ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на поставку программного обеспечения

2019 г.

1. Предмет закупки: поставка программного обеспечения.

2. Место, условия и сроки предоставление права на использование программного обеспечения, выполнения работ, оказание услуг:

2.1. Место поставки: на электронный почтовый ящик v.subbotin@ano-rsi.ru. Сроки предоставления права на использование программного обеспечения: в течение 7 (семи) рабочих дней с даты оплаты авансового платежа, за исключением программного обеспечения компании Microsoft. По регламенту компании Microsoft предоставление права использования программ для ЭВМ производится в течении от 3 до 45 рабочих дней, с даты оплаты авансового платежа, в связи с проверкой компании Заказчика по санкционным спискам.

2.2. Поставка, отгрузка должны производится силами и за счет Поставщика.

3. Порядок формирования цены закупки: Цена Договора включает в себя: все расходы, связанные с вознаграждением за передачу прав на использование программного обеспечения, а также расходы на страхование, уплату таможенных пошлин, налогов, сборов, финансовых рисков, инфляционных ожиданий и других расходов, связанных с исполнением Договора.

4. Форма, сроки и порядок оплаты: Оплата производится в следующем порядке: авансовый платеж в размере 20% (двадцать процентов) от общей цены договора подлежит перечислению в течение 10 (десяти) рабочих дней с даты подписания договора на основании счета Поставщика; окончательный расчет осуществляется в течение 10 (десяти) календарных дней после подписания Заказчика Акта предоставления прав в отношении всех программ для ЭВМ, согласованных в Спецификации

Характеристики предоставляемого программного обеспечения (лицензий):

№ п.п	Наименование	Технические характеристики	Ед. изм.	Кол-во
1.	Microsoft Office Home and Business 2019 All Lng PKL Onln CEE Only DwnLd C2R NR*	Комплект офисных программ, состоящий из: 1. Текстового редактора (Word); (Текстовый процессор с расширенными возможностями для создания и форматирования документов с поддержкой форматов: *.docx; *.docm; *.xml; *.dotx; *.dotm; *.doc; *.dot; *.dotx; *.htm; *.html; *.rtf; *.txt; *.odt и возможностью сохранять документы в формате *.pdf.). 2. Программы для работы с электронными таблицами (Excel); (Табличный процессор для работы с электронными таблицами и анализом данных с количеством строк в электронной таблице не менее одного миллиона и количеством столбцов не менее шестнадцати тысяч, создания отчетов, анализа информации, вариантов развития и тенденций, поддерживающий богатый инструментарий для визуализации данных с поддержкой форматов: *.xl; *.xlsx; *.xml; *.xlsm; *.xlsb; *.xlam; *.xltx; *.xitm; *.xls; *.xlt; *.htm; *.html; *.mht; *.mhtml; *.xla; *.xlm; *.xlw; *.odc; *.uxdc; *.ods и возможностью сохранять документы в формате *.pdf.) 3. Редактора презентаций (PowerPoint); (Генератор развернутых презентаций с высоким разрешением, поддержкой переходов, анимации, интеграцией аудио и видео материалов с поддержкой форматов: *.pptx; *.ppt; *.pptm; *.ppsx; *.pps; *.ppsm; *.xml; *.potx; *.pot; *.potm; *.htm; *.html; *.mht;	шт.	200

		*.mhtml; *.thmx; *.ppam; *.ppa; *.odp; и возможностью сохранять документы в форматах *.jpg; *.wmv; *.pdf.). 4. Программы для создания быстрых заметок (OneNote) (Приложение для хранения заметок с возможностями навигации и организации данных, позволяющее организовать удаленный доступ к записным книжкам и обмениваться сведениями через веб-браузер.). 5. Почтового клиента (Outlook); (Почтовый клиент для удобного управления сообщениями электронной почты с набором инструментов, встроенной системой поиска и поддержкой веб-сервисов.). Ключ активации Поддержка версий Windows 7, Windows 8, Windows 8.1, Windows 10 Поддержка открытых форматов OpenOffice XML9 (без промежуточной конвертации) и OpenDocument (непосредственно или с помощью дополнительных программных модулей). Должно обеспечивать гарантированную совместимость и интеграцию работы с ней программного обеспечения криптографической защиты информации КриптоПро CSP, в целях формирования и проверки электронных подписей на основе алгоритмов ГОСТ. Должно обеспечивать гарантированную поддержку макросов. Срок действия лицензии: бессрочная. Права пользования лицензией должны включать возможность продолжения пользования лицензией после модернизации компьютера/сервера, возможность переноса лицензии с одного компьютера на другой, возможность использовать предыдущие версии продукта. язык интерфейса – русский		
2.	WinSvrSTDCore 2019 Single OLV 16License NL Each Additional Product CoreLic *	Серверная операционная система Права использования программного обеспечения на условиях простой (неисключительной) лицензии с передачей их в бессрочное пользование. Предоставляемые неисключительные права (лицензия) включают в себя право на воспроизведение, ограниченное правом инсталляции, копирования и запуска программного обеспечения, предоставляемое с единственной целью передачи этого права конечным пользователям. При передаче Исполнитель предоставляет ссылки на сайт компании производителя программного обеспечения (далее – ПО) для получения информации об имеющихся экземплярах ПО, управления существующими лицензиями ПО и предоставлять возможность скачивания старых (downgrade) версий ПО в рамках приобретенной лицензии ПО. Языковая версия – русская. Функциональные, технические и (или) эксплуатационные характеристики: - Наличие маханизмов авторизации и аутентификации в Active Directory по протоколам Kerberos, NTLM. - Управление настройками систем и программным обеспечением с помощью групповых политик Active Directory - Обеспечение отказоустойчивости с помощью встроенной системы репликации	шт.	6

		- Наличие динамического переключения протоколов маршрутизации VPN подключений без разрыва соединений - Автоматическая настройка и прозрачное (незаметное для пользователя) подключение VPN с возможностью двустороннего управления программным обеспечением и конфигурациями систем - Наличие системы проверки соответствия политикам безопасности и установленным политиками ИТ конфигурациям при подлкючении пользователя к сети - Наличие встроенной системы виртуализации, с механизмами отказоустойчивой кластеризации, обеспечивающей высокую доступность с автоматической репликацией виртальных машин без прерывания сервиса - Наличие технологии «peer to peer», позволяющей снизить нагрузки на интернет-канал за счет локального кэширования данных на всех машинах локальной сети и распространения файлов по локальной сети параллельно из множества источников без выделенного кэш-сервера - Наличие встроенных средств контроля целостности кода ОС и стороннего ПО в процессе загрузки ОС с помощью TPM и Unified Extensible Firmware Interface (UEFI) - Строгая аутенфикация с использованием аппаратных возможностей TPM (trusted platform module) - Контроль целостности ОС и приложений с помощью аппаратного модуля TPM (trusted platform module) - Наличие технологии устранения дублирования (дедупликации) на уровне блоков для файлов, включая файлы, находящиеся в эксклюзивном использовании - Наличие механизма, позволяющего всем узлам кластера одновременно использовать тома LUN (Logical Unit Number) с файловой системой NTFS		
3.	Windows Server CAL 2019 Single OLV NL Each Additional Product Device CAL *	Лицензия, которая предоставляет устройству (ПК, переносные компьютеры, домашние ПК, карманные ПК и мобильные телефоны) право удаленной работы пользователя на имеющимся у Заказчика сервере посредством терминального доступа.	шт.	200
4.	SQLSvrStd 2019 SNGL OLV NL Each AP *	Система управления реляционными базами данных (СУРБД). Включает в себя следующие инструменты: - система передачи данных в распределенных сетях. - поддержка типа XML. - поддержка колоночных индексов (Colomn store). - поддержка языков программирования СУБД: Transact SQL and .NET languages. - возможность секционирования БД: горизонтальное секционирование. - наличие временных таблиц. - поддержка active directory. - развитая система уведомлений. - возможности извлечения, преобразования и загрузки для хранилищ данных и интеграции данных в масштабе предприятия. - Аналитические службы – аналитическая обработка в реальном времени (технология OLAP) для быстрого, сложного анализа больших и смешанных наборов данных, использующая многомерное хранение. - Службы отчетов – решение для создания, управления и доставки как традиционных бумажных отчётов, так и интерактивных отчетов, основанных на технологии WorldWideWeb.	шт.	2

		- Инструменты управления – должны включать средства управления для настройки баз данных. Должна поддерживаться тесная интеграция с такими инструментами, как системы мониторинга производительности и доступности сервисов, системы управления и удаленной инсталляции приложений, порталы, системы управления проектами и коммуникационные системы. - Должна поддерживать возможность интеграции с СУРБД других производителей для изъятия данных, их обработки и анализа. Должна обеспечиваться возможность получения данных из электронных таблиц Excel. - Должна поддерживаться возможность интеграции с источниками геоинформационных данных и использование этих данных при анализе. - Должна поддерживаться возможность обработки событий в реальном времени с помощью запросов с отправкой заданных результатов в сторонние системы. - Должен поддерживаться регулятор ресурсов, позволяющий устанавливать ограничение на использование ЦП и оперативной памяти для конкурирующих рабочих нагрузок на экземпляре СУРБД. - Отказоустойчивые кластеры (более 2-х узлов), катастрофоустойчивость за счет поддержки в удаленном ЦОДе (группы доступности) - Поддержка гибридных сценариев работы СУБД при использовании частного облака - Наличие интеграции с Microsoft Visual Studio. - Инструменты разработки – должны включаться интегрированные инструменты разработки для ядра базы данных, извлечения, трансформации и загрузки данных, извлечения информации, OLAP и отчётности, которые тесно должна быть обеспечена совместимость с технологией dotNET для предоставления сквозных возможностей разработки приложений. Программная платформа должна обеспечивать полную совместимость со службой каталогов Active Directory. Должно быть обеспечено право использования СУРБД максимум на 24 (двадцати четырех) физических процессорных ядрах или 4 (четырех) физических процессорах на сервере (в зависимости от того, что меньше). Размер поддерживаемой базы данных должен быть не более 524 PB (пятьсот двадцать четыре петабайт). Должна поддерживаться платформа x64. Права использования должны включать возможность продолжения использования программного обеспечения после модернизации сервера, а также возможность переноса программного обеспечения с одного сервера на другой. Должна предоставляться возможность отдельного приобретения аналогичной позиции, включающей обновление версии продукта в течение 3 лет		
5.	SQLCAL 2019 SNGL OLV NL Each AP DvcCAL *	Права на использование лицензий клиентского доступа с соответствующего устройства системе управления реляционными базами данных, которая должна отвечать следующим требованиям: - система передачи данных в распределенных сетях. - развитая система уведомлений. - возможности извлечения, преобразования и загрузки для хранилищ данных и интеграции данных в масштабе предприятия. - Аналитические службы – аналитическая обработка в реальном времени (технология OLAP) для быстрого, сложного анализа больших и смешанных наборов данных, использующая многомерное хранение.	шт.	200

		- Службы отчетов – решение для создания, управления и доставки как традиционных бумажных отчётов, так и интерактивных отчетов, основанных на технологии WWW. - Инструменты управления – должны включать средства управления для настройки баз данных. Должна поддерживаться тесная интеграция с такими инструментами, как системы мониторинга производительности и доступности сервисов, системы управления и удаленной инсталляции приложений, порталы, системы управления проектами и коммуникационные системы. - Должна поддерживать возможность интеграции с СУРБД других производителей для изъятия данных, их обработки и анализа. Должна обеспечиваться возможность получения данных из электронных таблиц Excel. - Должна поддерживаться возможность интеграции с источниками геоинформационных данных и использование этих данных при анализе. - Должна поддерживаться возможность обработки событий в реальном времени с помощью запросов с отправкой заданных результатов в сторонние системы. - Должен поддерживаться регулятор ресурсов, позволяющий устанавливать ограничение на использование ЦП и оперативной памяти для конкурирующих рабочих нагрузок на экземпляре СУРБД. - Инструменты разработки – должны включаться интегрированные инструменты разработки для ядра базы данных, извлечения, трансформации и загрузки данных, извлечения информации, OLAP и отчётности, которые тесно должна быть обеспечена совместимость с технологией dotNET для предоставления сквозных возможностей разработки приложений. Программная платформа должна обеспечивать полную совместимость со службой каталогов Active Directory. Должна поддерживаться компрессия данных и резервных копий независимо от поддержки подобного функционала со стороны приложений. Должно поддерживаться секционирование таблиц и индекса. Право на использование лицензий клиентского доступа к СУРБД должно обеспечивать возможность использования как текущей, так и предыдущих версий СУРБД. Должно быть обеспечено право использования текущей версии СУРБД на не менее чем 20 (Двадцати) физических процессорных ядрах. Для предыдущих версий СУРБД не должно быть ограничений со стороны прав на использование и технических возможностей СУРБД на количество используемых системой процессоров и оперативной памяти. Должно поддерживаться горячее добавление оперативной памяти и процессоров. Размер поддерживаемой базы данных должен быть не более 524 PB (пятьсот двадцать четыре петабайт). Должна поддерживаться платформа x64. Права использования должны включать возможность продолжения использования программного обеспечения после модернизации компьютера, а также возможность переноса программного обеспечения с одного компьютера на другой.		

		Должна предоставляться возможность отдельного приобретения аналогичной позиции, включающей обновление версии продукта в течение 3 лет		
6.	Exchange Server Standard 2019 Single OLV NL Each Additional Product *	Программное обеспечение должно иметь следующие характеристики: - обеспечивать возможность применения всех групповых политик домена Active Directory. - иметь средства коллективной работы с электронной почтой, голосовой почтой, общими календарями, контактами и задачами, поддержка протоколов SMTP, POP3, IMAP, MAPI, возможность архивации с помощью встроенных средств, детализированного поиска в нескольких почтовых ящиках одновременно, применение политики сохранения на уровне элемента, сбор юридически значимой информации из почтовых сообщений, средства защиты информации и контроля ее распространения (в том числе перехват, модерирование, шифрование и блокирование электронных сообщений). - поддерживаться возможность доступа к почтовому ящику с любых мобильных устройств. - право на использование программного обеспечения должны позволять выполнять администрирование на основе ролей и делегировать отдельные административные задачи пользователям, предоставлять пользователям единую точку доступа к электронной и голосовой почте, позволять управлять ими из одной консоли, обеспечивать высокую готовность системы и ее аварийное восстановление стандартными и простыми методами. - должно быть обеспечено функционирование системы в 64-битной среде. Должна быть реализована возможность кластеризации серверов с числом активных узлов не менее двух. Количество баз данных почтовых ящиков – не менее десяти. - должна быть обеспечена возможность интеграции с Active Directory. программное обеспечение должно содержать встроенные средства антивирусной и антиспам-защиты. - программное обеспечение должно поддерживать разнесение различных функциональных ролей на разные физические или виртуальные сервера без потери функциональности. - программное обеспечение должно быть локализовано на русском языке. - право использования программного обеспечения должно включать возможность продолжения использования программного обеспечения после модернизации сервера, а также возможность переноса с одного сервера на другой. - право использования должны включать возможность использования языковых редакций отличных от русской (английский, европейские языки и др.)	шт.	1
7.	Exchange Standard CAL 2019 Single OLV NL Each Additional Product User CAL *	**Программное обеспечение должно обеспечивать:** - Обеспечивать право подключения к почтовому серверу Microsoft Exchange Server Standard 2019; - Обеспечивать право подключения к почтовому серверу Microsoft Exchange Server Standard 2016; - Обеспечивать право подключения к почтовому серверу Microsoft Exchange Server Standard 2013.	шт.	200
8.	Win Pro 10 32-bit/64-bit All Lng PK Lic Online DwnLd NR *	**Программное обеспечение Microsoft Windows Professional 10 имеет следующие характеристики:** – Наличие 64-битной версии операционной системы; – Поддержка 64-разрядных процессоров архитектуры x86; – Обеспечение полной совместимости с имеющимися у Заказчика приложениями, разработанными и сертифицированными для работы под ОС Microsoft Windows	шт.	19

		версий 7, 8, 8.1, 10; – Возможность удаленного управления рабочим столом; – Возможность использования ОС в виртуальных средах на серверах сети и в физической среде; – Должна быть предусмотрена возможность запускать не менее одной копии в физической среде; – Интеграция с корпоративной службой единого каталога Active Directory Domain Services с поддержкой групповых политик и сценариев централизованного управления; – Поддерживаться протоколы HTTP, HTTPS, SMB, IPsec и SSL; – Встроенная возможность обеспечения регламентного функционирования программного обеспечения, эксплуатируемого Заказчиком, без необходимости внесения изменений в исходные коды (или иные первичные ресурсы) этого ПО; – Встроенная возможность обеспечения регламентного функционирования программного обеспечения, эксплуатируемого Заказчиком, без необходимости использования эмуляторов и/или средств виртуализации; – Встроенная возможность обеспечения регламентного функционирования компонентов пакета офисных приложений «Microsoft Office» 2016 / 2013 / 2010 / 2016 /2019 в различных редакциях, без необходимости использования эмуляторов и/или средств виртуализации. Программное обеспечение Microsoft Windows Professional 10 должно обеспечить полную, гарантированную на 100% совместимость работы с ним имеющихся у Заказчика программных продуктов: средства защиты информации средства защиты информации Крипто-ПРО, КриптоАРМ 5, Программный комплекс 1С: Бухгалтерия бюджетного учреждения 8, СПАРК, АЦК-Планирование, АЦК-Финансы, АЦК-Мунзаказ, СБИС, ДЕЛО-WEB, VIPNet, OTR, а также программных продуктов, использующих .NET framework разработанных и сертифицированных для работы под операционную систему Microsoft Windows. Программное обеспечение не должно быть демонстрационным или являться пробной версией **Неисключительное право, предоставляемое Заказчику, включает в себя право использовать программное обеспечение на территории Российской Федерации следующими способами:** – запись и хранение программного обеспечения в памяти ЭВМ и осуществление действий, необходимых для функционирования программного обеспечения в соответствии с его прямым назначением; – адаптация программного обеспечения встроенными в него средствами исключительно для собственных нужд; – изготовление копий программного обеспечения, при условии, что эти копии предназначены только для архивных целей, или для осуществления тестовых работ, проводимых для апробации модернизированной версии программного обеспечения перед вводом ее в эксплуатацию, или для замены экземпляра программного обеспечения в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования. **1. Антивирусные средства должны включать:** • Программные средства антивирусной защиты для рабочих станций Windows. • Программные средства антивирусной защиты для рабочих станций MacOS. • Программные средства антивирусной защиты для рабочих станций Linux. • Программные средства антивирусной защиты для файловых серверов Windows.		

		• Программные средства антивирусной защиты для файловых серверов Linux. • Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows. • Программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов). • Программные средства централизованного управления, мониторинга и обновления. • Обновляемые базы данных сигнатур вредоносных программ и атак. • Эксплуатационную документацию на русском языке. Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке. **Требования к программным средствам антивирусной защиты для рабочих станций Windows** Программные средства антивирусной защиты для рабочих станций Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: • Microsoft Windows 10, XP Professional SP3 и выше x86 • Microsoft Windows Vista SP2 и выше x86 /x64 • Microsoft Windows 7 Professional / Enterprise /Ultimate x86 / x64 • Microsoft Windows 7 Professional / Enterprise /Ultimate SP1 и выше x86 / x64 • Microsoft Windows 8 Professional / Enterprise x86 / x64 • Microsoft Windows 8.1 Professional / Enterprise x86 / x64 • Microsoft Windows Embedded Standard 7 SP1 x86 / x64 • Microsoft Windows Embedded POSReady 7 x86 / x64 • Microsoft Windows Embedded 8.0 Standard x64 • Microsoft Windows Embedded 8.1 Industry Pro x64 **Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:** • Резидентный антивирусный мониторинг. • Защита от программ-маскировщиков, программ автодозвона на платные сайты. • Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы. • Антивирусное сканирование по команде пользователя или администратора и по расписанию. • Запуск задач по расписанию и/или сразу после загрузки операционной системы. • Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем. • Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу. • Защита электронной корреспонденции от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP — независимо от используемого почтового клиента; • Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных сайтов. • Блокировка баннеров и всплывающих окон загружаемых с Web-страниц. • Распознавание и блокировка фишинг-сайтов.		

		• Проверка трафика ICQ и MSN, для обеспечения безопасности работы с интернет-пейджерами. • Защита от еще не известных вредоносных программ на основе анализа их поведения. • Возможность определения аномального поведения приложения с помощью анализа последовательности действий этого приложения. Возможность совершить откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных вредоносными программами файлов. • Возможность ограничения привилегий исполняемых программ таких как запись в реестр, доступ к файлам и папкам. Автоматическое определение уровней ограничения на основании репутации программы. • Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ • Защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные. • Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме MD5, так и по заранее заданным категориям приложений, предоставляемым вендором, а также обеспечивать возможность исключения из правил для определенных пользователей из AD. • Осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из AD. • Осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера, а также возможность блокировки определенного типа информации (аудио, видео и др.). Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из AD. • Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось. • Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. • Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства. • Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей. • Возможность установки только выбранных компонентов программного средства антивирусной защиты. • Полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии SingleSign On. Обязательно наличие инструментов восстановления зашифрованного содержимого в случае сбоев загрузочного агента		

		или файлов ОС. Должна быть реализована поддержка UEFI-систем. • Поддержка двухфакторной аутентификации при полнодисковом шифровании. • Шифрование файлов с возможностью гибкого указания шифруемого контента(по местоположению, по расширению, по создающему файл приложению). Наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений. • Шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации. • Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления. **Требования к программным средствам антивирусной защиты для файловых серверов Windows** Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: • Microsoft Windows Small Business Server 2008 Standard/Premium x32/x64 • Microsoft Windows Small Business Server 2011 Essentials / Standard x64 • Microsoft Windows MultiPoint Server 2011 x64 edition • Microsoft Windows Server 2003 Standard/Enterprise SP2 x32/x64 • Microsoft Windows Server 2003 R2 Standard/Enterprise Edition SP2 R2 x32/x64 • Microsoft Windows Server 2008 Standard/Enterprise SP1 x32/x64 • Microsoft Windows Server 2008 R2 x64 Standard/Enterprise • Microsoft Windows Server 2008 R2 x64 Standard/Enterprise SP1 и выше • Microsoft Windows Server 2008 Foundation • Microsoft Windows Server 2008 R2 Foundation • Microsoft Windows Server 2012 Foundation x64 • Microsoft Windows Server 2012 Standard/Essentials x64 • Microsoft Windows Server 2012 R2 Standard/Essentials x64 Edition **Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:** • Резидентный антивирусный мониторинг. • Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы. • Антивирусное сканирование по команде пользователя или администратора и по расписанию. • Запуск задач по расписанию и/или сразу после загрузки операционной системы. • Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу. • Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ • Защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные. • Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.		

		• Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем. • Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось. • Настройки проверки критических областей сервера в качестве отдельной задачи. • Регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме. • Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий). • Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей. • Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления. **Требования к программным средствам антивирусной защиты для файловых серверов Linux** Программные средства антивирусной защиты для файловых серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: • Red Hat Enterprise Linux 6.0 – 6.6 Server x32/x64 • Red Hat Enterprise Linux 5.* Server x32/x64 • Red Hat Enterprise Linux 7.0 Server x64 • CentOS-5.* x32/x64 • CentOS-6.0-6.6 x32/x64 • CentOS-7.0 x64 • SUSE Linux Enterprise Server 11 SP3 x32/x64 • SUSE Linux Enterprise Server 12 x64 • Novel Open Enterprise Server 11 SP1\SP2 x32/x64 • Ubuntu Server 12.04.2 LTS x32/x64 • Ubuntu Server 14.04 LTS x32/x64 • Ubuntu Server 14.10 LTS x32/x64 • Debian GNU/Linux 7.5/7.6/7.7 x32/x64 • OpenSuse 13.1 x32 • Oracle Linux 6.5 x32/x64 • Oracle Linux 7.0 x64 Программные средства антивирусной защиты для файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей: • Резидентный антивирусный мониторинг. • Антивирусное сканирование по команде пользователя или администратора и по расписанию. • Проверка ресурсов доступных по SMB/ CIFS/ NFS • Антивирусная проверка и лечение файлов в архивах. • Запуск задач по расписанию и/или сразу после загрузки операционной системы. • Помещение подозрительных и поврежденных объектов на карантин. • Формирование отчетов в форматах HTML, CSV, PDF и XLS. • Возможность перехвата и проверки файловых операций на уровне SAMBA. • Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность.		

		• Удаленно через веб-браузер управлять антивирусом и настраивать его. • Централизованно управляться с помощью единой системы управления. **Требования к программным средствам антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows** Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: • Microsoft Windows Server 2003 Standard/Enterprise x32/x64SP2 • Microsoft Windows Server 2003 R2 Standard/ Enterprise Edition x32/x64SP2 • Microsoft Windows Server 2008 Standard/ Enterprise/ DataCenter x32/x64 SP1 и выше. • Microsoft Windows Server 2008 Core Standard/ Enterprise / DataCenter x32/x64 SP1 и выше • Microsoft Windows Server 2008 R2 Standard/ Enterprise/ DataCenter x64 SP1 или выше. • Microsoft Windows Server 2008 R2 Core Standard/ Enterprise / DataCenter x64 SP1 и выше • Microsoft Windows Server 2012 Standard/ Essential/ DataCenter/Foundation • Microsoft Windows Server 2012 Core Standard/ Essential/ DataCenter/Foundation • Microsoft Windows Server 2012 R2 Standard/ Essential/ DataCenter/Foundation • Microsoft Windows Server 2012 R2 Core Standard/ Essential/ DataCenter/Foundation • Microsoft Windows Storage Server 2008 R2 x64 • Microsoft Windows Storage Server 2012 • Microsoft Windows Storage Server 2012 R2 • Microsoft Windows Hyper-V Server 2008 R2 SP1 • Microsoft Windows Hyper-V Server 2012 • Microsoft Windows Hyper-V Server 2012 R2 Терминальные сервера: • Microsoft Terminal Services на базе Windows Server 2003 • Microsoft Terminal Services на базе Windows Server 2008 • Microsoft Terminal Services на базе Windows Server 2012 • Microsoft Terminal Services на базе Windows Server 2012 R2 • Citrix Presentation Server 4.0/4.5 • Citrix XenApp 4.5/5.0/6.0/6.5/7.0/7.1/7.5/7.6 • Citrix XenDeskTop 7.0/7.1/7.5/7.6 **Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:** • Осуществление антивирусной проверки на серверах, выполняющих разные функции: Серверов терминалов и принт-серверов; Серверов приложений и контроллеров доменов; Файловых серверов. • Возможность использования для защиты кластера серверов. • Проверка следующих объектов защищаемого сервера при доступе к ним: Файлов при их записи и считывании; Альтернативных потоков файловых систем (NTFS-streams); Главной загрузочной записи и загрузочных секторов локальных жестких дисков и съемных носителей • Предотвращение вирусных эпидемий за счет фиксации возникновения вирусных атак. • Восстановление после заражения путем удаления всех связанных с ликвидированным вредоносным объектом записей в		

		системных файлах и реестре ОС, что предотвращает возможные сбои в работе операционной системы. • Непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting). Проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными. • Проверка по требованию, заключающаяся в однократной полной или выборочной проверке на наличие угроз объектов на сервере. • Проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи. • Помещение подозрительных и поврежденных объектов на карантин. Возможность восстановления файлов из карантина в сетевые папки • При защите терминальных серверов поддержка режимов публикации рабочего стола и публикации приложений. • Масштабируемость за счет задания количества рабочих процессов антивируса для ускорения обработки запросов к серверу при использовании многопроцессорных серверов. • Балансировка загрузки путем регулирования распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: антивирусная проверка может продолжаться в фоновом режиме. • Выбор доверенных процессов путем исключения из проверки безопасных процессов, работа которых может замедляться при антивирусной проверке (процесс резервного копирования данных, программы дефрагментации жесткого диска и другие) • Разделение прав администраторов, основанное на стандартных механизмах ОС Microsoft Windows. • Наличие встроенных исключений для стандартных ролей сервера (Контролер домена, Сервер БД и тд) • Уведомления различными методами администраторов и пользователей о событиях в антивирусной защите. Поддержка Simple Network Management Protocol (SNMP) • Поддержка технологий ReFS(Resilient file system) и CSV (Cluster Shared Volume) • Централизованно управляться с помощью единой системы управления **Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:** • Установка системы управления антивирусной защиты из единого дистрибутива. • Выбор установки в зависимости от количества защищаемых узлов. • Возможность чтения информации из AD, с целью получения данных об учетных записях компьютеров в организации • Возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети. • Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OUAD • Централизованные установка, обновление и удаление программных средств антивирусной защиты. Настройка, администрирование, просмотр отчетов и статистической информации по их работе. • Централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления. • Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, агент администрирования,		

		для локальной установки – возможность создать автономный пакет установки. • Удаленная установка программных средств антивирусной защиты с последней версией антивирусных баз. • Возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от УЗ, под которой пользователь вошел в систему , а также от того, в каком OU находится компьютер. Должна быть реализована возможность поддержки иерархии таких триггеров. • Автоматизированное обновление программных средств антивирусной защиты и антивирусных баз. • Автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей. • Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка обновлений на рабочие места пользователей сразу после их получения. • Распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере. • Автоматическое развертывание по требованию специализированной системы защиты для виртуальных инфраструктур на базе VMware ESXi, Microsoft Hyper-V, Citrix XenServer. • Построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне. • Наличие преднастроенных ролей пользователей средств централизованного управления. Должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к УЗ пользователей. • Создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня. • Поддержка мультиарендности (multi-tenancy) для серверов управления. • Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации. • Доступ к облачным серверам производителя антивирусного ПО через сервер управления. • Автоматическое распространение лицензии на клиентские компьютеры. • Инвентаризация установленного ПО и оборудования на компьютерах пользователей. • Возможность подключения по RDP или штатными средствами из консоли управления. Пользователю должен выводиться запрос на разрешение дистанционного подключения. • Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них. • Наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal). Должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ. Возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС.		

		• Возможность импортировать образ операционной системы из дистрибутивов (WIM) • Наличие системы контроля лицензий стороннего ПО с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии. • Автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др) и автоматическая централизованная установка этих пакетов приложений на компьютеры • Функция управления мобильными устройствами через сервер Exchange ActiveSync. • Функция управления мобильными устройствами через сервер iOS MDM. • Возможность отправки SMS-оповещений о заданных событиях. • Централизованная установка приложений на управляемые мобильные устройства. • Централизованная установка сертификатов на управляемые мобильные устройства. • Поддержка функциональности управления шифрованием данных. • Интеграция с CISCO NAC и MS NAP. • Встроенная функциональность контроля доступа к сети организации с возможностью блокировки запросов неизвестных устройства или переадресации этих запросов на портал авторизации. • Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления. • Возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления. • Построение графических отчетов как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и тд. • Экспорт отчетов в файлы форматов PDF и XML. • Интеграция с системами IBM Qradar и HP Arcsight. • Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение. • Создание внутренних учетных записей для аутентификации на сервере управления. • Создание резервной копии системы управления встроенными средствами системы управления. • Поддержка Windows Failover Clustering. • Поддержка интеграции с Windows сервисом Certificate Authority. • Наличие веб-консоли управления приложением. • Веб-консоль должна обеспечивать возможность подключения пользователей с целью: Установки агента управления на мобильное устройство, просмотр мобильных устройств, отправка команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя. • Наличие системы контроля возникновения вирусных эпидемий.		
9.	Photoshop CC for Teams Multiple Platforms Multi European Languages New Subscription *	**Программный продукт должен обладать следующими характеристиками:** • Локальная лицензия сроком на не менее 12 (двенадцати) календарных месяцев; • Локальная лицензия на пользователя, которая должна назначаться на учетную запись ПО;	шт.	15

		• Редактор растровой графики с поддержкой аппаратного ускорения, работы с трехмерной графикой; • Поддержка файлового формата JPEG; • Поддержка файлового формата PSD; • Поддержка файлового формата TIFF; • Поддержка файлового формата PNG; • Поддержка остальных файловых форматов фотокамер и большинства растровых форматов файлов; • Русифицированный язык интерфейса; • Возможность использования ПО без наличия постоянного подключения к Интернет; • Работа с 8/16/24/32-разрядными графическими данными и изображениями с произвольным числом каналов; • Поддержка 3D-принтеров и 3D-печати. **Программный продукт должен включать следующие основные функции:** • Возможность работы с трехмерной графикой; • Поддержка анализа изображений; • Наличие средств автоматической ретуши и пакетной обработки; • Поддержка изобразительных эффектов и средств цветокоррекции; • Управление цветом по стандарту ICC; • Поддержка цветовых пространств Lab, RGB, CMYK; • Сохранение данных в фоновом режиме и восстановление изображения после программных сбоев; • Возможность работы со слоями с управлением прозрачностью, режимами наложения цвета, фильтрацией слоев по ключевым признакам, группировкой слоев и сохранением переключаемых слоевых композиций; • Обратимое применение эффектов в виде настраиваемых корректирующих слоев и смарт-фильтров, примененных к контейнеру с оригиналом изображений; • Обратимое кадрирование изображений; • Функции с заполнением областей на базе анализа содержимого окружающих участков при удалении объектов, перемещении объектов, точечной ретуши; • Стабилизация дрожания камеры; • Функция трансформации изображений с сохранением пропорций значимых объектов; • Возможность создания 3D-логотипов и графических объектов на основе текстовых слоев, элементов, контуров и слоев-масок; • Динамическое применение к объектам эффектов, таких как закручивание, вращение, выдавливание, скос и деформация; • Создание множественных настраиваемых эффектов размытия на изображении; • Инструменты рисования с имитацией реальных кистей и возможностью задания параметров формы, длины, жесткости и затухания; • Автоматизация типовых операций обработки изображений с помощью условных действий. **Способ и срок передачи прав:** одновременно с передачей программного обеспечения Заказчику должно быть передано право использования вышеуказанного программного обеспечения на основе простой (неисключительной) лицензии следующими способами: 1) Воспроизводить, запускать и использовать программное обеспечение в соответствии с количеством переданных лицензий; 2) возможность делать архивную копию для целей		

		резервирования; 3) использовать программное обеспечение без каких-либо отчислений правообладателю. **Территория использования:** Российская Федерация. **Требования к технической и консультационной поддержке:** Экземпляры программного обеспечения должны включать право обновления программного обеспечения в течение 12 (двенадцати) календарных месяцев с момента подписания Лицензиатом акта приема-передачи ключевых (регистрационных) файлов. Консультационная поддержка должна осуществляться в течение 12 (двенадцати) календарных месяцев с момента подписания Лицензиатом акта приема-передачи ключевых (регистрационных) файлов.		
10.	Acrobat Pro DC for teams ALL Multiple Platforms Multi European Languages Team Licensing Subscription New *	Версия не ниже 2017 года Программа для работы с файлами PDF должна быть лицензионной. Программа работы с файлами PDF должна соответствовать правилам лицензирования компании-разработчика. **Adobe Acrobat Professional DC** – это полностью обновленная настольная версия лучшего в мире решения для работы с файлами PDF. В состав **Adobe Acrobat Professional DC** входит мобильное приложение, позволяющее заполнять, подписывать и отправлять формы PDF с любых устройств. Облачные сервисы Document Cloud в Acrobat Pro DC позволяют создавать, экспортировать, редактировать и отслеживать файлы PDF, открывая их в любом web-браузере. Последние версии файлов всегда будут доступны независимо от того, на каком устройстве происходит работа. В рамках планов подписок для бизнеса доступна веб-консоль Adobe Admin Console, с помощью которой можно с легкостью управлять лицензиями. Идеально подходит организациям, которые хотят приобрести инструменты для двух или более сотрудников. **Поддерживаемые операционные системы:** Microsoft Windows 7 с пакетом обновления 1, Windows 8.1 или Windows 10 Срок действия лицензии: 1 год.	шт.	43
11.	ABBYY FineReader 15 Business 1 year (Standalone) *	Программный продукт для оптического распознавания текстов (далее – «Программный продукт») должен соответствовать следующим требованиям: - функционировать на компьютерах, работающих под управлением операционных систем Microsoft® Windows® 8, Microsoft Windows 7, Microsoft Windows Vista®, Microsoft Windows XP, Microsoft Windows Server® 2008 R2, Microsoft Windows Server 2003; - быть совместимым с любыми TWAIN- и WIA-совместимыми сканерами и многофункциональными устройствами, подключенными, как локально, так и через вычислительную сеть; - обеспечивать возможность автоматического сканирования страниц документов из пачки с помощью сканера с автоподатчиком; - обеспечивать распознавание фотографий документов, сделанных цифровой камерой и камерой мобильного телефона;	шт.	76

		- иметь собственный интерфейс сканирования, а также поддерживать интерфейс сканера и/или многофункционального устройства; - поддерживать интеграцию с программными продуктами Microsoft® Word, Excel®, Outlook®, Word Pro®, WordPerfect® - не должен прерывать процесс сканирования и распознавания изображений, имеющих низкое качество; - иметь модуль выравнивания перекоса и трапециевидных искажений, возникших в процессе сканирования изображений или съемки камерой; - позволять пользователю просматривать полные изображения страниц документов; - иметь возможность автоматической предобработки изображения после открытия; - позволять пользователю выполнять ручную обработку сканированных или сфотографированных изображений, в том числе: • повороты изображений на углы, кратные 90° • инверсию изображения; • разбивку и обрезку изображений; • коррекцию яркости, контрастности, разрешения, уровней; • очищать изображения от искажений и помех; • удаление отдельных фрагментов изображения • повторное сканирование изображения; - автоматически определять язык(и) документа; - распознавать гиперссылки; - обеспечивать распознавание пакетов документов; - обеспечивать распознавание штрих-кодов, в том числе двухмерных типа PDF-417; - позволять настраивать цветовой режим документов: цветной или черно-белый; - позволять вручную указывать области для распознавания, изменять их назначение и удалять их; - поддерживать возможность распознавания с обучением, в т.ч. с использованием пользовательских эталонов; - поддерживать возможность создания пользовательских языков распознавания, подключения пользовательских словарей - содержать инструменты для улучшения результатов распознавания; - позволять вносить правки в результат распознавания, в т.ч. изменять форматирование распознанного текста; - определять и выделять неуверенно распознанные символы и предлагать варианты автозамены, используя встроенные словари для основных языков; - сохранять результаты распознавания в форматах DOC, DOCX, XLS, XLSX, PCX, DCX, PPTX, RTF, PDF, PDF/A, HTML, CSV, TXT; -обеспечивать возможность задания пароля в результирующих файлах в формате PDF; - позволять создавать PDF-документы с тегами, обеспечивающими удобство просмотра на экранах любого размера, в частности, на экранах карманных компьютеров;		

		- обеспечивать возможность сохранения черно-белых и цветных изображений в стандартных форматах: BMP, TIFF, PCX, DCX, JPEG, PNG; - содержать инструменты для удаления конфиденциальной информации; Пользователям должна быть предоставлена возможность получения технических консультаций по вопросам функционирования Программного продукта в режиме «on line» на русском языке.		
12.	Acronis Защита Данных Расширенная для физического сервера *	Требования к системе резервного копирования и аварийного восстановления данных сервера под управлением ОС семейств Windows и Linux 1. ПО должно соответствовать следующим системным требованиям: 1.1. ПО должно иметь возможность резервного копирования и аварийного восстановления данных на компьютерах, работающих под управлением следующих ОС: •Windows Server 2008 R2 — выпуски Standard, Enterprise, Datacenter, Foundation и Web •Windows MultiPoint Server 2010/2011/2012 •Windows Small Business Server 2011 — все выпуски •Windows 8 или 8.1 — все выпуски, кроме Windows RT (x86, x64) •Windows Server 2012/2012 R2 — все выпуски •Windows Storage Server 2003/2008/2008 R2/2012/2012 R2 •Windows Server 2016 — Technical Preview 4 •Любые дистрибутивы Linux с версией ядра от 2.4.6 1.2. ПО должно поддерживать следующие платформы: •32-разрядные (x86) •64-разрядные (x64) 1.3. ПО должно поддерживать следующие способы загрузки: •BIOS •UEFI 1.4. ПО должно поддерживать следующие файловые системы: •FAT16/32 •NTFS •ReFS •Ext2/Ext3/Ext4 •ReFS •ReiserFS3 •ReiserFS4 •XFS •JFS •Linux SWAP 1.5. ПО должно поддерживать следующие носители информации: •Жесткие диски HDD и SSD •Сетевые устройства хранения (SAN и NAS) •CD-R(W) •DVD-RW, DVD+R(W) •SCSI, ATAPI, ATA, SSA, SAS и SATA, а также RAID-массивы. и накопители USB 1.1 / 2.0 / 3.0 •Онлайн-хранилище •NFS •Жесткие диски (DAS); •Сетевые устройства хранения (SAN и NAS); •CD-R(W), DVD-RW, DVD+R(W);	шт.	6

		•ZIP®, Rev® и другие магнитооптические накопители; •P-ATA (IDE), S-ATA, SCSI, IEEE1394 (Firewire) и накопители USB 1.1 / 2.0 / 3.0, устройства хранения данных PCMCIA; •Сервер FTP или SFTP; •Облачное хранилище; •Ленточные устройства, автоматические загрузчики и библиотеки, а также управление носителями и поддержка баркодов 2. ПО должно обеспечивать следующие основные функции и возможности: 2.1. ПО должно обеспечивать резервное копирование и аварийное восстановление дисков и томов со всеми хранящимися на них данными (включая приложения). 2.2. Сервер управления ПО должен устанавливаться на OS Windows Server и OS Linux. 2.3. В ПО должен присутствовать WEB интерфейс управления сервером. 2.4. ПО должно обеспечивать резервное копирование и аварийное восстановление папок и файлов. 2.5. ПО должно поддерживать следующие функции и возможности резервного копирования. 2.5.1. Создание полных, дифференциальных и инкрементных резервных копий. 2.5.2. Слияние инкрементных и дифференциальных резервных копий. 2.5.3. Автоматическое удаление устаревших резервных копий. 2.5.4. Сжатие. 2.5.5. Исключение файлов. 2.5.6. Автоматическое или ручное разбиение резервных копий. 2.5.7. Дедубликацию 2.6. ПО должно поддерживать следующие функции и возможности восстановления из резервных копий. 2.6.1. Восстановление при загрузке. 2.6.2. Восстановление на «голое железо». 2.6.3. Восстановление файлов, сохраняя настройки безопасности 2.6.4. Возможность изменить SID пользователя при восстановлении 2.6.5. Копирование отдельных файлов или папок из резервной копии с помощью Windows Explorer. 2.7. ПО должно поддерживать следующие функции и возможности управления резервными копиями: 2.7.1. Шаблоны схем резервного копирования. 2.7.2. Pre и Post команды. 2.7.3. Настраиваемая схема резервного копирования. 2.7.4. Защита резервной копии с помощью пароля. 2.7.5. Условия удаления резервных копий – количество копий, возраст копии. 2.7.6. Создание резервной копии вместе с загрузочными компонентами на съемный загрузочный носитель для возможности аварийного восстановления. 2.8. ПО должно ограничивать доступ к управлению резервным копированием и восстановлением данных для пользователя и групп пользователей путём авторизации. 2.9. Должны поддерживаться следующие условия запуска заданий на создание резервной копии: 2.9.1. Согласно заданному расписанию.		

		2.10. ПО должно позволять создавать загрузочные носители на основе Linux и WinPE. 2.11. ПО должно предоставлять возможность восстановления резервной копии диска в новую виртуальную машину любого из типов: •VMware Workstation, vSphere •Microsoft Hyper-V 3. ПО должно поддерживать следующие дополнительные функции. 3.1. Восстановление образов серверов на «голое» железо и на оборудование, отличное от того, с которого были сняты резервные копии, или на виртуальные машины. 3.2. Миграция систем с физической на виртуальную и с виртуальной на физическую. 4. ПО должно сопровождаться подпиской на техническую поддержку на период до одного года. Подписка на техническую поддержку должна предоставлять следующие возможности: 4.1. Контакт со службой технической поддержки посредством телефона, электронной почты и интерактивного чата. 4.2. Обозначение критичности проблемы при создании заявке в службе технической поддержке. 4.3. Подписка на техническую поддержку в период своего действия должна гарантировать бесплатные обновления ПО, в том числе переход на новую версию ПО. 5. ПО должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных.		
13.	Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 150-249 Node 1 year Base License *	Общие требования Антивирусные средства должны включать: • программные средства антивирусной защиты для рабочих станций Windows; • программные средства антивирусной защиты для рабочих станций MacOS; • программные средства антивирусной защиты для рабочих станций Linux; • программные средства антивирусной защиты для файловых серверов Windows; • программные средства антивирусной защиты для файловых серверов Linux; • программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов); • программные средства централизованного управления, мониторинга и обновления; • обновляемые базы данных сигнатур вредоносных программ и атак; • эксплуатационную документацию на русском языке. Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.	шт.	150

		Требования к программным средствам антивирусной защиты для рабочих станций Windows Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий: • Windows 7 Home / Professional / Enterprise (32 / 64-разрядная); • Windows 8 Professional / Enterprise (32 / 64-разрядная); • Windows 8.1 Professional / Enterprise (32 / 64-разрядная); • Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядная). Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий: • Windows Small Business Server 2008 Standard / Premium (64-разрядная); • Windows Small Business Server 2011 Essentials / Standard (64-разрядная); • Windows MultiPoint Server 2011 (64-разрядная); • Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная); • Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядная); • Windows Server 2012 Foundation / Essentials / Standard (64-разрядная); • Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная); • Windows Server 2016 (64-разрядная); • Windows Server 2019 (64-разрядная). Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей: • антивирусного сканирования в режиме реального времени и по запросу из контекстного меню объекта; • антивирусного сканирования по расписанию; • антивирусное сканирование подключаемых устройств; • эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы; • нейтрализации действий активного заражения; • анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; • анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;		

		• откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; • ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия; • облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу; • антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; • защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP; • фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов; • проверку трафика, поступающего на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики; • блокировку баннеров и всплывающих окон на загружаемых Web-страницах; • распознавания и блокировку фишинговых и небезопасных сайтов; • встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиту от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные; • контроль сетевых соединений, устанавливаемых с помощью сетевых мостов, с возможностью блокировки одновременной установки нескольких сетевых соединений; • создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме MD5 или SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме		

		черного или белого списка, а также в режиме сбора статистики или блокировки; • контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory; • записи в журнал событий о записи и/или удалении файлов на съемных дисках; • контроля работы пользователя с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory; • защиты от атак типа BadUSB; • запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. • полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On; • восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем; • поддержка двухфакторной аутентификации при полнодисковом шифровании; • шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы в не защищенного периметра с помощью пароля; • шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации; • защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; • установки только выбранных компонентов программного средства антивирусной защиты; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;		

		• запуск задач по расписанию и/или сразу после загрузки операционной системы; • гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; • ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • возможность проверки целостности антивирусной программы; • возможность добавления исключений из антивирусной проверки по хеш сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи; • наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления; • наличие защищенного хранилища для отчетов о работе антивируса; • возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей; • возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий); • возможность интеграции с Windows Defender Security Center; • наличие поддержки Antimalware Scan Interface (AMSI); • наличие поддержки Windows Subsystem for Linux (WSL); • возможность распределения прав доступа к корпоративным ресурсам (MTP) в рамках контроля устройств. Требования к программным средствам антивирусной защиты для рабочих станций Mac Программные средства антивирусной защиты для рабочих станций Mac должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: • macOS Mojave 10.14; • macOS High Sierra 10.13; • macOS Sierra 10.12. Программные средства антивирусной защиты для рабочих станций Mac должны обеспечивать реализацию следующих функциональных возможностей: • резидентный антивирусный мониторинг; • облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу; • автоматическое обновление антивирусных баз по расписанию; • резервное копирование зараженных файлов перед их удалением, для возможности восстановления;		

		• эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы; • защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные; • блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты; • защита информации, передаваемой через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик); • ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления, с возможностью управлять шифрованием FileVault. Требования к программным средствам антивирусной защиты для рабочих станций Linux Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 32-битных операционных систем следующих версий: • Ubuntu 16.04 LTS; • Red Hat Enterprise Linux 6.7 и выше; • Red Hat Enterprise Linux 7.2 и выше; • CentOS 6.7 и выше; • Debian GNU / Linux 8.6 и выше; • Debian GNU / Linux 9.4 и выше; • Linux Mint 18.2 и выше; • Linux Mint 19 (последняя версия); • Альт Линукс СПТ 7.0.6 (работа с помощью графического пользовательского интерфейса (GUI) не поддерживается); • Альт Линукс СПТ 8.0.0 Рабочая станция; • Альт Линукс СПТ 8.0.0 Сервер; • Альт Линукс 8.2 Рабочая станция; • Альт Линукс 8.2 Рабочая станция К; • Альт Линукс 8.2 Сервер; • Альт Линукс 8.2 Образование; • Лотос; • Гослинукс 6.6. Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 64-битных операционных систем следующих версий: • Ubuntu 16.04 LTS; • Ubuntu 18.04 LTS; • Red Hat Enterprise Linux 6.7 и выше; • Red Hat Enterprise Linux 7.2 и выше; • CentOS 6.7 и выше;		

		• CentOS 7.2 и выше; • Debian GNU / Linux 8.6 и выше; • Debian GNU / Linux 9.4 и выше; • OracleLinux 7.3 и выше; • SUSE Linux Enterprise Server 15; • openSUSE 15; • Альт Линукс СПТ 7.0.6 (работа с помощью графического пользовательского интерфейса (GUI) не поддерживается); • Альт Линукс СПТ 8.0.0 Рабочая станция; • Альт Линукс СПТ 8.0.0 Сервер; • Альт Линукс 8.2 Рабочая станция; • Альт Линукс 8.2 Рабочая станция К; • Альт Линукс 8.2 Сервер; • Альт Линукс 8.2 Образование; • Amazon Linux AMI; • Linux Mint 18.2 и выше; • Linux Mint 19 (последняя версия); • Micro Focus Open Enterprise Server 2018; • Astra Linux Special Edition 1.5 (обычный режим и режим замкнутой программной среды); • Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды); • Циркон 36КТ; • Циркон 36СТ; • ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем; • ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем; • ЕМИАС 1.0; • Гослинукс 6.6; • Лотос; • РЕД ОС 7.2. Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей: • резидентного антивирусного мониторинга; • облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу; • проверку ресурсов доступных по SMB / NFS; • эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; • антивирусное сканирование по команде пользователя или администратора и по расписанию; • антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.; • проверку сообщений электронной почты в текстовом формате (Plain text); • наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм		

		кеширования информация о проверенных и не измененных после проверки файлов); • защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования; • помещение подозрительных и поврежденных объектов на карантин; • проверку почтовых баз приложений Microsoft Outlook • возможность перехвата и проверки файловых операций на уровне SAMBA; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность экспортировать и сохранять отчеты в форматах HTML и CSV; • гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; • сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность; • возможность управления через пользовательский графический интерфейс без root прав; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления. Требования к программным средствам антивирусной защиты для файловых серверов Windows Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: **32-разрядных операционных систем Microsoft Windows** • Windows Server® 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Server 2008 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше. **64-разрядных операционных систем Microsoft Windows** • Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;		

		• Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Microsoft Small Business Server 2008 Standard / Premium; • Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше; • Microsoft Small Business Server 2011 Essentials / Standard; • Microsoft Windows MultiPoint™ Server 2011 Standard / Premium; • Windows Server 2012 Foundation / Essentials / Standard / Datacenter; • Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter; • Microsoft Windows MultiPoint Server 2012 Standard / Premium; • Windows Storage Server 2012; • Windows Hyper-V Server 2012; • Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; • Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter; • Windows Storage Server 2012 R2; • Windows Hyper-V Server 2012 R2; • Windows Server 2016 Essentials / Standard / Datacenter; • Windows Server 2016 MultiPoint; • Windows Server 2016 Core Standard / Datacenter; • Microsoft Windows MultiPoint Server 2016; • Windows Storage Server 2016; • Windows Hyper-V Server 2016; • Windows Server 2019 Essentials / Standard / Datacenter; • Windows Server 2019 Core; • Windows Storage Server 2019; • Windows Hyper-V Server 2019. Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей: • антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов; • антивирусное сканирование по команде пользователя или администратора и по расписанию; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;		

		• антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB; • защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков; • непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными. Анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • возможность проверки контейнеров Microsoft Windows; • защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные; • защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления; • наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп); • компонент создания специальных правил должен контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме MD5 или SHA256; • компонент создания специальных правил должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должен иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы; • осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory; • осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем; • информирование администратора о подключении внешних устройств;		

		• механизмы защиты от эксплуатирования уязвимостей в памяти процессов с помощью техник снижения рисков; • ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи; • настройки проверки критических областей сервера в качестве отдельной задачи; • регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме; • наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий); • ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом; • возможность интеграции с SIEM системами; • наличие механизмов автоматической генерации правил для контроля устройств и приложений; • возможность указания количества рабочих процессов антивируса вручную; • возможность отключить графический интерфейс; • наличие удаленной и локальной консоли управления; • управления параметрами антивируса из командной строки; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • возможность защиты подключаемых по ICAP, RPC сетевых хранилищ; возможность защиты от шифрования для устройств NetApp; Требования к программным средствам антивирусной защиты для файловых серверов Linux Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 32-битных операционных систем следующих версий: • Ubuntu 16.04 LTS; • Red Hat Enterprise Linux 6.7 и выше; • Red Hat Enterprise Linux 7.2 и выше; • CentOS 6.7 и выше; • Debian GNU / Linux 8.6 и выше; • Debian GNU / Linux 9.4 и выше; • Linux Mint 18.2 и выше;		

		• Linux Mint 19 (последняя версия); • Альт Линукс СПТ 7.0.6 (работа с помощью графического пользовательского интерфейса (GUI) не поддерживается); • Альт Линукс СПТ 8.0.0 Рабочая станция; • Альт Линукс СПТ 8.0.0 Сервер; • Альт Линукс 8.2 Рабочая станция; • Альт Линукс 8.2 Рабочая станция К; • Альт Линукс 8.2 Сервер; • Альт Линукс 8.2 Образование; • Лотос; • Гослинукс 6.6. Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 64-битных операционных систем следующих версий: • Ubuntu 16.04 LTS; • Ubuntu 18.04 LTS; • Red Hat Enterprise Linux 6.7 и выше; • Red Hat Enterprise Linux 7.2 и выше; • CentOS 6.7 и выше; • CentOS 7.2 и выше; • Debian GNU / Linux 8.6 и выше; • Debian GNU / Linux 9.4 и выше; • OracleLinux 7.3 и выше; • SUSE Linux Enterprise Server 15; • openSUSE 15; • Альт Линукс СПТ 7.0.6 (работа с помощью графического пользовательского интерфейса (GUI) не поддерживается); • Альт Линукс СПТ 8.0.0 Рабочая станция; • Альт Линукс СПТ 8.0.0 Сервер; • Альт Линукс 8.2 Рабочая станция; • Альт Линукс 8.2 Рабочая станция К; • Альт Линукс 8.2 Сервер; • Альт Линукс 8.2 Образование; • Amazon Linux AMI; • Linux Mint 18.2 и выше; • Linux Mint 19 (последняя версия); • Micro Focus Open Enterprise Server 2018; • Astra Linux Special Edition 1.5 (обычный режим и режим замкнутой программной среды); • Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды); • Циркон 36КТ; • Циркон 36СТ; • ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем; • ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем; • ЕМИАС 1.0; • Гослинукс 6.6; • Лотос; • РЕД ОС 7.2.		

		Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей: • резидентного антивирусного мониторинга; • облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу; • проверку ресурсов доступных по SMB / NFS; • эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; • антивирусное сканирование по команде пользователя или администратора и по расписанию; • антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.; • проверку сообщений электронной почты в текстовом формате (Plain text); • наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов); • защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования; • помещение подозрительных и поврежденных объектов на карантин; • проверку почтовых баз приложений Microsoft Outlook • возможность перехвата и проверки файловых операций на уровне SAMBA; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность экспортировать и сохранять отчеты в форматах HTML и CSV; • гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; • сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность; • возможность управления через пользовательский графический интерфейс без root прав; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.		

		Требования к программным средствам антивирусной защиты мобильных устройств Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС: • Android 4.2– 9.0; • Apple iOS 10.0 – 12. Программные средства для антивирусной защиты смартфонов для ОС Android должны обеспечивать следующую функциональность: • постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки на репутационных облачных сервисам производителя антивирусных средств защиты; • проверка файловой системы устройства по требованию и по расписанию; • мгновенная проверка устанавливаемых приложений • блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты; • поддержка белых списков разрешенных сайтов; • наличие хранилища для изолирования зараженных объектов; • обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию; • блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений; • поддержка белых списков разрешенных приложений; • блокировка системных приложений; • возможность отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM); • базовая поддержка Android for Work; • наличие возможности создания\добавления специальной оболочки для мобильных программ с целью контроля действий программы, возможностью удаления данных и настроек программы, добавления дополнительного пароля для старта приложения, в том числе с помощью учетных данных Active Directory ; • возможность заблокировать wi-fi и bluetooth модули, а так же использование камеры мобильного устройства; • возможность указать параметры подключения к wi-fi сетям; • возможность указать обязательные к установке приложения; • возможность блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset); • постоянная проверка телефона на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления		

		данных, запрета запуска корпоративных приложений при выявлении несоответствий; • поддержка технологий Samsung KNOX1 и KNOX2. Программные средства для антивирусной защиты смартфонов для ОС Apple iOS должны обеспечивать следующую функциональность, в том числе и с установленным плагином управления: • возможность удаленной настрйоки параметров iOS MDM-устройств с помощью групповых политик; • возможность отправки команды блокирвоания и удаления данных; • возможность создавать групповые политики безопасности мобильных устройств; • удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM; • получать отчеты и статистику о работе мобильных устройств пользователей; • блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты; • возможность определения местоположения устройства. Решение должно централизованно управлять с помощью единой консоли управления. Требования к программным средствам централизованного управления, мониторинга и обновления Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: • Microsoft Windows 7 32-разрядная / 64-разрядная; • Microsoft Windows 8 32 разрядная / 64-разрядная; • Microsoft Windows 8;1 32-разрядная / 64-разрядная; • Microsoft Windows 10 32-разрядная / 64-разрядная; • Windows Server 2008, 2008 R2 32-разрядная / 64-разрядная; • Windows Server 2012, 2012 R2 64-разрядная; • Windows Server 2016 64-разрядная. Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах: • VMware vSphere 5.5, 6; • VMware Workstation 12.x Pro; • Microsoft Hyper-V Server 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2; • Microsoft Virtual PC 2007 (6.0.156.0); • Citrix XenServer 6.2, 6.5, 7; • Parallels Desktop 11 для Mac; • Oracle VM VirtualBox 4.0.4-70112 (поддерживаются гостевые операционные системы Windows).		

		Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: • Microsoft SQL Server 2008 Express 32-разрядная; • Microsoft SQL 2008 R2 Express 64-разрядная; • Microsoft SQL 2012 Express, 2014 Express 64-разрядная; • Microsoft SQL Server 2008 (все редакции) 32-разрядная / 64-разрядная; • Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная; • Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная; • Microsoft SQL Server 2012 (все редакции) 64-разрядная; • Microsoft SQL Server 2014 (все редакции) 64-разрядная; • Microsoft SQL Server 2016 (все редакции) 64-разрядная; • Microsoft SQL Server 2017 (для Windows) 64-разрядная; • Microsoft Azure SQL Database; • MySQL 5.5 32-разрядная / 64-разрядная (не поддерживаются версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5); • MySQL Enterprise 5.5 32-разрядная / 64-разрядная; • MySQL 5.6 32-разрядная / 64-разрядная; • MySQL Enterprise 5.6 32-разрядная / 64-разрядная; • MySQL 5.7 32-разрядная / 64-разрядная; • MySQL Enterprise 5.7 32-разрядная / 64-разрядная. Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей: • установка системы управления антивирусной защиты из единого дистрибутива; • выбор установки в зависимости от количества защищаемых узлов; • возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации; • возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети; • автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD; • централизованные установка, обновление и удаление программных средств антивирусной защиты; Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе; • централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления; • сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям; • наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO,		

		средствами системы управления, для локальной установки – возможность создать автономный пакет установки; • возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от УЗ, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности; Должна быть реализована возможность поддержки иерархии таких триггеров; • автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; • тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка обновлений на рабочие места пользователей сразу после их получения; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; • наличие преднастроенных ролей пользователей средств централизованного управления; • должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей; • создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня; • поддержка мультиарендности (multi-tenancy) для серверов управления; • обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации; • доступ к облачным серверам производителя антивирусного ПО через сервер управления; • автоматическое распространение лицензии на клиентские компьютеры; • инвентаризация установленного ПО и оборудования на компьютерах пользователей; • возможность подключения по RDP или штатными средствами из консоли управления; • пользователю должен выводиться запрос на разрешение дистанционного подключения; • наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;		

		• наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal); • должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ; • возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС; • возможность импортировать образ операционной системы из дистрибутивов (WIM) • наличие системы контроля лицензий стороннего ПО с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии; • автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др) и автоматическая централизованная установка этих пакетов приложений на компьютеры • функция управления мобильными устройствами через сервер Exchange ActiveSync; • функция управления мобильными устройствами через сервер iOS MDM; • возможность отправки SMS-оповещений о заданных событиях; • централизованная установка приложений на управляемые мобильные устройства; • централизованная установка сертификатов на управляемые мобильные устройства; • поддержка функциональности управления шифрованием данных; • возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления; • возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления; • построение графических отчетов как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и тд; • наличие преднастроенных стандартных отчетов о работе системы; • экспорт отчетов в файлы форматов PDF и XML; • централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение; • создание внутренних учетных записей для аутентификации на сервере управления;		

		• создание резервной копии системы управления встроенными средствами системы управления; • поддержка Windows Failover Clustering; • поддержка интеграции с Windows сервисом Certificate Authority; • наличие веб-консоли управления приложением; • наличие портала самообслуживания пользователей; • портал самообслуживания должен обеспечивать возможность подключения пользователей с целью: Установки агента управления на мобильное устройство, просмотр мобильных устройств, отправка команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя; • наличие системы контроля возникновения вирусных эпидемий; • возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF. • возможность установки в облачной инфраструктуре Microsoft Azure; • возможность интеграции по OpenAPI • возможность Требования к обновлению антивирусных баз Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей: • регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток; • множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации; • проверку целостности и подлинности обновлений средствами электронной цифровой подписи. Требования к эксплуатационной документации Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе «Руководство пользователя (администратора)». Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты. Требования к технической поддержке Техническая поддержка антивирусного программного обеспечения должна: • Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по телефону, электронной почте и через Интернет. • Web-сайт производителя АПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов.		
14.	Radmin 3 - Пакет из 150 лицензий на	Версия не ниже 3.5 Поддержка переключения сессий пользователей в Windows 10, Windows 8, Windows 7, Vista и Windows XP.	шт.	1

	150 компьютеров (за лицензию) *	Выбор режима передачи экрана: 2, 4, 16, 256, 65 тысяч или 16 миллионов цветов. Полная поддержка отображения курсора удалённого ПК: его формы, анимации и прозрачности. Поддержка прокрутки с помощью колеса мыши. Поддержка специальных клавиш и сочетаний клавиш. Поддержка высоких разрешений (ограничение на максимальное разрешение дисплея отсутствует). Возможность отображения экрана удалённого ПК в отдельном окне или в полноэкранном режиме с плавным изменением масштаба и сохранением пропорций. Поддержка нескольких одновременных соединений. Совместимость Radmin Viewer с Wine (удаленный доступ с машин, где установлена ОС Linux). Двусторонняя работа с буфером обмена с поддержкой Unicode. Адресная книга без ограничений на количество записей, древовидной структурой, drag-and-drop для записей и папок. Подключение к удалённому ПК из адресной книги в один клик. Встроенный сканер серверов Radmin. Встроенная справочная система. Режим Telnet. Текстовый и гоглосовой чаты. Удалённое управление на аппаратном уровне с поддержкой технологии Intel AMT. Удалённое выключение и перезагрузка компьютера. Доступ к BIOS удалённого ПК. Возможность загрузки удаленного компьютера с локального CD или файла образа диска. Запуск Radmin Server исключительно как системной службы. Совместимость с предыдущими версиями Radmin Server 2.x. Защита от угадывания пароля с задержкой после пяти последовательных неудачных попыток. Запись в лог файл имени пользователя и DNS расшифровки его адреса. Безопасный обмен файлами с функцией «докачки» (в случае сбоя сети можно продолжить передачу файла с момента сбоя, а не с самого начала). Интерфейс режима обмена файлами аналогичен интерфейсу Проводника Windows. Защита передаваемых данных по стандарту AES. Возможность комфортной работы для каналов с низкой пропускной способностью. Возможность использования системы безопасности Radmin с индивидуальными правами доступа для каждого пользователя и защищенной аутентификацией по логину и паролю.		

** Примечание: указание на товарный знак (его словесное обозначение) обусловлено необходимостью обеспечения совместимости приобретаемого программного продукта с программным обеспечением уже используемым Заказчиком, а также в связи с тем, что не имеется другого способа, обеспечивающего более точное и четкое описание характеристик объекта закупки, по этой причине указанное программное обеспечение не может быть заменено на эквивалент.*

Общие требования к оказанию услуг:

1. Форма поставки — электронная, осуществляется средствами электронной связи (ИНТЕРНЕТ).

   Поставщик отправляет электронное сообщение Заказчику на электронный почтовый ящик v.subbotin@ano-rsi.ru, содержащее в себе необходимые активационные ключи

доступа (коды активации), ссылки на загрузку дистрибутива программного обеспечения с сайта компании-производителя и необходимые для этого пароли.

2. Поставщик обязан предоставить права на программное обеспечение в полном объеме и в нужные сроки.
3. Передача прав на программное обеспечение должна сопровождаться оформленными в соответствии с законодательством Российской Федерации сертификатами, соглашениями, свидетельствами, подтверждающими их оригинальность. Поставщик должен представить документы, подтверждающие его полномочия на использование неисключительных (пользовательских) прав на программное обеспечение, и обслуживание этих программ в России. Если Поставщик не является производителем программного обеспечения, то он может предоставить копии дистрибьюторских или дилерских соглашений, оригиналы писем производителей продукции, предоставляющие Заказчику право использования неисключительных (пользовательских) прав на программное обеспечение. Авторизация и статус могут подтверждаться сертификатами от производителей.
4. **Дополнительные требования:** Поставщик должен являться официальным лицом, обладающим правами предоставлять (передавать), на условиях простой (неисключительной) лицензии, право на использование программ для ЭВМ, включающее использование следующими способами: неисключительное право на воспроизведении программы для ЭВМ, ограниченное правом инсталляции, копирования и запуска программы для ЭВМ. Поставщик должен подтвердить, что он действует в пределах прав и полномочий, предоставленных ему правообладателем программ для ЭВМ, и на момент предоставления (передачи) Заказчику права на использование программ для ЭВМ оно не заложено, не арестовано, не являются предметом исков третьих лиц и является лицензионным продуктом.