Приложение 1 к извещению

***Описание объекта закупки***

**Наименование предмета контракта:** Продление лицензии на использование антивирусного программного обеспечения Касперский (Лицензия Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 1000-1499 Node 1 year Renewal License).

Код КТРУ: 58.29.50.000-00000001 Услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение. Единицы измерения (количество товара, объем работы, услуги по ОКЕИ – штука). Обязательно 01.01.2025**.**Не используется.

ОКПД 2: 58.29.50.000 «Услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение»

Цель 2 задача 14 мероприятие 14.1 Оказание услуг (выполнение работ) учреждениями в сфере занятости населения и охраны труда (Постановление Правительства СО от 21.10.2013 №1272-ПП «Об утверждении государственной программы Свердловской области «Содействие занятости населения СО»).

**Приказ 189** от 21.06.2016 **«**Об утверждении нормативных затрат на обеспечение функций Департамента по труду и занятости населения Свердловской области и подведомственных ему государственных казённых учреждений службы занятости населения Свердловской области**»:** пункт 19, глава 3, раздел 1, часть II.

**Приказ 155** от 21.05.2018 **«**Об утверждении требований к отдельным видам товаров, работ, услуг (в том числе предельных цен товаров, работ, услуг), закупаемым Департаментом по труду и занятости населения Свердловской области и подведомственными ему государственными казёнными учреждениями службы занятости населения Свердловской области»: отсутствует данная закупка.

**Место оказания:** Свердловская обл., г. Екатеринбург, ул. 8 Марта, д. 12.

**Сроки (периоды) оказания услуг:** в течение 10 (Десяти) рабочих дней с даты заключения контракта (ч. 5 ст. 51 Закона о контрактной системе). Срок, на который передаются права на использование ПО, определяется в соответствии с Лицензионным соглашением на право использования и составляет 1 (Один) год с 06.01.2025 г.

**Срок действия контракта**: контракт считается заключенным и вступает в силу с даты заключения (ч. 5 ст. 51 Закона о контрактной системе) и действует по 13.09.2024 г. (включительно).

**Техническое задание**

**на продление неисключительных прав на программы для ЭВМ Лицензия Kaspersky Endpoint Security для бизнеса Расширенный Russian Edition на 1 год**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Кол-во** |
| 1 | Лицензия Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 1000-1499 Node 1 year Renewal License \* | 230 |

***\*эквивалент недопустим в связи с необходимостью обеспечения совместимости с использующимся у Заказчика программным обеспечением.***

Требуется продление установленного у Заказчика программного обеспечения на 1 (один) год:

Название ПО (продукта): Лицензия Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 1000-1499 Node 1 year Renewal License

Количество объектов:230 Users

Срок окончания текущей лицензии на ПО: до 2025-01-05

**№ имеющейся у заказчика лицензии (подлежащей продлению): 2B1E-230728-122008-5-10114.**

Указанное программное обеспечение зарегистрировано в Едином реестре российских программ для электронных вычислительных машин и баз данных в соответствии с Постановлением Правительства РФ от 16.11.2015 г. № 1236:

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование в реестре** | **Рег. номер ПО** | **Производитель, страна происхождения** | **Ссылка на реестр** |
| Kaspersky Endpoint Security для бизнеса Расширенный | 207 | АО «Лаборатория Касперского», Российская Федерация | https://reestr.digital.gov.ru/reestr/301482/  |

**Технические требования к системе антивирусной защиты**

# **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 и серверов Linux;

- программные средства антивирусной защиты для файловых 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 и английском языке.

Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.

# **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).

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

* + антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
	+ антивирусное сканирование 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, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
	+ антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
	+ защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
	+ фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
	+ проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c 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;
	+ защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
	+ защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
	+ контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
	+ создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или 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, 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;
	+ управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
	+ записи в журнал событий о записи и/или удалении файлов на съемных дисках;
	+ назначение приоритета для правил доступа к устройствам с файловой системой;
	+ контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории 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;
	+ защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
	+ управления параметрами Kaspersky Endpoint Security через доверенные программы удаленного администрирования;
	+ установки только выбранных компонентов программного средства антивирусной защиты;
	+ централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
	+ запуска задач по расписанию и/или сразу после запуска приложения;
	+ 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;
	+ проверки целостности антивирусной программы;
	+ добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
	+ импорта и экспорта списков правил и исключений в XML-формат;
	+ наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
	+ наличие защищенного хранилища для отчетов о работе антивируса;
	+ включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
	+ интеграции с Windows Defender Security Center;
	+ наличие поддержки Antimalware Scan Interface (AMSI);
	+ наличие поддержки Windows Subsystem for Linux (WSL);
	+ защитить паролем восстановление объектов из резервного хранилища;
	+ ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
	+ запуск специальной задачи для обнаружения и закрытия 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, поддержка UEFI-систем;
	+ 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 за пределами организации с помощью пароля;
	+ шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;
	+ формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий).

**Требования к программным средствам антивирусной защиты для серверов Windows**

Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий:

- 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) (с ограничениями);

- Windows Server 2019 (64-разрядная) (с ограничениями).

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

* антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование 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;
* 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;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* 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;
* проверки целостности антивирусной программы;
* добавления исключений из антивирусной проверки по контрольной 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;
* включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
* интеграции с Windows Defender Security Center;
* наличие поддержки Antimalware Scan Interface (AMSI);
* наличие поддержки Windows Subsystem for Linux (WSL);
* защитить паролем восстановление объектов из резервного хранилища.
* импорта и экспорта списков правил и исключений в XML-формат;
* ограничения сетевого трафика в том случае, если подключение к интернету является лимитным
* 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, 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;
* формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);
* запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.

**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 10.13, 10.14, 10.15 или 11.0;

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

* 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;
* проверку сетевого трафика, передаваемого через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик);
* контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем
* 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.
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault.

**Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux**

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 32-битных операционных систем следующих версий:

- Ubuntu 16.04 LTS и выше.

- Red Hat Enterprise Linux 6.7 и выше.

- CentOS 6.7 и выше.

- Debian GNU / Linux 9.4 и выше.

- Debian GNU / Linux 10.

- Linux Mint 18.2 и выше.

- Linux Mint 19 и выше.

- Альт 8 СП Рабочая Станция.

- Альт 8 СП Сервер.

- Альт Рабочая Станция 8.

- Альт Рабочая Станция К 8.

- Альт Сервер 8.

- Альт Образование 8.

- Альт Сервер 9.

- Альт Рабочая Станция 9.

- Альт Образование 9.

- Гослинукс 6.6.

- Mageia 4.

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий:

- Ubuntu 16.04 LTS и выше.

- Ubuntu 18.04 LTS и выше.

- Red Hat Enterprise Linux 6.7 и выше.

- Red Hat Enterprise Linux 7.2 и выше.

- Red Hat Enterprise Linux 8.0 и выше.

- CentOS 6.7 и выше.

- CentOS 7.2 и выше.

- CentOS 8.0 и выше.

- Debian GNU / Linux 9.4 и выше.

- Debian GNU / Linux 10.1 и выше.

- Oracle Linux 6,7 и выше.

- Oracle Linux 7,3 и выше.

- Oracle Linux 8 и выше.

- SUSE Linux Enterprise Server 12 SP3 и выше.

- SUSE Linux Enterprise Server 15 и выше.

- openSUSE Leap 15 и выше.

- Альт 8 СП Рабочая Станция.

- Альт 8 СП Сервер.

- Альт Рабочая Станция 8.

- Альт Рабочая Станция К 8.

- Альт Сервер 8.

- Альт Образование 8.

- Альт Рабочая Станция 9.

- Альт Сервер 9.

- Альт Образование 9.

- Amazon Linux 2.

- Linux Mint 18.2 и выше.

- Linux Mint 19 и выше.

- Astra Linux Special Edition, версия 1.5 (стандартное ядро и ядро PaX).

- Astra Linux Special Edition, версия 1.6 (стандартное ядро и ядро PaX).

- Astra Linux Common Edition, версия 2.12.

- ОС РОСА "КОБАЛЬТ" 7.3 для клиентских систем.

- ОС РОСА "КОБАЛЬТ" 7.3 для серверных систем.

- Гослинукс 6.6.

- Гослинукс 7.2.

- AlterOS 7.5 и выше.

- Pardus OS 19.1.

- RED OS 7.2.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

* 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;
* возможность проверки памяти ядра;
* 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;
* включения опции блокирования файлов во время проверки;
* помещение подозрительных и поврежденных объектов на карантин;
* 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;
* 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;
* управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;
* управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;
* проверки съемных дисков;
* отслеживания во входящем сетевом трафике активности, характерной для сетевых атак
* проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым
* получения данных о действиях программ на компьютере пользователя;
* проверки памяти ядра.

**Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных 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 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 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 SP2 или выше;

- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

- Microsoft Small Business Server 2008 Standard / Premium SP2 или выше;

- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;

- Windows Server 2008 R2 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 SP1 или выше;

- Microsoft Windows MultiPoint Server 2011 Standard / Premium;

- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;

- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;

- Microsoft 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;

- Windows 10 Enterprise multi-session.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

* 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;
* проверки контейнеров Microsoft Windows;
* защиты от эксплуатирования уязвимостей в памяти процессов;
* должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
* добавлять процессы в список защищаемых;
* 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;
* 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;
* интеграции с SIEM системами;
* указания количества рабочих процессов антивируса вручную;
* 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;
* защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;
* контроль устройств, в том числе сетевых карт и модемов;
* веб-контроль
* защита от почтовых угроз (плагин для Outlook)
* 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;
* 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);
* создания специальных правил должно контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме;
* создания специальных правил должно работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должно 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;
* наличие механизмов автоматической генерации правил для контроля устройств и приложений;

**Требования к программным средствам антивирусной защиты мобильных устройств**

Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС:

- Android 4.2-11.0.

- iOS 10.0-14.0 или iPadOS.

В программном средстве антивирусной защиты смартфонов для ОС Android должны быть реализованы следующие функциональные возможности:

* постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;
* проверка файловой системы устройства по требованию и по расписанию;
* мгновенная проверка устанавливаемых приложений
* блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* 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, в рамках контроля запуска приложений;
* отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM);
* заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
* указать параметры подключения к wi-fi сетям;
* указать обязательные к установке приложения;
* блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);
* создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;
* поддержка технологий Samsung KNOX1 и KNOX2.

В программном средстве защиты смартфонов для ОС Apple iOS должны быть реализованы следующие функциональные возможности:

* удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;
* отправки команды блокирования и удаления данных;
* 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, при использовании supervised mode;
* централизованного управления с помощью единой консоли управления;
* наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari или Game Center, на управляемом устройстве.

**Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows**

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows 10 20H2 32-разрядная / 64-разрядная;

- Microsoft Windows 10 20H1 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Pro 19H1 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Enterprise 19H1 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Education 19H1 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Pro 19H2 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Enterprise 19H2 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Education 19H2 32-разрядная / 64-разрядная;

- Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная;

- Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная;

- Microsoft Windows 8 Pro 32-разрядная / 64-разрядная;

- Microsoft Windows 8 Enterprise 32-разрядная / 64-разрядная;

- Microsoft Windows 7 Professional Service Pack 1 32-разрядная / 64-разрядная;

- Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32-разрядная / 64-разрядная;

- Windows Server 2019 Standard 64-разрядная;

- Windows Server 2019 Standard 64-разрядная;

- Microsoft Windows Server 2019 Datacenter 64-разрядная;

- Microsoft Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-разрядная;

- Microsoft Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-разрядная;

- Microsoft Windows Server 2016 (вариант установки Server Core RS3 (v1709) (LTSB/CBB) 64-разрядная;

- Microsoft Windows Server 2016 Standard (LTSB) 64-разрядная;

- Microsoft Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;

- Microsoft Windows Server 2016 Datacenter (LTSB) 64-разрядная;

- Microsoft Windows Server 2012 R2 Standard 64-разрядная;

- Microsoft Windows Server 2012 R2 Server Core 64-разрядная;

- Microsoft Windows Server 2012 R2 Foundation 64-разрядная;

- Microsoft Windows Server 2012 R2 Essentials 64-разрядная;

- Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;

- Microsoft Windows Server 2012 Standard 64-разрядная;

- Microsoft Windows Server 2012 Server Core 64-разрядная;

- Microsoft Windows Server 2012 Foundation 64-разрядная;

- Microsoft Windows Server 2012 Essentials 64-разрядная;

- Microsoft Windows Server 2012 Datacenter 64-разрядная;

- Microsoft Windows Storage Server 2016 64-разрядная;

- Microsoft Windows Storage Server 2012 R2 64-разрядная;

- Microsoft Windows Storage Server 2012 64-разрядная;

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

- VMware vSphere 6.7;

- VMware vSphere 7.1;

- VMware Workstation 15 Pro;

- VMware Workstation 16 Pro;

- Microsoft Hyper-V Server 2012 64-разрядная;

- Microsoft Hyper-V Server 2012 R2 64-разрядная;

- Microsoft Hyper-V Server 2016 64-разрядная;

- Microsoft Hyper-V Server 2019 64-разрядная;

- Citrix XenServer 7.1 LTSR;

- Citrix XenServer 8.x;

- Parallels Desktop 16;

- Oracle VM VirtualBox 6.x.

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:

- Microsoft SQL Server 2012 Express 64-разрядная;

- Microsoft SQL Server 2014 Express 64-разрядная;

- Microsoft SQL Server 2016 Express 64-разрядная;

- Microsoft SQL Server 2017 Express 64-разрядная;

- Microsoft SQL Server 2019 Express 64-разрядная;

- Microsoft SQL Server 2014 (все редакции) 64-разрядная;

- Microsoft SQL Server 2016 (все редакции) 64-разрядная;

- Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;

- Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная;

- Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная;

- Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная;

- MySQL Standard Edition 5.7 32-разрядная / 64-разрядная;

- MySQL Enterprise Edition 5.7 32-разрядная / 64-разрядная;

- Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;

- MariaDB Server 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

* выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
* чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
* настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
* 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 работе средств защиты;
* 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;
* указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
* иерархии триггеров, по которым происходит перераспределение;
* 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 прав 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;
* 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;
* отправки SMS-оповещений о заданных событиях;
* централизованная установка сертификатов на управляемые мобильные устройства;
* указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
* 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 по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
* 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 портала самообслуживания пользователей;
* портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
* наличие системы контроля возникновения вирусных эпидемий;
* установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
* интеграции по OpenAPI;
* управления антивирусной защитой с использованием WEB консоли;
* автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
* 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;
* возможность подключения по RDP или штатными средствами из консоли управления;
* пользователю должен выводиться запрос на разрешение дистанционного подключения;
* 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, установленного на компьютере 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;
* поддержка функциональности управления шифрованием данных;
* возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF
* двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;
* использования дополнительной аутентификация после изменения параметров учетной записи пользователя.

**Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux**

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Ubuntu 18.04 LTS;

- Ubuntu 20.04 LTS;

- Debian GNU / Linux 10.5;

- Astra Linux Common Edition, версия 2.12;

- Astra Linux Special Edition, версия 1.6;

- CentOS 7.9.2009;

- CentOS 8.3.2011;

- Red Hat Enterprise Linux 7.9;

- Red Hat Enterprise Linux 8.3;

- ALT 8.3;

- ALT 9.1.

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

- FusionCompute 8.0;

- FusionSphere OpenStack 6.5.13.

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: MariaDB Server 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB.

Kaspersky Security Center 13 Linux предназначен для развертывания и управления защитой устройств с операционной системой Linux с помощью Сервера администрирования на базе Linux в соответствии с требованиями чистых сред Linux®.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* иерархии триггеров, по которым происходит перераспределение;
* 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 прав 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;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ;
* 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;
* наличие системы контроля возникновения вирусных эпидемий;
* управления антивирусной защитой с использованием WEB консоли.

**Требования к обновлению антивирусных баз**

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

* + создания правил обновления 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 электронной почте и через Интернет.

- Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.

**Требования к надежности и гарантийным обязательствам**

Исполнитель гарантирует оказание услуг в соответствии с законодательством Российской Федерации, требованиями иных нормативных правовых актов, регулирующих порядок предоставления такого вида услуг, устанавливающих требования к качеству такого вида услуг, в соответствии с условиями Контракта. Исполнитель подтверждает, что он действует в пределах прав и полномочий, позволяющих ему осуществлять операции по Контракту.

Программное обеспечение, электронные носители информации и т.п., используемые Исполнителем при оказании услуг, не должны содержать вредоносных программ и должны быть совместимы с системами и оборудованием Заказчика.

Исполнитель, в соответствии со ст. 727 Гражданского кодекса Российской Федерации (часть вторая) от 26.01.1996 №14-ФЗ, обеспечивает конфиденциальность полученной информации. Сведения любого характера (производственные, технические, организационные) в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) не передаются Исполнителям третьим лицам.

Права на использование ПО предоставляются Заказчику путем передачи ему:

- регистрационной информации в виде ключевого файла/авторизационного номера/кода активации, которая генерируется Правообладателем персонально для Заказчика и необходима для полнофункциональной работоспособности ПО, которая направляется на адрес электронной почты, указанный Заказчиком;

- Лицензионного соглашения между Правообладателем и Заказчиком на бумажном носителе (высылается по договоренности Сторон по почте, либо посредством курьерской доставки в адрес Заказчика), и/или в электронном виде (направляется на адрес электронной почты, указанный Заказчиком, и/или прикрепляется в виде файла к документу о приемки, сформированного с помощью ЕИС).

**Требования к патентной чистоте**

В процессе сопровождения Системы должны соблюдаться положения законодательных актов Российской Федерации по соблюдению авторских прав и защите специальных знаков. При установке Системы должны быть выполнены требования части четвертой Гражданского Кодекса Российской Федерации, а также международные патентные соглашения.

**Требования к соблюдению авторских прав**

На основании статей 1229, 1233, 1234, 1262 Гражданского кодекса Российской Федерации от Исполнителя требуется наличие прав на предлагаемое программное обеспечение (в том числе на доработку и внесение изменений (при необходимости) в исходный код) - свидетельство о государственной регистрации программы (в случае если Исполнитель является правообладателем указанной программы), либо лицензионный (сублицензионный) или иной договор либо документ, подтверждающий наличие у Исполнителя прав в отношении программного обеспечения (в случае если Исполнитель не является правообладателем указанной программы).

Исполнитель после заключения государственного контракта обязан подтвердить наличие у него свидетельства о государственной регистрации программы (в случае если является правообладателем указанной программы), либо лицензионного (сублицензионного) или иного договора либо документа, подтверждающий наличие прав в отношении программного обеспечения (в случае если не является правообладателем указанной программы). Не предоставление вышеуказанных документов (копий) является основанием для расторжения Контракта.

**Условия оплаты (срок, документы):** Расчеты между Заказчиком и Исполнителем производятся единовременным платежом не позднее 7 (Семи) рабочих дней с даты подписания Заказчиком документа о приемке с приложением (*приложение* *при необходимости*), с использованием единой информационной системы, на основании счета, счета-фактуры (*при необходимости*) при условии отсутствия у Заказчика претензий к Услуге и комплекту документов (информации), передаваемых после продления права использования лицензионной программы Исполнителем. Сбор и предоставление всех необходимых для оплаты сопроводительных документов (информации) осуществляет Исполнитель. Аванс не предусмотрен.