие графических средств настройки сохранения и восстановления сессии пользователя (восстановление при старте запущенных программ и их расположения после полного отключения электропитания автоматизированного рабочего места); наличие графических средств настройки потребления электроэнергии (яркость экрана, потухание, выключение монитора, переход в ждущий режим, сон и гибернацию) в случае изменения настроек электропитания (питание от

			сети, питание от батареи, низкий заряд батареи); наличие графических средств монтирования usb устройств по сети (usbip или аналог) для подключения к нескольким персональным компьютерам; наличие графических средств настройки одновременной работы нескольких сотрудников на одном персональном компьютере с разделяемыми профилями; наличие графических средств создания системных отчётов, предназначенных для сбора, сжатия, сохранения и для отправки в службу сопровождения диагностических данных о работе системы; наличие графических средств запуска работы с удалёнными, отдельными и вложенными графическими сессиями; наличие графических средств настройки планирования времени завершения работы без участия пользователя (завершение сессии, выключение автоматизированного рабочего места, перехода в энергосберегающие режимы) с настройкой уведомления о событии; наличие графических средств запуска приложений с изменением приоритета выполнения с возможностью запуска от имени другого пользователя; наличие графических средств настройки параметров загрузчика операционной системы (загружаемая операционная система по умолчанию, передаваемые параметры ядра, таймаут для ожидания действий пользователя, выбора источника ввода данных при загрузке, выбор терминала для вывода информации); наличие графических средств расчёта контрольных сумм файлов и их сравнения; наличие графических средств работы с архивами (zip, rar, 7zip, tar, tgz, tar.gz, tar.bz, tar.xz, iso); наличие графических средств для оповещения пользователя о конфликте IP-адресов при подключении к сети; наличие графических средств настройки системы, в том числе: установки и синхронизация времени; управления пользователями; просмотра системных журналов; настройки и обслуживания принтеров; наличие графических средств настройки цветового баланса для каждого монитора по отдельности; наличие возможности присвоить пользовательские наименования звуковым устройствам при помощи графического интерфейса; наличие графических средств ввода в домен, в том числе с возможностью добавить компьютер в нужное подразделение (OU, Organizational Unit) для клиента Active Directory;

			наличие графического центра уведомлений на рабочем столе с следующими возможностями: настройка расположения уведомлений; возможность индивидуальных настроек для конкретных приложений; настройка отображения уведомлений на экране блокировке и при разблокировки; наличие графических инструментов глобального поиска по расположению, содержимому, времени создания или изменения, размеру файла, с отображением результатов поискового запроса в интерактивном окне со следующими возможностями: группировки и фильтрации результатов по найденным категориям (файлы, приложения, папки, архивы); отображения свойств найденных файлов (имя, тип, путь, размер); наличие графического инструмента для настройки частот процессора. Операционная система должна поддерживать следующий функционал: графический интерфейс, адаптированный под использование на портативных устройствах с поддержкой управления настройками системы, приложениями и сервисами (включая контекстные меню) с помощью touchscreen (сенсорный экран) с возможностью автоматического отключения при подключении мышки; возможность подключения к сети wi-fi до входа в систему, а также аутентификация в сети wi-fi с использованием смарт-карты; наличие в репозитории операционной системы браузера из единого реестра российских программ для электронных вычислительных машин и баз данных; возможность ввода аутентификационных данных пользователя при входе в систему и при разблокировке экрана с использованием виртуальной клавиатуры без необходимости дополнительных настроек. Операционная система должна обеспечивать поддержку файловых систем и сетевых протоколов: ext2/3/4, fat, ntfs, iso9660, XFS, ZFS, BTRFS; TCP/IP, DHCP, DNS, FTP, TFTP, SMTP, IMAP, HTTP(S), NTP, SSH, NFS, SMB; поддержка стандарта ISO9660; наличие средств подключения ресурсов WebDAV в качестве локальной файловой системы для возможности использования их стандартными приложениями операционной системы. Операционная система должна обеспечивать возможность создания точек восстановления (снапшотов) для последующего возвращения системы к исходному состоянию в случае сбоя, а

			также иметь возможность возврата к состоянию до начала установки обновлений. Операционная система должна обеспечивать среду функционирования для сертифицированных средств криптографической защиты информации, предназначенных для создания и проверки электронной подписи. Установщик операционной системы должен иметь следующий функционал: обеспечивать возможность запуска VNC сервера для удаленного подключения к клиентским машинам и управления ими как на этапе загрузки с установочного диска в главном меню программы установки, так и непосредственно в LiveCD; возможность автоматической установки при помощи файла конфигурации формата .yaml; возможность задания параметров для администратора и нескольких локальных пользователей; предоставлять возможность установки любых пакетов из репозитория операционной системы во время установки. Операционная система должна предоставлять инструмент для обновления между мажорными версиями с сохранением настроек операционной системы и ПО. Операционная система должна предоставлять средства для локальной виртуализации (виртуальные машины, созданные на рабочей станции или удаленном сервере и используемые в однопользовательском режиме) с графическим интерфейсом управления и возможностью группировать отображаемые виртуальные машины. Операционная система должна предоставлять специальные возможности: экранный диктор и синтезатор речи для русского языка; голосовой ввод; настройка визуальных и звуковых уведомлений на события, связанные со специальными возможностям; настройка залипающих, замедленных и прыгающих клавиши; настройка управления курсором мыши с помощью цифровой клавиатуры. Дополнительные функциональные компоненты: клиентское ПО, для осуществления подключения по протоколу RDP; агенты служб централизованного управления системой; приложение для сканирования документов с возможностью пропуска пустых страниц и с сохранением размера области сканирования; средство просмотра и редактирования файлов.pdf; средство для эмуляции запуска исполняемых

			файлов.exe; средства просмотра и редактирования графики и изображений; средство оптического распознавания символов.

Поставщик должен соответствовать требованиям, устанавливаемым в соответствии с законодательством Российской Федерации к лицам, осуществляющим техническую поддержку средств криптографической защиты информации, в том числе иметь действующие лицензии ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств на следующие виды работ.

Сроки поставки Лицензии и ПО:
Сроки передачи - в течение 10 (десяти) рабочих дней с даты получения Исполнителем заявки от Заказчика, направленной посредством цифровой платформы закупок «РЖД-Медицина».

Ведущий инженер по защите информации Богданас Н.А.