Техническая спецификация

№	Наименование закупаемых товаров, работ и услуг	Краткая характеристика (описание) товаров, работ и услуг	Дополнительная характеристика
1	Лицензия	на программный продукт (кроме услуг по предоставлению лицензии)	**Основные характеристики** • **Решение, которое позволит создавать, редактировать, согласовывать, сравнивать и защищать документы, а также конвертировать их в редактируемые форматы.** • **Категория:** для Организаций • **Назначение:** Редактирование документов • **Платформа**: Десктоп, Сервер • **ОС:** Windows • **Год выпуска:** не ранее 2017г • **Срок использования:** Бессрочное • **Язык интерфейса:** Мультиязычный (русский присутствует) • **Форма поставки:** Конверт с лицензией • **Объект лицензирования:** Рабочая станция, Per Seat **Совместимость** • Microsoft Windows 10 / 8.1 / 8 / 7 • Microsoft Windows Server 2016 / 2012 / 2012 R2 / 2008 R2 • Работа приложения в терминальном режиме была протестирована для следующих конфигураций: • Microsoft Windows Server 2012 R2 (Remote Desktop, RemoteApp и Remote Desktop Web Access). • Citrix XenApp 7.9 (с использованием установленного приложения, которое доступно с сервера). **Особенности** • **Распознавание текста и конвертирование:** Есть • **Открытие и просмотр PDF:** Есть • **Создание и объединение PDF из разных форматов:** Есть • **Внесение изменений напрямую в PDF-документы:** Есть • **Рецензирование и согласование PDF-документов:** Есть • **Защита PDF-документов и публикация:** Есть • **Работа с PDF-формами:** Есть • **Автоматическая обработка:** Есть • **Количество поддерживаемых языков:** 192 (русский и английский обязательно) • **Создание PDF-документов из форматов:** TIFF, JPEG, JPEG 2000, JBIG2, PNG, BMP, PCX, GIF, DjVu, XPS, DOC(X), XLS(X), PPT(X), VSD(X), HTML, RTF, TXT, ODT, ODS, ODP • **Защита PDF-документов:** С использованием уровней шифрования 40-bit RC4, 128-bit AES, 256-bit AES • **Системные требования** • Процессор: x86 или x64 с тактовой частотой от 1 ГГц и поддержкой набора инструкций SSE2

			• Место на диске: 1,2 ГБ для установки и 1,2 ГБ для работы • Дисплей: Не менее 1024x768 • Вес брутто: не более 10 г
2	Лицензия	на программный продукт (кроме услуг по предоставлению лицензии)	**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 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 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 • Microsoft Windows 10 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

			неквалифицированных пользователей. • Возможность установки только выбранных компонентов программного средства антивирусной защиты. • Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления. **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: • Mac OS X 10.9 (Mavericks) • Mac OS X 10.8 (Mountain Lion) • Mac OS X 10.7 (Lion) • Mac OS X 10.6 (Snow Leopard) • Mac OS X 10.5 (Leopard) • Mac OS X 10.4 (Tiger) • Mac OS X Server 10.6 • Mac OS X Server 10.7 Программные средства антивирусной защиты для рабочих станций Mac 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. • 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. **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 операционных систем следующих версий: • Canaima 3 x32/x64 • Red Flag Desktop 6.0 SP2 x32/x64 • Red Hat Enterprise Linux 5.8 Desktop x32/x64 • Red Hat Enterprise Linux 6.2 Desktop x32/x64 • Fedora 16 x32/x64 • CentOS-6.2 x32/x64 • SUSE Linux Enterprise Desktop 10 SP4 x32/x64 • SUSE Linux Enterprise Desktop 11 SP2 x32/x64 • openSUSE Linux 12.1 x32/x64 • openSUSE Linux 12.2 x32/x64 • Debian GNU/Linux 6.0.5 x32/x64 • Mandriva Linux 2011 x32 • Ubuntu 10.04 LTS x32/x64 • Ubuntu 12.04 LTS x32/x64 Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей:

			• Проверка ресурсов доступных по SMB/ CIFS/ NFS • Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы. • Антивирусное сканирование по команде пользователя или администратора и по расписанию. • 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. • Возможность экспортировать и сохранять отчеты в форматах HTML и CSV. • Возможность перехвата и проверки файловых операций на уровне SAMBA. • 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. • 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 • Microsoft Windows Server 2016 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

			• 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

			• 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

			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 **Требования к программным средствам антивирусной защиты мобильных устройств** Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС: • Android • Apple iOS 7.0 – 11 • Windows Phone 8.1 Решение должно централизованно управлять с помощью единой консоли управления. 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. Мгновенная проверка устанавливаемых приложений Проверка файловой системы устройства по требованию и по рассписанию • Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных

			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 получения политик безопасности через Google Cloud Messaging • Наличие возможности создания 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 AD. • Возможность заблокировать wi-fi и bluetooth модули, а так же использование камеры мобильного устройства. • Указание параметров подключения к wi-fi сетям • Наличие возможности указания обязательных к установке приложений • Блокирование нежелательных SMS сообщений. • 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. Возможность получения текущего номера SIM-карты телефона посредством СМС, возможность автоматической блокировки устройства при смене SIM-карты или при включении телефона без SIM-карты. • Поддержка технологий Samsung KNOX1 и KNOX2 Программные средства для антивирусной защиты смартфонов для ОС Apple iOS должны обеспечивать следующую функциональность: • Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты. • Наличие возможности создания 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 AD. Программные средства для антивирусной защиты смартфонов для ОС Windows Phone должны обеспечивать следующую функциональность: • Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты. • Возможность определения местоположения устройства. **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 XP Professional x32 / x64 SP2 и выше • Microsoft Windows Vista Business/Enterprise/Ultimate x86 / x64 SP1 и выше • Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64

			• Microsoft Windows 8.1 Professional / Enterprise x86 / x64 • Microsoft Windows Server 2003 x86 / x64 SP2 • Microsoft Windows Server 2008 x86 / x64 • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Small Business Server 2003 SP2 • Microsoft Windows Small Business Server 2008 • Microsoft Windows Small Business Server 2011 Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: • Microsoft SQL Express 2005/2008/2008R2/2012/2014 • Microsoft SQL Server 2005/2008/2008R2/2012/2014 • MySQL 5.0.67, 5.0.77, 5.0.85, 5.0.87(SP1), 5.0.91 • MySQL Enterprise 5.0.60(SP1), 5.0.70, 5.0.82(SP1), 5.0.90 Программные средства централизованного управления, мониторинга и обновления должны функционировать на виртуальных платформах следующих версий: • VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5) • Microsoft Hyper-V: 2008, 2008 R2, 2012, 20012 R2 • KVM интегрированный с: RHEL 5.4, 5.x и выше, SLES 11 SPx, Ubuntu 10.10 LTS • Microsoft VirtualPC 6.0.156.0 • Parallels Desktop 7 и выше • CitrixXenServer 5.6.1 FP1ивыше • Oracle VM VirtualBox 4.0.4-70112 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

			реализована возможность поддержки иерархии таких триггеров. • Автоматизированное обновление программных средств антивирусной защиты и антивирусных баз. • Автоматизированный поиск 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. • 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. • 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. • 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. • 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.

			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. **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 Республики Казахстан круглосуточно без праздников и выходных 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. **Дополнительно:** В стоимость входит - Установка и настройка центра администрирования Срок лицензии не менее 1 (одного года)
3	Система конференц связи, дискуссионная, комплект оборудования		**Технические характеристики:** • Особенности пользовательского интерфейса • Сенсорный дисплей с мультисенсорным интерфейсом для управления на основе жестов • Не менее 5-дюймовый ЖК-экран с разрешением не менее 720 x 1280 пикселей, формат изображения не менее 9:16 • Экранная виртуальная клавиатура • Не менее 1 хост-порт USB 2.0 типа A, подзарядка аккумулятора через USB в соответствии со стандартом BC1.21 • Не менее 1 порт USB 2.0 Micro B для подключения устройств • Встроенные функции Bluetooth 4.0 и NFC • Не менее 3 кнопки отключения микрофона с подсветкой • Поддержка Unicode (UTF-8) • Многоязычный интерфейс пользователя: арабский, английский (Канада/США/ Великобритания), датский, испанский, итальянский, китайский, корейский, немецкий, норвежский, польский, португальский, русский, словенский, французский, шведский и

			японский Аудиопараметры • Не менее 3 кардиоидных микрофона • Громкоговоритель - Частота: 100–22 000 Гц - Громкость: не менее 92 дБ на расстоянии 0,5 м при пиковом уровне • Зона уверенной работы микрофона — не менее 6 м (20 футов) • Поддерживаемые кодеки: - G.711 (A-характеристика и μ-характеристика) - G.719 - G.729AB - iLBC (13,33 и 15,2 Кбит/с) - Opus (8–24 Кбит/с) - G.722 - G.722.1, G.722.1C • HD Voice™ • Технология Acoustic Clarity™, обеспечивающая полнодуплексную передачу голоса, подавление эхо и подавление фоновых шумов — совместимость Type 1 (IEEE 1329 полный дуплекс) • Определение наличия голосового сигнала • Генерация комфортного шума • Генерация DTMF-тонов (RFC 2833 и внутриполосная) • Передача звуковых пакетов с малой задержкой • Адаптивные буферы пакетов • Скрытие потери пакетов • Сопряжение устройств по Bluetooth для широкополосной передачи звука и мультимедиа (HFP/AD2P) • Функции распределения вызова • 1 линия (регистрация) • Одновременный вызов на несколько линий/ спаренные линии • Раздельная обработка входящих вызовов/ожидание вызова • Таймер вызова и ожидание вызова • Переадресация, удержание, перенаправление и ответ на вызов • Информация о принятых, набранных вызовах и о подключении других участников • Локальная пятисторонняя голосовая конференцсвязь • Ускоренный набор одним нажатием • Функция «Не беспокоить» • Планы нумерации и звонков с возможностью локальной настройки • Доступ к корпоративному справочнику по протоколу LDAP • Визуальное управление конференциями Сеть и ресурсы • Открытые SIP-платформы и SIP-платформы для Microsoft Lync 2013 и Skype for Business • SDP • Стандарт IETF SIP (RFC 3261 и сопутствующие RFC) • Двухпортовый коммутатор Gigabit Ethernet - 10/100/1000Base-TX через порты LAN и второй порт - Второй порт поддерживает IEEE 802.3af PSE • Сетевая коммутация 802.11 a/b/g/n (Wi-Fi) • Настройка сети: протокол динамической конфигурации хоста (DHCP) и установка параметров вручную • Синхронизация времени и даты по протоколу SNTP • Централизованное (серверное) выделение ресурсов FTP/TFTP/HTTP/HTTPS • Поддержка автоматической настройки Polycom • Поддержка выделения ресурсов и резервных серверов обработки вызовов

			Fi Multimedia) • VLAN — CDP, DHCP VLAN обнаружение • LLDP-MED для обнаружения VLAN Обеспечение безопасности • Аутентификация 802.1X и протокол EAPOL • Шифрование носителей данных по протоколу SRTP • Безопасность на транспортном уровне (TLS) • Шифрование файлов конфигурации • Дайджест-аутентификация • Проверка пароля при входе • Поддержка синтаксиса URL с паролем для адреса сервера загрузки • Защищенная процедура настройки с использованием HTTPS • Поддержка подписанных исполняемых файлов • Шифрование Wi-Fi: WEP, WPA-Personal, WPA2-Personal, WPA2-Enterprise с 802.1X (EAP-TLS, PEAP-MSCHAPv2) Питание • LAN IN: Встроенное обнаружение IEEE 802.3at. Устройство PoE (класс 4)1 . Обратная совместимость с IEEE 802.3af. • LAN OUT: Оборудование для источника питания со встроенным обнаружением IEEE 802.3af1 Разрешения • MIC/VCCI Class B (Япония) • FCC, Часть 15 (CFR 47) Class B • ICES-003 Class B • EN55022 Class B • CISPR22 Class B • VCCI Class B • EN55024 • EN61000-3-2; EN61000-3-3 • Telepermit (Новая Зеландия) • A&C Tick (Австралия) • Соответствие требованиям Директивы RoHS • 19471-0715 Радиосвязь • США - FCC, Часть 15.247 - FCC, Часть 15.407 - FCC, Часть 15.225 • Канада - RSS 247 выпуск 1 • Европейский союз - ETSI EN 300 328 версия 1.9.1 - ETSI EN 301 893 версия 1.7.1 - ETSI EN 300 330 - ETSI EN 301 489-3 - ETSI EN 301 489-17 • Япония - Статья 19 (Япония) - Статья 19-3 (Япония) - Статья 19-3-2 (Япония) • Австралия - AS/NZ4268 WiFi • 2,4 ГГц 18,52 дБм – 5 ГГц 20,68 дБм - 2400 МГц – 2483,5 МГц - 5150 МГц – 5250 МГц - 5250 МГц – 5350 Мгц - 5470 МГц – 5725 Мгц - 5725 МГц – 5825 Мгц • Bluetooth – 7,15 дБм - 2400 МГц – 2483,5 МГц • NFC –12,7 дБмкА/м - 13,56 МГц Безопасность • UL 60950-1 • CE Mark • CAN/CSA-C22.2 No. 60950-1-03 **Комплектность** • Телефонная консоль • Сетевой кабель CAT 5e 7,6 м (25 футов) • Кабель USB 2.0 2 м (6,5 футов) • Кабельная стяжка • Сенсорная накладка для большей доступности • Инструкции по настройке Дополнительное оборудование • Дополнительные микрофоны того же производителя, что и телефонная консоль • В комплект питания входит расширяемый одно портовый гигабитный инжектор, соответствующий требованиям 802.3at типа 2, локальный кабель питания и сетевой кабель (7200-23490-xxx) • Компонент + для презентации контента и видео (2200-13339-xxx) Гарантия • не менее 1 год Размеры телефона (Д x Ш x В) • не более 40 x 8 x 35 см • Вес устройства: не более 1 кг PoE Skype for Business/Microsoft Lync edition 1. Требуется полный вход источника питания класса 4 для операций LAN IN **Дополнительно** • Гарантийный срок – не менее 1 года • В стоимость входит – Настройка, установка, тестирование оборудования • Инструкция по установке

4	Лицензия	на программный продукт (кроме услуг по предоставлению лицензии)	**Создание, редактирование и работа с файлами PDF** • Просмотр и работа со всеми типами контента в файлах PDF • Создание файлов PDF из любых приложений, поддерживающих функцию печати • Объединение нескольких документов в один файл PDF в браузере • Перетаскивание документов и страниц для просмотра и упорядочения перед объединением в один файл PDF • Создание защищенных файлов PDF с ограниченными возможностями копирования и редактирования в Microsoft Word • Редактирование документов PDF • Экспорт файлов PDF в форматы Microsoft Office в браузере или на мобильном устройстве • Интуитивно понятное редактирование файлов PDF, перекомпоновка абзацев путем перетаскивания • Поиск и перенос текста одним щелчком мыши • Сбор электронных подписей и отслеживание полученных подписей в реальном времени • Создание файлов PDF, отвечающих требованиям WCAG 2.0 и PDF/UA к расширенному доступу, и проверка имеющихся документов на соответствие этим стандартам • Срок использования: бессрочное
5	Картридж тонерный	черный	• 101R00432 Xerox Принт-картридж • Картриджи должны быть новыми и изготовлены производителем печатной техники. Дата изготовления картриджа -- не ранее 2017 года. • Не допускается поставка не оригинальных картриджей, либо произведенных путем перезаправки, восстановления или модификации. • Поставка должна быть в оригинальной упаковке фирмы производителя, производственный код на упаковке должен совпадать с кодом указанным в технической спецификации, а так же на самом картридже. • Прием картриджей будет осуществляться после проведения экспертизы представителем авторизованного сервис провайдера на предмет соответствия требованиям технической спецификации. • Картриджи не соответствующие технической спецификации приниматься не будут. • Гарантийный срок – не менее 1 года • Дата изготовления – не ранее 2017 года
6	Кабель-канал	пластиковый	• Гибкий напольные кабель-каналы • Прочный • Большая гибкость • Возможность отрегулировать длину по мере необходимости с помощью ножниц или ножа • Длина – не менее 3 метра • Ширина - не менее 100 мм • Высота – не более 20 мм • Форма – дуга образный • Объём – не менее 4 кабеля • Цвет - серый
7	Органайзер	кабельный, размер 1U, 19", горизонтальный, металлический	• органайзер кабельный настольный для ПК • гибкий • длина – не менее 1 м

			• Возможность отрегулировать длину по мере необходимости с помощью ножниц или ножа • Цвет – черный • Объём – не менее 4 кабеля