УТВЕРЖДАЮ:

Директор ООО «УК «Зеленая роща»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А.С. Муромский

(подпись)

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025 г.

**ИЗВЕЩЕНИЕ**

**О ЗАПРОСЕ КОТИРОВОК В ЭЛЕКТРОННОЙ ФОРМЕ**

на право заключения договора  
на оказание услуг по передаче неисключительных лицензионных прав на использование антивирусной защиты Kaspersky endopoint security для бизнеса расширенный (продление лицензии)

Согласовали:

|  |  |  |  |
| --- | --- | --- | --- |
| должность | подпись | Ф.И.О. | дата |
| Первый заместитель директора |  | С.В. Мартюхин |  |
| Заместитель директора |  | А.Н. Семёнов |  |
| Начальник юридического отдела |  | О.В. Сидорова |  |
| Главный бухгалтер |  | Е.А. Плыгунова |  |
| Начальник планово-экономического отдела |  | Е.В. Баюшкина |  |
| Главный инженер |  | Р.В. Субботин |  |
| Начальник IT-отдела |  | О.С. Коптев |  |

**г. Орел-2025**

**Часть** **I. Информационная карта**

|  |  |  |
| --- | --- | --- |
| 1 | Наименование, место нахождения, почтовый адрес, адрес электронной почты, номер контактного телефона заказчика | **Заказчик:** Общество с ограниченной ответственностью «Управляющая компания «Зеленая роща»  **Место нахождения, почтовый адрес заказчика:** 302040 г. Орел, ул. Ломоносова, дом 6, помещение 31, этаж 4  **Контактное лицо:** начальник ПЭО ООО «УК «Зеленая роща» Баюшкина Е.В.  **Электронная почта:** zakupki@greenpark57.ru **Контактный телефон:** 8(910)-748-10-04 (доб. 711) |
| 2 | Способ закупки | Запрос котировок в электронной форме. Победителем признается соответствующий требованиям Извещения о закупке Участник запроса котировок, предложивший наиболее низкую цену Договора. |
| 3 | Предмет (наименование) закупки | Оказание услуг по передаче неисключительных лицензионных прав на использование антивирусной защиты Kaspersky endopoint security для бизнеса расширенный (продление лицензии) |
| 4 | Сведения о начальной (максимальной) цене договора Н(М)ЦД (предельной цене поставки/работ/ услуг в случае ее установления в проекте договора), порядок формирования Н(М)ЦД | **236 890,45 (двести тридцать шесть тысяч восемьсот девяносто) руб. 45 копеек**Цена договора должна включать стоимость оказываемых услуг, все налоги и сборы, а также все подлежащие уплате налоги, сборы и другие обязательные платежи, за исключением стоимости материалов, предоставленных Заказчиком, а также все расходы и риски Исполнителя, возникающие в связи с исполнением Договора.Стоимость поставки товара указывается цифрами и прописью, в случае разночтения преимущество имеет цена, указанная прописью.Расчет начальной (максимальной) цены произведен методом сопоставимых рыночных цен (анализ рынка). Приведен в Разделе IV «Обоснование начальной (максимальной) цены договора» Извещения |
| 5 | Адрес электронной площадки в информационно-телекоммуникационной сети Интернет (при осуществлении закупки в электронной форме) | Электронная торговая площадка Электронный торги России https://torgi82.ru/ |
| 6 | Предмет договора с указанием количества поставляемого товара, объема выполняемой работы, оказываемой услуги, а также краткое описание предмета закупки в соответствии с [ч. 6.1 ст. 3](https://login.consultant.ru/link/?req=doc;base=RZR;n=287303;fld=134;dst=199) Закона N 223-ФЗ (при необходимости)количество поставляемого товара | В соответствии с проектом договора и техническим заданием |
| 7 | ОКПД2  ОКВЭД2 | 58.29.50.00058.29 |
| 8 | Место, условия  и сроки поставки товара (оказания услуги): | в соответствии с проектом договора |
| 9 | Функциональные характеристики (потребительские свойства), технические и качественные характеристики, а также эксплуатационные характеристики предмета закупки | указаны в Технической части к Извещению об осуществлении процедуры закупки, Приложение 2 к проекту Договору. |
| 10 | Место, срок и порядок предоставления информации о закупке, размер, порядок и сроки внесения платы, взимаемой заказчиком за предоставление документации | Информация о закупке и сопутствующая документация доступна для ознакомления и скачивания бесплатно на официальном сайте единой информационной системы (далее-ЕИС) в сфере закупок (http://zakupki.gov.ru) или на сайте оператора Электронной торговой площадки Электронный торги России https://torgi82.ru/ со дня ее размещения и до окончания срока подачи заявок на участие в закупке. |
| 11 | Дата начала срока приема заявок, порядок и место подачи заявок на участие | « » \_\_\_ 2025 г  Электронная торговая площадка Электронный торги России https://torgi82.ru/ |
| 12 | Размер и порядок предоставления обеспечения заявки | Не установлено. |
| 13 | Дата и время окончания срока подачи заявок на участие в процедуре закупки | « » \_\_\_\_ 2025 г  После окончания срока подачи заявок на участие в процедуре закупки Оператор электронной торговой площадки направляет Заказчику поступившие заявки.  В случае принятия решения Заказчиком о внесении изменений в извещение о проведении запроса котировок, размещаются Заказчиком на электронной площадке и в ЕИС не позднее трех дней со дня принятия решения об изменениях.  В результате внесения указанных изменений срок подачи заявок на участие в запросе котировок продлевается таким образом, чтобы до даты окончания срока подачи заявок на участие в закупке оставалось не менее половины срока подачи заявок на участие в конкурентной закупке, установленного в настоящей карте. |
| 14 | Порядок, дата и время окончания срока предоставления участникам закупки разъяснений положений извещения и всей информации (документации) о закупке | Дата и время окончания срока предоставления участникам закупки разъяснений положений извещения и (или) документации о закупке:  « » \_\_\_\_\_ 2025 г  Любой участник закупки вправе направить запрос на предоставление разъяснений положений извещения о проведении закупки. Запрос на предоставление разъяснений подается посредством функционала электронной площадки.  Запрос на предоставление разъяснений положений извещения о проведении закупки подается в произвольной форме.  Заказчик предоставляет разъяснение положений извещения о проведении закупки в течение 3 (трех) рабочих дней при условии, что запрос на разъяснение поступил не позднее чем за 3 (три) рабочих дня до даты окончания срока подачи заявок на участие в закупке. Если запрос был направлен в нарушение данных сроков, заказчик имеет право не давать разъяснения по такому запросу.  Разъяснения размещаются в ЕИС без указания участника закупки, от которого поступил запрос на разъяснение. |
| 15 | Место, дата и время рассмотрения и оценки заявок на участие в закупке: | Место рассмотрения и оценки заявок на участие в запросе котировок в электронной форме:  302040 г. Орел, ул. Ломоносова, дом 6, помещение 31, этаж 4  Дата рассмотрения и оценки заявок:  « » \_\_\_\_ 2025 г |
| 16 | Место, дата и время подведения итогов закупки: | Не позднее « » \_\_\_\_ 2025 г  по адресу: 302040 г. Орел, ул. Ломоносова, дом 6, помещение 31, этаж 4  В ходе подведения итогов осуществляется оценка заявок путем сравнения предложений участников запроса котировок в электронной форме о цене договора и их ранжирования по степени предпочтительности в порядке возрастания.  Заявке на участие в закупке, в которой содержится предложение о наименьшей цене договора, присваивается первый номер. Участник закупки, подавший заявку, которой по результатам оценки заявок присвоен первый номер, является победителем запроса котировок.  В случае если в нескольких заявках содержатся одинаковые предложения о цене договора, меньший порядковый номер присваивается заявке, которая поступила ранее других, содержащих такие же предложения. |
| 17 | Требования к участникам закупки | Обязательные требования к участникам закупки:  1) соответствие требованиям, устанавливаемым в соответствии с законодательством Российской Федерации и настоящим Положением, к лицам, осуществляющим поставки товаров, выполнение работ, оказание услуг, являющихся предметом закупки;  2) участник закупки - юридическое лицо не находится в процессе ликвидации;  3) в отношении участника закупки - юридического лица или индивидуального предпринимателя не выносилось судебных решений о признании несостоятельным (банкротом) и об открытии конкурсного производства;  4) неприостановление деятельности участника закупки в порядке, предусмотренном Кодексом Российской Федерации об административных правонарушениях, на дату подачи заявки на участие в закупке;  5) отсутствие у участника закупки недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации за прошедший календарный год, размер которых превышает двадцать пять процентов балансовой стоимости активов участника закупки, по данным бухгалтерской отчетности за последний отчетный период. Данное требование не распространяется на суммы, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной или которые признаны безнадежными к взысканию в соответствии с законодательством Российской Федерации о налогах и сборах);  6) отсутствие у участника закупки - физического лица либо у руководителя, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа, или главного бухгалтера юридического лица - участника закупки судимости за преступления в сфере экономики и (или) преступления, предусмотренные статьями 289, 290, 291, 291.1 Уголовного кодекса Российской Федерации (за исключением лиц, у которых такая судимость погашена или снята), а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся объектом осуществляемой закупки, и административного наказания в виде дисквалификации;  7) непривлечение участника закупки - юридического лица в течение двух лет до момента подачи заявки на участие в закупке к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях;  8) отсутствие сведений об участнике закупки в реестре недобросовестных поставщиков, предусмотренном статьей 5 Федерального закона от 18.07.2011 г. N 223-ФЗ;  9) отсутствие сведений об участнике закупки в реестре недобросовестных поставщиков, предусмотренном Федеральным законом от 5 апреля 2013 года N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд";  10) отсутствие между участником закупки и Заказчиком конфликта интересов;  11) участник закупки не является офшорной компанией;  12) отсутствие у участника закупки ограничений для участия в закупках, установленных законодательством Российской Федерации.  Требования, предъявляемые к участникам закупки, закупаемым товарам, работам, услугам, условиям исполнения договора, а также критерии и порядок оценки и сопоставления заявок на участие в закупке применяются в равной степени в отношении всех участников закупки.  13) Участником закупки является любое юридическое лицо или несколько юридических лиц, выступающих на стороне одного участника закупки, независимо от организационно-правовой формы, формы собственности, места нахождения и места происхождения капитала, **за исключением юридического лица, являющегося иностранным агентом в соответствии с Федеральным** [**законом**](consultantplus://offline/ref=17C7BCAE0E9E6D9CE8FFD8A446707473486FFC58A7424E2305574AD25FA5B2642D62CDAAB06A0CCC66429C1376A0F7H) **от 14 июля 2022 года N 255-ФЗ** "О контроле за деятельностью лиц, находящихся под иностранным влиянием", либо любое физическое лицо или несколько физических лиц, выступающих на стороне одного участника закупки, в том числе индивидуальный предприниматель или несколько индивидуальных предпринимателей, выступающих на стороне одного участника закупки, **за исключением физического лица, являющегося иностранным агентом в соответствии с Федеральным** [**законом**](consultantplus://offline/ref=17C7BCAE0E9E6D9CE8FFD8A446707473486FFC58A7424E2305574AD25FA5B2642D62CDAAB06A0CCC66429C1376A0F7H) **от 14 июля 2022 года N 255-ФЗ** "О контроле за деятельностью лиц, находящихся под иностранным влиянием". |
| 18 | Требования к содержанию, форме, оформлению и составу заявки на участие в закупке. | Заявка на участие в закупке может быть подана только в электронной форме посредством функционала электронной площадки.  Участник вправе подать только одну заявку на участие в процедуре закупки в любое время с момента размещения Извещения о ее проведении до даты и времени окончания срока подачи заявок. Участник вправе изменить или отозвать поданную заявку. Изменение или отзыв заявки после окончания срока подачи заявок невозможен.  Порядок отзыва и изменения заявки осуществляется посредством функционала электронной площадки и в соответствии с регламентом электронной площадки, на которой проводится закупка.  Заявка на участие в закупке подается по форме и оформленная согласно образцу заявки (Часть II «**Образцы форм и документов для заполнения участниками закупки»** настоящего извещения о закупке). В заявке участнику необходимо указать информацию, предусмотренную пунктами 31, 32, 33 настоящей Информационной карты/ Извещения (если данными пунктами такое требование установлено).  Заявка на участие в закупке должна содержать:  1) документ, содержащий сведения об участнике закупок, подавшем заявку: ИНН/КПП/ОГРН, фирменное наименование (полное наименование), организационно-правовую форму, место нахождения, почтовый адрес (для юридического лица), фамилию, имя, отчество, ИНН/ОГРНИП (при наличии), паспортные данные, место жительства (для физического лица), номер контактного телефона;  2) копии учредительных документов участника закупок (для юридических лиц);  3) копии документов, удостоверяющих личность (для физических лиц);  4) выписку из Единого государственного реестра юридических лиц (для юридических лиц) либо Единого государственного реестра индивидуальных предпринимателей (для индивидуальных предпринимателей), полученную не ранее чем за месяц до дня размещения в ЕИС извещения о проведении запроса котировок, или нотариально заверенную копию такой выписки;  5) надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица или индивидуального предпринимателя согласно законодательству соответствующего государства (для иностранных лиц). Эти документы должны быть получены не ранее чем за шесть месяцев до дня размещения в ЕИС извещения о проведении запроса котировок;  6) документ, подтверждающий полномочия лица осуществлять действия от имени участника закупок - юридического лица (копия решения о назначении или об избрании физического лица на должность, в соответствии с которым это физическое лицо обладает правом действовать от имени участника без доверенности). Если от имени участника запроса котировок действует иное лицо, заявка должна включать и доверенность на осуществление действий от имени участника закупок, заверенную печатью участника закупок (при наличии) и подписанную от его имени лицом (лицами), которому в соответствии с законодательством РФ, учредительными документами предоставлено право подписи доверенностей (для юридических лиц), либо нотариально заверенную копию такой доверенности;  7) решение об одобрении или о совершении крупной сделки (его копию), если требование о необходимости такого решения для совершения крупной сделки установлено законодательством РФ, учредительными документами юридического лица и если для участника закупок поставка товаров, выполнение работ, оказание услуг, выступающих предметом договора, предоставление обеспечения исполнения договора являются крупной сделкой. Если указанные действия не считаются для участника закупки крупной сделкой, представляется соответствующее письмо;  8) документ, декларирующий следующее:  - соответствие требованиям, устанавливаемым в соответствии с законодательством Российской Федерации и настоящим Положением, к лицам, осуществляющим поставки товаров, выполнение работ, оказание услуг, являющихся предметом закупки;  - участник закупки - юридическое лицо не находится в процессе ликвидации;  - в отношении участника закупки - юридического лица или индивидуального предпринимателя не выносилось судебных решений о признании несостоятельным (банкротом) и об открытии конкурсного производства;  - неприостановление деятельности участника закупки в порядке, предусмотренном Кодексом Российской Федерации об административных правонарушениях, на дату подачи заявки на участие в закупке;  - отсутствие у участника закупки недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации за прошедший календарный год, размер которых превышает двадцать пять процентов балансовой стоимости активов участника закупки, по данным бухгалтерской отчетности за последний отчетный период. Данное требование не распространяется на суммы, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной или которые признаны безнадежными к взысканию в соответствии с законодательством Российской Федерации о налогах и сборах);  - отсутствие у участника закупки - физического лица либо у руководителя, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа, или главного бухгалтера юридического лица - участника закупки судимости за преступления в сфере экономики и (или) преступления, предусмотренные статьями 289, 290, 291, 291.1 Уголовного кодекса Российской Федерации (за исключением лиц, у которых такая судимость погашена или снята), а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся объектом осуществляемой закупки, и административного наказания в виде дисквалификации;  - непривлечение участника закупки - юридического лица в течение двух лет до момента подачи заявки на участие в закупке к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях;  - отсутствие сведений об участнике закупки в реестре недобросовестных поставщиков, предусмотренном статьей 5 Федерального закона от 18.07.2011 г. N 223-ФЗ;  9) отсутствие сведений об участнике закупки в реестре недобросовестных поставщиков, предусмотренном Федеральным законом от 5 апреля 2013 года N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд";  - отсутствие между участником закупки и Заказчиком конфликта интересов;  - участник закупки не является офшорной компанией;  - отсутствие у участника закупки ограничений для участия в закупках, установленных законодательством Российской Федерации.  9) предложение о цене договора;  10) документы (их копии), подтверждающие соответствие участника запроса котировок требованиям законодательства РФ и извещения о проведении запроса котировок к лицам, которые осуществляют поставки товаров, выполнение работ, оказание услуг;  11) документы (их копии), подтверждающие соответствие товаров, работ, услуг требованиям законодательства РФ к таким товарам, работам, услугам, если законодательством РФ установлены требования к ним и, если представление указанных документов предусмотрено извещением о проведении запроса котировок. Исключение составляют документы, которые, согласно гражданскому законодательству, могут быть представлены только вместе с товаром;  12) обязательство участника запроса котировок представить до момента заключения договора сведения о цепочке собственников, включая бенефициаров (в том числе конечных), и документы, подтверждающие эти сведения, если требование о предоставлении таких сведений было установлено в извещении о проведении запроса котировок;  13) согласие на поставку товаров, выполнение работ, оказание услуг в соответствии с условиями, установленными извещением о проведении запроса котировок:  1-1) при размещении закупки на поставку товара:  а) согласие участника процедуры закупки на поставку товара в случае:  - если участник процедуры закупки предлагает для поставки товар, указание на товарный знак которого содержится в документации о закупке или указание на товарный знак предлагаемого для поставки товара и конкретные показатели этого товара, соответствующие значениям эквивалентности, установленным документацией о закупке;  - если участник процедуры закупки предлагает для поставки товар, который является эквивалентным товару, указанному в документации о закупке, при условии содержания в документации о закупке указания на товарный знак, а также требования о необходимости указания в заявке на участие в закупке на товарный знак;  б) конкретные показатели, соответствующие значениям, установленным документацией о закупке, и товарный знак (при его наличии) предлагаемого для поставки товара при условии отсутствия в документации о закупке указания на товарный знак;  2-1) согласие участника процедуры закупки на выполнение работ, оказание услуг на условиях, предусмотренных документацией о закупке, при условии размещения закупки на выполнение работ, оказание услуг;  3-1) при размещении закупки на выполнение работ, оказание услуг для выполнения, оказания которых используется товар:  - согласие, предусмотренное пунктом 2-1 настоящей части, в том числе, означающее согласие на использование товара, указание на товарный знак которого, содержится в документации о закупке, или согласие, предусмотренное пунктом 2-1 настоящей части, указание на товарный знак предлагаемого для использования товара и конкретные показатели этого товара, соответствующие значениям эквивалентности, установленным документацией о закупке, если участник процедуры закупки предлагает для использования товар, который является эквивалентным товару, указанному в документации о закупке, при условии содержания в документации о закупке указания на товарный знак используемого товара, а также требования о необходимости указания в заявке на участие в закупке на товарный знак (при его наличии);  - согласие, предусмотренное пунктом 2-1 настоящей части, а также конкретные показатели, соответствующие значениям, установленным документацией о закупке, и товарный знак (при его наличии) предлагаемого для использования товара при условии отсутствия в документации о закупке указания на товарный знак используемого товара;  14) иные документы в соответствии с требованиями настоящего Положения и извещением о проведении запроса котировок.  Предоставляемые в составе заявки документы должны быть четко напечатаны. Подчистки, дописки, исправления в сканированных документах, подготовленных самим участником, не допускаются, за исключением тех случаев, когда эти исправления (дописки) заверены рукописной надписью «исправленному верить», собственноручной подписью уполномоченного лица, расположенной рядом с каждым исправлением (допиской) и скреплены печатью участника закупки. |
| 19 | Критерии оценки и сопоставления заявок на участие в закупке | Единственным критерием оценки и сопоставления заявок на участие в закупке является цена. |
| 20 | Привлечение соисполнителей и требования к Участнику по ним: | Не установлено |
| 21 | Участниками запроса котировок могут быть только субъекты малого и среднего предпринимательства: | Не установлено |
| 22 | Требования кописанию участниками закупки поставляемого товара, оказания услуги, выполнения работы, которые являются предметом закупки, его функциональных характеристик (потребительских свойств), количественных и качественных характеристик | Участник закупки должен предложить к поставке товар, соответствующий требованиям, установленным заказчиком к такому товару (Часть V «Техническая часть» настоящего извещения)  Участнику закупки необходимо указать страну происхождения товара.  В случае, если в настоящей документации о закупке содержится указание на товарные знаки в отношении товара, поставка которого является предметом договора, применительно к таким товарным знакам следует читать «или эквивалент». Для определения эквивалентности предлагаемого к поставке товара служат указанные заказчиком технические характеристики такого товара.  Товары, предлагаемые к поставке, должны быть новыми, не бывшими в употреблении.  Для определения соответствия предлагаемых к поставке товаров требованиям заказчика, при заполнении заявки не допускается использование слов «не более», «не менее», «или эквивалент», «или аналог», «(+/-)», использование диапазонов значений при указании конкретных показателей и других выражений, допускающих разночтения или двусмысленное толкование. Исключения составляют случаи, когда показатели в соответствии с действующими нормативными документами, техническими или физическими условиями, данными производителей товаров указываются в виде диапазона значений или с допустимыми погрешностями. |
| 23 | Последствия признания закупки несостоявшейся | Если по окончании срока подачи заявок на участие в запросе котировок подана только одна заявка или не подано ни одной заявки, запрос котировок признается несостоявшимся. Если к участию в запросе котировок не был допущен ни один участник либо был допущен только один участник, запрос котировок признается несостоявшимся. |
| 24 | Размер и порядок предоставления обеспечения исполнения договора | Не установлено. |
| 25 | Срок подписания договора | Договор по результатам закупки заключается не ранее чем через 10 (десять) дней и не позднее чем через 20 (двадцать) дней с даты размещения на ЕИС итогового протокола, составленного по результатам процедуры закупки. |
| 26 | Условия допуска к участию и отстранения от участия в закупках | Комиссия по закупкам при рассмотрении заявок на соответствие требованиям законодательства, настоящего Положения и извещения о проведении запроса котировок обязана отказать участнику в допуске в случаях:  1) выявлено несоответствие участника хотя бы одному из требований, перечисленных в [п. 1.9.1](#Par427) настоящего Положения;  2) участник закупки и (или) его заявка не соответствуют иным требованиям документации о закупке (извещению о проведении запроса котировок) или настоящего Положения;  3) участник закупки не представил документы, необходимые для участия в процедуре закупки;  4) в представленных документах или в заявке указаны недостоверные сведения об участнике закупки и (или) о товарах, работах, услугах;  5) участник закупки не предоставил обеспечение заявки на участие в закупке, если такое обеспечение предусмотрено документацией о закупке.  Если выявлен хотя бы один из фактов, указанных в [п. 1.10.1](#Par442) настоящего Положения, комиссия по закупкам обязана отстранить участника от процедуры закупки на любом этапе ее проведения до момента заключения договора.  В случае выявления фактов, предусмотренных в [п. 1.10.1](#Par442), в момент рассмотрения заявок информация об отказе в допуске участникам отражается в протоколе рассмотрения заявок. При этом указываются основания отказа, факты, послужившие основанием для отказа, и обстоятельства выявления таких фактов. |
| 27 | Порядок рассмотрения и оценки заявок на участие в закупке | Комиссия по закупкам рассматривает заявки на участие в запросе котировок на предмет их соответствия требованиям законодательства, Положения о закупке товаров, работ, услуг ООО «УК «Зеленая роща» и извещения о проведении запроса котировок.  В течение 1 (одного) часа с даты и времени окончания срока подачи заявок на участие в запросе котировок оператор электронной площадки направляет Заказчику посредством функционала электронной площадки все заявки, поданные на участие в таком запросе.  Заказчиком составляется протокол открытия доступа к поданным заявкам |
| 28 | Порядок подведения итогов закупки | В ходе подведения итогов осуществляется оценка заявок путем сравнения предложений участников запроса котировок в электронной форме о цене договора и их ранжирования по степени предпочтительности в порядке возрастания. Оцениваются только заявки, допущенные комиссией по результатам рассмотрения.  При оценке заявок соблюдаются особенности, установленные пп. «х» п. 4 Постановления №1875:  При осуществлении в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" закупки программного обеспечения, указанного **в позиции 146 приложения N 1** к постановлению, заявка на участие в закупке, в которой содержится предложение программного обеспечения, реестровая запись о котором в реестре российского программного обеспечения или реестре евразийского программного обеспечения не содержит информацию о соответствии предлагаемого программного обеспечения дополнительным требованиям к программному обеспечению, приравнивается к заявке на участие в закупке, в которой содержится предложение программного обеспечения, происходящего из иностранного государства, если на участие в такой закупке подана заявка на участие в закупке, признанная по результатам ее рассмотрения соответствующей установленным в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" требованиям и содержащая предложение о программном обеспечении, реестровая запись о котором в реестре российского программного обеспечения или реестре евразийского программного обеспечения содержит информацию о соответствии предлагаемого программного обеспечения дополнительным требованиям к программному обеспечению.  Победителем запроса котировок признается участник, предложивший наименьшую цену договора. При наличии двух заявок с одинаково низкой ценой победителем признается участник, чья заявка поступила раньше. |
| 29 | Антидемпинговые меры | В случае, если участником закупки предложена цена, которая ниже начальной (максимальной) цены договора (цены лота) на 25 (двадцать пять) процентов и более (далее - демпинговая цена договора), то Заказчиком могут применяться следующие антидемпинговые меры:  1) требованиями к составу заявки на участие в конкурентной закупке, содержащей предложение о демпинговой цене договора (цене лота), может быть предусмотрено, что в составе такой заявки участник обязан представить обоснование предлагаемой цены договора (цены лота), которое может включать в себя гарантийное письмо от производителя с указанием цены и количества поставляемого товара, документы, подтверждающие наличие товара у участника, иные документы и расчеты, подтверждающие возможность участника осуществить поставку товара по предлагаемой цене.  В случае осуществления закупки работ, услуг требованиями к составу заявки на участие в конкурентной закупке, содержащей предложение о демпинговой цене договора (цене лота), может быть предусмотрено, что в составе такой заявки участник обязан представить расчет предлагаемой цены договора (цены лота) и ее обоснование.  Обоснование, расчеты и заключения, указанные в настоящем подпункте, представляются:  участником, предложившим демпинговую цену договора в составе заявки на участие в конкурсе, запросе котировок, запросе предложений. В случае невыполнения таким участником этого требования или признания комиссией предложенной цены договора необоснованной заявка на участие в конкурентной закупке такого участника отклоняется. Указанное решение комиссии фиксируется в протоколе;  участником, предложившим демпинговую цену договора и с которым заключается договор, при направлении заказчику подписанного проекта договора при проведении аукциона, в том числе в электронной форме. В случае невыполнения таким участником такого требования он признается уклонившимся от заключения договора. При признании заказчиком предложенной цены договора (цены лота) необоснованной, договор с таким участником не заключается и право заключения договора переходит к участнику аукциона, который предложил такую же, как и победитель аукциона, цену договора или предложение о цене договора (цене лота) которого содержит лучшие условия по цене договора (цене лота), следующие после условий, предложенных победителем аукциона. В этих случаях решение заказчика оформляется протоколом, который размещается в единой информационной системе не позднее 3 дней со дня подписания;  2) Комиссия по закупкам при обнаружении предложений, стоимость которых ниже среднеарифметической цены всех поданных участниками предложений более чем на 15 процентов, имеет право запросить дополнительные разъяснения порядка ценообразования и обоснованности такого снижения цены, а при отсутствии обоснованных разъяснений - отклонить поданное предложение. |
| 30 | 30.1 При осуществлении закупок предоставляется национальный режим, обеспечивающий происходящему из иностранного государства или группы иностранных государств (далее – иностранное государство) товару, работе, услуге, соответственно выполняемой, оказываемой иностранным гражданином или иностранным юридическим лицом (далее – иностранное лицо), равные условия с товаром российского происхождения, работой, услугой, соответственно выполняемой, оказываемой российским гражданином или российским юридическим лицом (далее – российское лицо), за исключением случаев принятия Правительством Российской Федерации мер, предусмотренных пунктом 1 части 2 статьи 3.1-4 Федерального закона № 223-ФЗ. Если иное не предусмотрено мерами, принятыми Правительством Российской Федерации в соответствии с пунктом 1 части 2 статьи 3.1-4 Федерального закона № 223-ФЗ, положения указанной статьи, касающиеся товара российского происхождения, работы, услуги, соответственно выполняемой, оказываемой российским лицом, применяются также в отношении товара, происходящего из иностранного государства, работы, услуги, соответственно выполняемой, оказываемой иностранным лицом, которым предоставляются равные условия с товаром российского происхождения, работой, услугой, соответственно выполняемой, оказываемой российским лицом.  30.2. Заказчик в случае принятия Правительством Российской Федерации мер, предусмотренных пунктом 1 части 2 статьи 3.1-4 Федерального закона № 223-ФЗ:  1) применяет:  а) запрет закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств, работ, услуг, соответственно выполняемых, оказываемых иностранными лицами;  б) ограничение закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств, работ, услуг, соответственно выполняемых, оказываемых иностранными лицами, в том числе минимальную обязательную долю закупок товаров российского происхождения;  в) преимущество в отношении товаров российского происхождения (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), работ, услуг, соответственно выполняемых, оказываемых российскими лицами;  2) устанавливает в извещении о проведении закупки, документации о проведении закупки требование к участникам закупки о предоставлении информации и перечень документов, которые подтверждают страну происхождения товара.  30.3. Заказчик при осуществлении закупки товара:  1) в случае установления Правительством Российской Федерации запрета закупок товара, указанного в подпункте «а» подпункта 1 пункта 2 настоящего раздела Извещения о закупке, не вправе:  а) заключать договор на поставку такого товара;  б) при исполнении договора осуществлять замену такого товара на происходящий из иностранного государства товар, в отношении которого установлен данный запрет;  2) в случае установления Правительством Российской Федерации ограничения закупок товара, указанного в подпункте «б» подпункта 1 пункта 2 настоящего раздела Извещения о закупке, не вправе:  а) заключать договор на поставку товара, происходящего из иностранного государства, если поданы заявка на участие в закупке, окончательное предложение, признанные по результатам их рассмотрения соответствующими требованиям Положения о закупке, извещения об осуществлении конкурентной закупки (в случае проведения конкурентной закупки), документации о конкурентной закупке (в случае проведения конкурентной закупки) и содержащие предложения о поставке товара российского происхождения;  б) при исполнении договора осуществлять замену товара на происходящий из иностранного государства товар, в отношении которого установлено данное ограничение, если договор предусматривает поставку товара российского происхождения;  3) в случае установления Правительством Российской Федерации преимущества в отношении товара российского происхождения, указанного в подпункте «в» подпункта 1 пункта 2 настоящего раздела Извещения о закупке:  а) при рассмотрении, оценке, сопоставлении заявок на участие в закупке, окончательных предложений осуществляет снижение на пятнадцать процентов ценового предложения, поданного в соответствии с Федеральным законом № 223-ФЗ и Положением о закупке участником закупки, предлагающим к поставке товар только российского происхождения, либо увеличение на пятнадцать процентов ценового предложения этого участника закупки в случае подачи им предложения о размере платы, подлежащей внесению за заключение договора;  б) в случае заключения договора с участником закупки, указанным в подпункте «а» настоящего подпункта, такой договор заключается без учета снижения либо увеличения ценового предложения, осуществленных в соответствии с подпунктом «а» настоящего подпункта;  в) при исполнении договора допускается замена товара исключительно на товар российского происхождения, если договор предусматривает поставку товара российского происхождения.  30.4. При установлении Правительством Российской Федерации случаев, при которых при осуществлении закупок промышленной продукции, в отношении которых Правительством Российской Федерации приняты меры, предусмотренные пунктом 1 части 2 статьи 3.1-4 Федерального закона № 223-ФЗ, заявка на участие в закупке, окончательное предложение, в которых содержится предложение о поставке товара российского происхождения, приравниваются соответственно к заявке на участие в закупке, окончательному предложению, в которых содержится предложение о поставке товара, происходящего из иностранного государства, если на участие в такой закупке поданы заявка на участие в закупке, окончательное предложение, признанные по результатам их рассмотрения соответствующими требованиям Положения о закупке, извещения об осуществлении конкурентной закупки (в случае проведения конкурентной закупки), документации о конкурентной закупке (в случае проведения конкурентной закупки) и содержащие предложения о поставке товара российского происхождения, в наибольшей степени удовлетворяющего требованиям к промышленной продукции, предъявляемым в соответствии с законодательством в сфере промышленной политики в целях отнесения этой продукции к российской промышленной продукции.  30.5. Заказчик при осуществлении закупки работы, услуги:  1) в случае установления Правительством Российской Федерации запрета закупки таких работы, услуги, соответственно выполняемой, оказываемой иностранным лицом, предусмотренного подпунктом «а» пункта 1 части 2 статьи 3.1-4 Федерального закона № 223-ФЗ, не вправе:  а) заключать договор на выполнение такой работы, оказание такой услуги с подрядчиком (исполнителем), являющимся иностранным лицом;  б) осуществлять перемену подрядчика (исполнителя) (в случае, если эта перемена допускается гражданским законодательством), с которым заключен указанный договор, на иностранное лицо, которое зарегистрировано на территории иностранного государства, в отношении которого установлен данный запрет;  2) в случае установления Правительством Российской Федерации ограничения закупки таких работы, услуги, соответственно выполняемой, оказываемой иностранным лицом, предусмотренного подпунктом «б» пункта 1 части 2 статьи 3.1-4 Федерального закона № 223-ФЗ, не вправе:  а) заключать договор с участником закупки, являющимся иностранным лицом, если российским лицом поданы заявка на участие в закупке, окончательное предложение, признанные по результатам их рассмотрения соответствующими требованиям положения о закупке, извещения об осуществлении конкурентной закупки (в случае проведения конкурентной закупки), документации о конкурентной закупке (в случае проведения конкурентной закупки);  б) осуществлять перемену подрядчика (исполнителя) (в случае, если эта перемена допускается гражданским законодательством), с которым заключен договор, на иностранное лицо, которое зарегистрировано на территории иностранного государства, в отношении которого установлено данное ограничение, если договор заключен с российским лицом;  3) в случае установления Правительством Российской Федерации преимущества в отношении таких работы, услуги, соответственно выполняемой, оказываемой иностранным лицом, предусмотренного подпунктом «в» пункта 1 части 2 статьи 3.1-4 Федерального закона № 223-ФЗ, не вправе:  а) при рассмотрении, оценке, сопоставлении заявок на участие в конкурентной закупке, заявок на участие в неконкурентной закупке, окончательных предложений осуществлять снижение на пятнадцать процентов ценового предложения, поданного в соответствии с Федеральным законом № 223-ФЗ и Положением о закупке участником закупки, являющимся российским лицом, либо увеличение на пятнадцать процентов ценового предложения этого участника закупки в случае подачи им предложения о размере платы, подлежащей внесению за заключение с ним договора;  б) в случае заключения договора с участником закупки, указанным в подпункте «а» настоящего подпункта, заключать договор без учета снижения либо увеличения ценового предложения, осуществленных в соответствии с подпунктом «а» настоящего подпункта;  в) осуществлять перемену подрядчика (исполнителя) (в случае, если эта перемена допускается гражданским законодательством), с которым заключен договор, допускается исключительно на российское лицо, если договор заключен с российским лицом | |
| 31 | Запрет закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств, работ, услуг, соответственно выполняемых, оказываемых иностранными лицами; | **Применяется. Позиция 146 в Приложении №1 постановления Правительства Российской Федерации от 23.12.2024 № 1875.**  1.1. Документом, подтверждающими страну происхождения товара Российская Федерация, для закупки по позиции 146 (Программа для электронной вычислительной машины и (или) базы данных по коду ОКПД2 58.29) Приложении №1 является - **порядковый номер реестровой записи из единого реестра российских программ для электронных вычислительных машин и баз данных.**  1.2. Документом, подтверждающими страну происхождения товара Российская Федерация, для закупки по позиции 146 (Программа для электронной вычислительной машины и (или) базы данных по коду ОКПД2 58.29) Приложении №1 и его соответствия дополнительным требованиям к программам и базам данных, сведения о которых включены в реестр российского программного обеспечения, утвержденным ПП РФ от 23.03.2017 № 325 является - **порядковый номер реестровой записи из реестра российского программного обеспечения, содержащей информацию о соответствии программного обеспечения дополнительным требованиям к программному обеспечению.**  1.3. Документом, подтверждающими страну происхождения товара из государств - членов Евразийского экономического союза (за исключением Российской Федерации), для закупки по позиции 146 (Программа для электронной вычислительной машины и (или) базы данных по коду ОКПД2 58.29) Приложении №1 является - **порядковый номер реестровой записи из единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации.**  1.4. Документом, подтверждающими страну происхождения товара из государств - членов Евразийского экономического союза (за исключением Российской Федерации), для закупки по позиции 146 (Программа для электронной вычислительной машины и (или) базы данных по коду ОКПД2 58.29) Приложении №1 и его соответствия дополнительным требованиям к программам и базам данных, сведения о которых включены в реестр российского программного обеспечения, утвержденным ПП РФ от 23.03.2017 № 325 является - **порядковый номер реестровой записи из реестра евразийского программного обеспечения, содержащей информацию о соответствии программного обеспечения дополнительным требованиям к программному обеспечению.**  **В случае непредоставления вышеуказанной информации в составе заявки - товар приравнивается к иностранному.** |
| 32 | Ограничение закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств, работ, услуг, соответственно выполняемых, оказываемых иностранными лицами | Не применяется. Товар отсутствует в Приложении №2 постановления Правительства Российской Федерации от 23.12.2024 № 1875 |
| 33 | Преимущество в отношении товаров российского происхождения (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), работ, услуг, соответственно выполняемых, оказываемых российскими лицами. | Не применяется. |

**Часть II. Образцы форм и документов для заполнения участниками закупки**

**ФОРМА 1**

**(обязательная)**

**ЗАЯВКА НА УЧАСТИЕ В ЗАПРОСЕ КОТИРОВОК В ЭЛЕКТРОННОЙ ФОРМЕ**

1. Изучив извещение и документацию о запросе котировок в электронной форме №\_\_\_\_\_\_\_\_\_\_\_ «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_», включая проект договора, который

*(наименование закупки)*

будет заключен с победителем запроса котировок, а также применимые к данному запросу котировок законодательство и нормативные правовые акты,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(наименование участника закупки)*

зарегистрированное (ный, ная) в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (наименование регистрирующего органа) за основным государственным регистрационным номером \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (свидетельство о внесении записи в Единый государственный реестр юридических лиц (индивидуальных предпринимателей) №\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_),в лице\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(наименование должности руководителя и его Ф.И.О. Ф.И.О. указываются полностью)*

действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(устав, доверенность, свидетельство с указанием его реквизитов и т.п.)*

сообщает о согласии исполнить условия данного договора и направляет настоящую заявку на участие в запросе котировок в электронной форме.

1. Настоящей заявкой подтверждаем, что \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(наименование участника закупки)*

соответствует следующим требованиям:

1. Участник закупки не находится в процессе ликвидации (для участника - юридического лица), не признан по решению арбитражного суда несостоятельным (банкротом) (для участника - как юридического, так и физического лица);

2. На день подачи заявки деятельность участника закупки не приостановлена порядке, предусмотренном Кодексом РФ об административных правонарушениях;

3. У участника закупки отсутствует недоимка по налогам, сборам, задолженность по иным обязательным платежам в бюджеты бюджетной системы РФ за прошедший календарный год, размер которых превышает 25 процентов от балансовой стоимости активов участника закупки по данным бухгалтерской отчетности за последний отчетный период;

4. Сведения об участнике закупки отсутствуют в реестрах недобросовестных поставщиков, ведение которых предусмотрено Законом N 223-ФЗ и Законом N 44-ФЗ;

Мы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ с соблюдением требований и срока исполнения обязательств по договору.

с ценой договора: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) рублей \_\_\_ копеек,

(цифрой) (прописью)

в том числе НДС по ставке \_\_\_% в сумме: \_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) рублей \_\_\_ копеек

(цифрой) (прописью)

*(либо НДС не предусмотрен).*

В указанную цену включены\*: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(\*указать затраты участника, связанные с исполнением договора, в соответствии с Разделом 12 ЧастиI документации о закупке)

**Таблица №1**

**Наименование и количество товара:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование** | **Ед. изм.** | **Кол-во** | **Цена за ед., руб. без учета НДС/с НДС** | **Сумма, руб. без учета НДС/с НДС** | | **Страна происхождения товара** |
| **1.** |  |  |  |  |  | |  |
| **2.** |  |  |  |  |  | |  |
| **Итого:** | | | | | |  |  |

3. В случае, если мы будем признаны победителем запроса котировок в электронной форме, мы берем на себя обязательство подписать договор с Обществом с ограниченной ответственностью «Управляющая компания «Зеленая роща» в соответствии с требованиями документации о запросе котировок в электронной форме и условиями наших предложений.

4. Мы уведомлены о том, что в случае принятия заказчиком решения о заключении с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ договора, и нашего уклонения от заключения

(наименование участника закупки)

договора, сведения о нашей организации будут включены в Реестр недобросовестных поставщиков.

5. Сообщаем, что для оперативного уведомления нас по вопросам организационного характера и взаимодействия с Заказчиком нами уполномочен:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(Ф.И.О., телефон, адрес электронной почты работника участника закупки)

Все сведения просим сообщать указанному уполномоченному лицу.

6. Наши наименование, юридический адрес и банковские реквизиты:

|  |  |
| --- | --- |
| Место нахождения (для юридического лица), место жительства (для физического лица): |  |
| Почтовый адрес (для юридического лица) |  |
| Контактный телефон: |  |
| Факс (при наличии): |  |
| Адрес электронной почты: |  |
| ИНН |  |
| КПП |  |
| ОГРН |  |
| ОКПО |  |
| **Банковские реквизиты:** |  |
| Наименование обслуживающего банка |  |
| Расчетный счет |  |
| Корреспондентский счет |  |
| БИК |  |

7. Подпись руководителя (уполномоченного лица):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г. (наименование должности, подпись, Ф.И.О) **М.П. (при наличии)**

Приложение № 1

к заявке на участие в запросе котировок в электронной форме

**Согласие на обработку и передачу своих персональных данных[[1]](#footnote-1)**

В соответствии с Федеральным законом РФ № 152-ФЗ от 27 июля 2006 г. «О персональных данных»

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

|  |
| --- |
| (ФИО полностью) |

паспорт серии \_\_\_\_\_\_ №\_\_\_\_\_\_\_\_\_ выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| *(кем выдан)* |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_ г.,

|  |
| --- |
| *(дата выдачи)* |

зарегистрированный (-ая) по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

дата рождения \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, контактный телефон \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

даю согласие Обществу с ограниченной ответственностью «УК «Зеленая роща» ИНН 5753062527 (далее – ООО «УК «Зеленая роща»), на обработку и передачу своих персональных данных в Минэнерго России, Росфинмониторинг, ФНС России, ФАС России, ФСТ России и иные организации, осуществляющие контроль над деятельностью ООО «УК «Зеленая роща» в рамках действующего законодательства РФ.

Настоящее согласие действует со дня его подписания и передачи в ООО «УК «Зеленая роща» моих персональных данных и действует до даты отзыва, направленного мною в письменном виде в ООО «УК «Зеленая роща».

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| Дата | Подпись | ФИО |

Приложение № 2

к заявке на участие в запросе котировок в электронной форме

**Анкета Участника\***

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование** | **Сведения об Участнике** | |
|  | Организационно-правовая форма и наименование фирмы Участника, дата регистрации (полная и сокращенная) |  |
|  | Юридический адрес |  |
|  | Почтовый адрес |  |
|  | Фактический адрес |  |
|  | Должность, Ф.И.О., избранного (назначенного) на должность единоличного исполнительного органа юридического лица, либо иного лица, имеющего право без доверенности действовать от имени данного юридического лица |  |
|  | Телефоны Участника (с указанием кода города) |  |
|  | Факс Участника (с указанием кода города) |  |
|  | Адрес электронной почты Участника, web-сайт |  |
|  | ИНН/КПП Участника |  |
|  | Банковские реквизиты (наименование и адрес банка, номер расчетного счета Участника в банке, телефоны банка, прочие банковские реквизиты) |  |
|  | Учредители (перечислить наименование или организационно-правовую форму или Ф.И.О. всех учредителей, чья доля в уставном капитале превышает 10%) |  |
|  | Филиалы: перечислить наименования и почтовые адреса |  |
|  | Свидетельство о внесении записи в Единый государственный реестр юридических лиц (дата, номер, кем выдано) |  |
|  | Фамилия, Имя и Отчество ответственного лица Участника с указанием должности и контактного телефона |  |
|  | Сведения о необходимости одобрения заключения сделки уполномоченными органами управления Участника/Заказчика |  |

**Руководитель (или уполномоченный представитель)** \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / /

(подпись)

**Главный бухгалтер** \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / /

(подпись)

М.П.

|  |
| --- |
| *\* Инструкция по заполнению Формы:* |

1. Данную инструкцию не следует воспроизводить в Заявке и приложениях к ней, подготовленных Участником.

2.  Изменение данной Формы допустимо только в случае внесения дополнительных сведений об организации.

3. Участник закупки, являющийся юридическим лицом, должен указать свое полное наименование (с указанием организационно-правовой формы) и адрес место нахождения. Участник закупки, являющийся физическим лицом, в том числе индивидуальным предпринимателем, указывает полностью фамилию, имя, отчество, паспортные данные, адрес регистрации.

4. Форма обязательна для заполнения!!! В случае отсутствия/незаполнения настоящей Формы заявка Участника не рассматривается и подлежит отклонению!!!

Приложение № 3

к заявке на участие в запросе котировок в электронной форме

(представляется в случае, если документы Заявки на участие в Запросе котировок в электронной форме подписываются не руководителем, форма является примерной, документ может быть предоставлен по любой другой форме, установленной локально-нормативными актами Участника)

**Доверенность на подписание заявки и иных документов, входящих в ее состав**

На бланке организации

Дата

**ДОВЕРЕННОСТЬ № \_\_\_\_**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| *(прописью число, месяц и год выдачи доверенности)* |

Организация – Участник:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| *(наименование организации)* |

доверяет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| *(фамилия, имя, отчество, должность)* |

паспорт серии \_\_\_\_\_\_ №\_\_\_\_\_\_\_\_\_ выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ представлять Заказчику/Заказчику процедуры запроса котировок в электронной форме и подписывать необходимые документы для участия, в том числе Заявку \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| *(наименование Запроса предложений)* |

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ удостоверяем.

|  |  |
| --- | --- |
| *(Ф.И.О. поверенного)* | *(Подпись поверенного)* |

Доверенность действительна по «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

**Руководитель организации** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| /Фамилия И.О./ | (подпись) |

М.П.

**ФОРМА 2**

**(рекомендуемая)**

Дата, исх. номер

**ЗАПРОС НА РАЗЪЯСНЕНИЕ ДОКУМЕНТАЦИИ И (ИЛИ) ИЗВЕЩЕНИЯ О ЗАПРОСЕ КОТИРОВОК**

№\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»

(предмет закупки)

Прошу Вас разъяснить следующие положения документации и (или) извещения о запросе котировок в электронной форме:

|  |  |  |
| --- | --- | --- |
| **Раздел документации и (или) извещения** | **Ссылка на пункт Раздела документации и (или) извещения** | **Содержание запроса на разъяснение положений документации и (или) извещения** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Ответ на запрос прошу направить по адресу:

*( e-mail организации, направившей запрос)*

Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(*подпись, расшифровка подписи)*

# **Часть III. Обоснование начальной (максимальной) цены договора**



# **Часть IV. Проект договора**

**на оказание услуг по продлению срока действия лицензий на неисключительное право использования антивирусного программного обеспечения «Касперский»**

г. Орел «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.

**Общество с ограниченной ответственностью «Управляющая компания «Зеленая роща»** именуемое в дальнейшем «Заказчик», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ с одной стороны,

и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_именуемый в дальнейшем «Исполнитель» в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующей на основании \_\_\_\_\_\_\_\_\_\_\_ с соблюдением требований Гражданского кодекса Российской Федерации, Федерального закона от 18.07.2011 №223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», и положения о закупке для нужд ООО «УК «Зеленая роща» и по результатам осуществления закупки в форме запроса котировок в электронной форме (Протокол от "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_ 2025 г. №\_\_\_), заключили настоящий договор о нижеследующем:

**1. Предмет договора**

1.1. Заказчик поручает, а Исполнитель принимает на себя обязанности по оказанию услуг по продлению срока действия лицензий на неисключительное право использования антивирусного программного обеспечения «Касперский» в соответствии с требованиями, указанными в Техническом задании (Приложение № 1 к договору) и в Спецификации (Приложение № 2 к договору) (далее – услуги), а Заказчик обязуется принять результат услуг и оплатить в порядке и на условиях, определенных настоящим договором.

**2. Цена договора и порядок расчетов**

2.1 Общая сумма договора составляет – \_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_) рублей \_\_\_\_\_ копеек, включая налог на добавленную стоимость (\_\_ процентов): \_\_\_\_\_ (\_\_\_\_\_\_) рублей \_\_\_\_копеек *(если НДС не облагается, указать основание. В случае если договор будет заключен с физическим лицом, за исключением индивидуального предпринимателя или лица, занимающегося частной практикой сумма, подлежащая уплате такому физическому лицу, уменьшается на размер налоговых платежей, связанных с оплатой договора)*.

Цена договора включает в себя все прямые и дополнительные затраты и начисления, связанные с оказанием всего объема услуг, предусмотренных настоящим договором, а также включает все налоги, сборы, пошлины и прочие обязательные платежи, предусмотренные законодательством Российской Федерации.

2.2. Форма оплаты – безналичный расчет. Оплата за фактически оказанные услуги осуществляется на основании акта об оказанных услугах, счета, представленного Исполнителем, в течение 7 (семи) рабочих дней со дня подписания Заказчиком документов о приемке услуг.

2.3. Авансирование не производится.

2.4. Днем оплаты оказанных Услуг считается день списания соответствующей суммы денежных средств со счета Заказчика.

**3. Место и сроки оказания услуг**

3.1. Место оказания услуг: 302040, Орловская область, г. Орел, Ломоносова, д.6 каб.408

3.2. Срок оказания услуг: передача неисключительных (пользовательских) прав осуществляется Исполнителем в течение 10 рабочих дней с момента подписания договора сторонами.

3.3. Срок действия лицензии должен быть не менее 12 месяцев с даты активации ключа.

3.4. Обязательство Исполнителя по оказанию услуг считается исполненным с момента подписания Заказчиком акта оказанных услуг.

**4. Права и обязанности сторон**

**4.1. Заказчик имеет право:**

4.1.1. Требовать от Исполнителя надлежащего исполнения обязательств в соответствии с настоящим Договором.

4.1.2. Требовать от Исполнителя своевременного устранения недостатков, выявленных в ходе оказания Услуг и (или) сдачи-приёмки Услуг, а также возникших на протяжении всего гарантийного срока, по всему объёму оказанных Услуг.

4.1.3. Требовать от Исполнителя предоставления надлежащим образом оформленной документации, подтверждающей исполнение обязательств по настоящему договору.

4.1.4. Проверять ход и качество оказываемых Исполнителем услуг, не вмешиваясь в его деятельность.

4.1.5. Заказчик вправе, письменно уведомив Исполнителя, приостановить все платежи по настоящему Договору, если Исполнитель не выполняет своих обязательств (или часть обязательств) по Договору, при условии, что такое уведомление о приостановлении платежей определяет характер невыполнения обязательств исодержит требование того, чтобы Исполнитель исправил положение в течение периода времени, не превышающего тридцати дней после получения Исполнителем такого уведомления.

**4.2. Заказчик обязан:**

4.2.1. Назначить ответственного представителя по представлению интересов Заказчика во взаимодействии с Исполнителем по настоящему Договору.

4.2.2. Своевременно сообщать в письменной форме Исполнителю о выявленных недостатках в ходе оказания услуг.

4.2.3. Обеспечить своевременную приемку оказанных Услуг, в случае отсутствияпретензий относительно их объема, качества и соблюдения сроков их оказания, подписать акт оказанных услуг и передать один экземпляр Исполнителю.

4.2.4. Произвести оплату в порядке и в сроки, предусмотренные настоящим Договором.

**4.3. Исполнитель имеет право:**

4.3.1. Требовать оплаты оказанных Заказчику услуг в соответствии с подписанным актом оказанных услуг.

4.3.2. Требовать обеспечения своевременной приемки оказанных Услуг и подписания акта оказанных услуг либо обоснованного отказа от его подписания в установленные сроки.

**4.4. Исполнитель обязан:**

4.4.1. Своевременно и надлежащим образом оказывать Услуги в соответствии с Техническим заданием и настоящим Договором.

4.4.2. Предоставлять Заказчику информацию, касающуюся оказываемых Услуг по настоящему Договору**.**

4.4.3. Предупреждать Заказчика о вероятных конкретных событиях или обстоятельствах в будущем, которые могут негативно повлиять на качество Услуг.

4.4.4. Своими силами и за свой счет устранить допущенные по своей вине недостатки в оказанных Услугах.

4.4.5. Представлять Заказчику акт оказанных услуг не позднее десяти календарных дней после оказания Услуг.

4.4.6. Исполнитель обязан файл-ключ и сканированную копию лицензионного сертификата в pdf-файле направить Заказчику по сети Интернет на электронный почтовый адрес administrator@greenpark57.ru. Оригинал лицензионного сертификата передать Заказчику в течение срока оказания Услуг.

4.4.7. Исполнитель обязан гарантировать, что программное обеспечение, на неисключительные права использования которого передаются лицензии в соответствии с Техническим заданием и настоящим Договором, является полностью лицензионным, правомерно введено в гражданский оборот на территории Российской Федерации и обеспечивается технической поддержкой соответствующих правообладателей (производителей), а также, что предоставляемые в соответствии с данными лицензиями неисключительные права использования программного обеспечения не нарушают каких-либо авторских прав, неимущественных и/или имущественных прав любых третьих лиц.

4.4.8. Исполнитель обязан обеспечить гарантийное обслуживание поставляемого программного обеспечения без дополнительных расходов со стороны Заказчика. Под гарантийным обслуживанием подразумевается восстановление работоспособности программного обеспечения при выходе его из строя по причинам, не связанным с некорректной эксплуатацией в гарантийный период. В том числе консультации технических специалистов по телефону («горячая линия»), выезд специалиста к Заказчику в течение 5 рабочих дней, диагностика и устранение неисправностей на территории Заказчика.

4.4.9. Исполнитель, в отношении услуг которого постановлением Правительства Российской Федерации предоставлен приоритет услуг российского происхождения по отношению к услугам, происходящим из иностранного государства, не вправе заменить страну происхождения услуг, за исключением случая, когда в результате такой замены вместо иностранных услуг оказываются российские услуги, при этом качество, технические и функциональные характеристики (потребительские свойства) таких услуг не уступают качеству и соответствующим техническим и функциональным услуг, указанных в настоящем Договоре.

4.4.10. Исполнитель гарантирует, что он надлежащим образом исполняет свои налоговые обязательства, в том числе своевременно сдает налоговую отчетность (декларацию), отражающую реальные факты своей хозяйственной деятельности, декларирует свои налоговые обязательства по сделкам, совершаемым от его имени и уплачивает налоги в соответствии с реально осуществляемыми операциями, представляет информацию и документы по запросам налоговых органов, его должностные лица не дисквалифицированы, не находятся в местах лишения свободы и не существует иных препятствий для осуществления ими своих полномочий и обязанностей, он имеет все необходимые ресурсы для надлежащего исполнения настоящего договора, в том числе помещения, штат сотрудников, материально-техническую базу, разрешения и лицензии и обязуется надлежащим образом исполнить вышеуказанные обязанности.

4.4.11. Исполнитель гарантирует, что он проявляет должную осмотрительность и осторожность при выборе своих контрагентов, исходя из условий и обстоятельств совершаемых сделок, не привлекает к исполнению договорных обязательств контрагентов, не осуществляющих реальную предпринимательскую деятельность и не декларирующих свои налоговые обязательства по сделкам, оформляемых от его имени.

4.4.12. Если по вине Исполнителя и/или его должностных лиц будет отказано в применении налоговых вычетов по налогам, а также применены иные меры ответственности, Исполнитель обязуется возместить Заказчику все соответствующие убытки в размере доначисленных или не возвращенных из бюджета РФ налогов, а так же все суммы пеней и штрафов, которые налоговые органы в этой связи удержали с Заказчика. Под виной Исполнителя для целей настоящего Договора понимается любая ситуация, когда налоговый орган прямо или косвенно признает Исполнителя и/или его контрагентов недобросовестным налогоплательщиком.

**5. Порядок приема-сдачи оказанных услуг**

5.1. Заказчик назначает своего представителя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(фамилия, имя, отчество, должность, контактный телефон представителя Заказчика)

который от имени Заказчика осуществляет взаимодействие с Исполнителем по вопросам оказания Услуг.

5.2. Исполнитель назначает своего представителя - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(фамилия, имя, отчество, должность, контактный телефон представителя Исполнителя) который от имени Исполнителя осуществляет взаимодействие с Заказчиком по вопросам оказания Услуг, в том числе, осуществляет техническое оформление всех документов, без права их подписи от имени Исполнителя.

5.3. По факту оказания Услуг составляется и подписывается акт об оказании услуг представителями Заказчика и Исполнителя.

5.4. В течение 5 дней со дня получения актов об оказании услуг Заказчик должен направить Исполнителю подписанный акт об оказании услуг или мотивированный отказ от приемки Услуг.

5.5. При обнаружении отступлений от требований Заказчика и (или) условий настоящего Договора, ухудшающих результат Услуг, или иных недостатков в Услугах, Заказчик обязан немедленно заявить об этом Исполнителю и отразить замечания в Акте с указанием срока их исправления.

5.6. Услуга считается оказанной с момента подписания Сторонами актов об оказании услуг.

**6. Ответственность сторон**

6.1. За невыполнение или ненадлежащее выполнение обязательств по договору Стороны несут ответственность в соответствии с действующим законодательством РФ.

6.2. В случае просрочки исполнения (ненадлежащего исполнения) Исполнителем обязательств, предусмотренных Договором, а также в иных случаях неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Договором, Заказчик вправе направить Исполнителю требование об уплате неустоек (штрафов, пеней). Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного Договором, начиная со дня, следующего после дня истечения установленного Договором срока исполнения обязательства. Такая пеня устанавливается Договором в размере одной трехсотой действующей на день уплаты пеней ключевой ставки Центрального банка Российской Федерации от стоимости не оказанных в срок услуг.

6.3. В случае просрочки исполнения Заказчиком обязательства, предусмотренного настоящим Договором, Исполнитель вправе потребовать уплату неустойки (штрафа, пеней). Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного Договором, начиная со дня, следующего после дня истечения установленного Договором срока исполнения обязательства. Такая пеня устанавливается Договором в размере одной трехсотой действующей на день уплаты пеней ключевой ставки Центрального банка Российской Федерации от неуплаченной в срок суммы.

6.4. Сторона освобождается от уплаты неустойки (штрафа, пеней), если докажет, что просрочка исполнения указанных обязательств произошла вследствие непреодолимой силы или по вине другой Стороны.

6.5. Сторона, не исполнившая или ненадлежащим образом исполнившая обязательство, несет ответственность, если не докажет, что надлежащее исполнение оказалось невозможным вследствие непреодолимой силы, то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств.

Доказательством наличия обстоятельств непреодолимой силы и их продолжительности будут служить свидетельства соответствующих компетентных органов.

6.6. Неустойка (штрафы, пени) должна быть перечислена одной Стороной по письменному запросу другой Стороны в течение 10-ти рабочих дней со дня получения такого запроса.

Возмещение ущерба, убытков и уплата штрафов и пеней не освобождает виновную Сторону от выполнения своих обязательств по договору. Ни при каких условиях, ни одна из Сторон не возмещает другой Стороне упущенную выгоду.

**7. Срок действия договора**

7.1. Настоящий Договор вступает в силу с даты подписания его обеими Сторонами и действует до полного исполнения Сторонами своих обязательств.

**8. Форс-мажор**

8.1. Понятием обстоятельств непреодолимой силы охватываются внешние и чрезвычайные события, отсутствовавшие во время подписания настоящего договора и наступившие помимо воли и желания Сторон, действия которых Стороны не могли предотвратить мерами и средствами, которые оправданно и целесообразно ожидать от добросовестно действующей Стороны. К подобным обстоятельствам Сторон относят: военные действия, эпидемии, пожары, природные катастрофы, акты и действия государственных органов, делающие невозможными исполнение обязательств по настоящему договору в соответствии с законным порядком.

8.2. Сторона, для которой наступили обстоятельства непреодолимой силы, должна немедленно письменно известить другую Сторону о наступлении, виде и возможной продолжительности действия обстоятельств непреодолимой силы, препятствующих исполнению обязательств по настоящему договору. Если о вышеупомянутых событиях не будет своевременно сообщено, Стороны теряют право ссылаться на указанные обстоятельства как на причину невыполнения своих обязательств по настоящему договору.

8.3. Наступление обстоятельств непреодолимой силы при условии, что приняты установленные меры по извещению об этом других Сторон, продлевает срок выполнения обязательств по договору на период, по своей продолжительности соответствующий продолжительности обстоятельств и разумному сроку для устранения их последствий.

8.4. Если действие обстоятельств непреодолимой силы продолжается более 3-х месяцев подряд, Стороны должны договориться о судьбе настоящего договора. Если соглашение Сторонами не достигнуто, любая из Сторон вправе в одностороннем, порядке расторгнуть настоящий договор путем направления заказным письмом другой Стороне соответствующего извещения не позднее, чем за 15 дней до предполагаемой даты расторжения договора.

**9. Порядок разрешения споров**

9.1. Спорные вопросы, возникающие в ходе исполнения настоящего договора, разрешаются Сторонами путем совместных переговоров.

9.2. Если, по мнению одной из Сторон, отсутствует возможность разрешить возникший между Сторонами спор, он разрешается в Арбитражном суде Орловской области.

**10. Порядок изменения и расторжения договора**

10.1. Настоящий Договор может быть изменен и дополнен по Соглашению Сторон только по основаниям, предусмотренным действующим законодательством Российской Федерации и настоящим договором.

10.2. Все изменения и дополнения к настоящему Договору действительны, если они оформлены в виде дополнительного соглашения к настоящему договору и подписаны надлежаще уполномоченными на то представителями Сторон.

10.3. Расторжение договора допускается по соглашению Сторон, по решению суда или в связи с односторонним отказом Стороны договора от исполнения Договора в соответствии с действующим законодательством Российской Федерации.

**11. Прочие условия**

11.1. Настоящий договор составлен в двух идентичных экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

11.2. В случае изменения у какой-либо из Сторон названия, адреса (местонахождения), банковских и иных реквизитов, контактных телефонов, она обязана немедленно письменно известить об этом другую Сторону, путём направления уведомления.

11.3. Неотъемлемой частью настоящего договора являются:

- Приложение № 1 – Спецификация;

- Приложение № 2 – Техническое задание.

**12. Адреса, реквизиты и подписи Сторон**

|  |  |
| --- | --- |
| **Заказчик** | **ИСПОЛНИТЕЛЬ** |
| ИНН/КПП\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ОГРН\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Юр./факт. адрес:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  р/с № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  в\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  к/сч\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  БИК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ОКПО\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Телефон/факс:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ИНН/КПП\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ОГРН\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Юр./факт. адрес:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  р/с № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  к/сч \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  БИК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ОКПО\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Телефон/факс:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **ПОДПИСИ СТОРОН:** | |
| **от Заказчика:** | **от Исполнителя:** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_/  м.п. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/  м.п. |

Приложение №1

к договору №\_\_\_\_\_\_\_\_\_\_\_ от «\_\_»\_\_\_\_\_\_\_\_2025г.

**СПЕЦИФИКАЦИЯ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование услуг** | **Ед.**  **изм.** | **Кол-во** | **Цена за ед., с НДС/без НДС** | **Общая сумма, руб., с НДС/без НДС** | **Страна производитель** |
| 1 | Kaspersky Endpoint Security для бизнеса - Расширенный на срок 1 год | шт. | 101 |  |  |  |
| 2 |  |  |  |  |  |  |

|  |  |
| --- | --- |
| **ПОДПИСИ СТОРОН:** | |
| **от Заказчика:** | **от Исполнителя:** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_/  м.п. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/  м.п. |

Приложение №2

к договору №\_\_\_\_\_\_\_\_\_\_\_ от «\_\_»\_\_\_\_\_\_\_\_2025г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**1.** **Предмет контракта**: передача неисключительных прав на использование программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный для нужд общества с ограниченной ответственностью «Управляющая компания «Зеленая Роща».

**2. Общие требования:** исполнитель обеспечивает предусмотренную производителями функциональность программного обеспечения в том числе и в рамках продления действующей лицензии на программное обеспечение Kaspersky Endpoint Security для бизнеса № 8A452E1F-6411-4559-BE0D-DA7E0CEA4994.

**3. Перечень предоставляемых прав:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование | Характеристика | Ед.  изм. | Кол-во |
| 1 | Право на использование Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 100-149 Node 1 year Renewal License | Приложение № 1 к техническому заданию. Продление действующей лицензии на антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса – Расширенный на срок 1 год с учётом имеющейся у Заказчика лицензии **№ 8A452E1F-6411-4559-BE0D-DA7E0CEA4994**  Комплектация:  - ключевой файл для активации программного обеспечения; | Шт. | 1 |
| 2 | Право на использование Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 100-149 Node 1 year Renewal License | Приложение № 1 к техническому заданию. Продление действующей лицензии на антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса – Расширенный на срок 1 год с учётом имеющейся у Заказчика лицензии **№ 8A452E1F-6411-4559-BE0D-DA7E0CEA4994**  Комплектация:  - ключевой файл для активации программного обеспечения; | Шт. | 100 |

# 

# **Характеристики**

Продление действующей лицензии на антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса – Расширенный на срок 1 год с учётом имеющейся у Заказчика лицензии № 8A452E1F-6411-4559-BE0D-DA7E0CEA4994 с дополнительным модулем предотвращения утечек данных.

Комплектация:

- ключевой файл для активации программного обеспечения;

Страна происхождения программного обеспечения: Российская Федерация

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 / Ultimate / Enterprise Service Pack 1 и выше;
* Windows 8 Professional / Enterprise (32 / 64-разрядная);
* Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
* Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise;
* Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise

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 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;
  + наличие инструмента мониторинга сети по протоколам TCP и UDP;
  + возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
  + возможность установки ограничение длительности выполнения задачи;
  + возможность ставить задачи проверки в очередь, если проверка уже выполняется.
  + 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;
  + возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий)
  + возможность создавать служебную учетную запись агента аутентификации при шифровании диска;
  + поддержка стороннего поставщика учетных данных ADSelfService Plus для работы SSO при полнодисковом шифровании.

# 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), Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2;
* Windows MultiPoint Server 2011 (64-разрядная);
* Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;
* Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2016 Essentials / Standard / Datacenter;
* Windows Server 2019 Essentials / Standard / Datacenter;
* Windows Server 2022.

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;
* поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов.
* возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
* возможность установки ограничения длительности выполнения задачи;
* возможность ставить задачи проверки в очередь, если проверка уже выполняется.

# 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 10.14 - 12;

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;
* возможность установки расширений из командной строки с помощью новой команды kav;
* возможность задавать исключения при проверке указанных областей на уровне перехватов файловых операций;
* возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены.

# 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:

* CentOS 6.7 и выше.
* Debian GNU/Linux 10.1 и выше.
* Debian GNU/Linux 11.
* Mageia 4.
* Red Hat Enterprise Linux 6.7 и выше.
* Альт 8 СП Рабочая Станция.
* Альт 8 СП Сервер.
* Альт Образование 10.
* Альт Рабочая Станция 10.

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

* AlmaLinux OS 8 и выше.
* AlmaLinux OS 9 и выше.
* AlterOS 7.5 и выше.
* Amazon Linux 2.
* Astra Linux Common Edition 2.12.
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
* Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
* CentOS 6.7 и выше.
* CentOS 7.2 и выше.
* CentOS Stream 9.
* Debian GNU/Linux 10.1 и выше.
* Debian GNU/Linux 11.
* EMIAS 1.0.
* EulerOS 2.0 SP5.
* LinuxMint 19.2 и выше.
* LinuxMint 20.3 и выше.
* openSUSE Leap 15.0 и выше.
* Oracle Linux 7.3 и выше.
* Oracle Linux 8.0 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.
* Red Hat Enterprise Linux 9.
* Rocky Linux 8.5 и выше.
* SUSE Linux Enterprise Server 12.5 и выше.
* SUSE Linux Enterprise Server 15 и выше.
* Ubuntu 20.04 LTS.
* Ubuntu 22.04 LTS.
* Альт 8 СП Рабочая станция.
* Альт 8 СП Сервер.
* Альт Образование 10.
* Альт Рабочая Станция 10.
* Альт Сервер 10.
* Атлант, сборка Alcyone, версия 2022.02.
* Гослинукс 7.17.
* Гослинукс 7.2.
* РЕД ОС 7.3.
* РОСА "Кобальт" 7.9.
* РОСА "Хром" 12.
* ОСОН "ОСНова".

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

* Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
* EulerOS 2.0 SP8.
* SUSE Linux Enterprise Server 15 SP3.
* Ubuntu 20.04 LTS.
* Альт 8 СП Сервер.
* РЕД ОС 7.3.

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;
* получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация);
* создание файлов трассировки при запуске программы;
* получение информации обо всех исполняемых файлах программ, установленных на компьютерах;
* проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;
* сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий.

# 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 Server 2022;
* 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;
* включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов.
* 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 5.0–13 (включая Android 12L, исключая Go Edition);
* iOS 10–16 или iPadOS 13–15;

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 Enterprise 2015 LTSB 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 2019 LTSC 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 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 11 Home 64-разрядная;
* Microsoft Windows 11 Pro 64-разрядная;
* Microsoft Windows 11 Enterprise 64-разрядная;
* Microsoft Windows 11 Education 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 2008 R2 with Standard Service Pack 1 и выше 64-разрядная;
* Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;
* Windows Server 2012 Server Core 64-разрядная;
* Windows Server 2012 Datacenter 64-разрядная;
* Windows Server 2012 Essentials 64-разрядная;
* Windows Server 2012 Foundation 64-разрядная;
* Windows Server 2012 Standard 64-разрядная;
* Windows Server 2012 R2 Server Core 64-разрядная;
* Windows Server 2012 R2 Datacenter 64-разрядная;
* Windows Server 2012 R2 Essentials 64-разрядная;
* Windows Server 2012 R2 Foundation 64-разрядная;
* Windows Server 2012 R2 Standard 64-разрядная;
* Windows Server 2016 Datacenter (LTSB) 64-разрядная;
* Windows Server 2016 Standard (LTSB) 64-разрядная;
* Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
* Windows Server 2019 Standard 64-разрядная;
* Windows Server 2019 Datacenter 64-разрядная;
* Windows Server 2019 Core 64-разрядная;
* Windows Server 2022 Standard 64-разрядная;
* Windows Server 2022 Datacenter 64-разрядная;
* Windows Server 2022 Core 64-разрядная;
* Windows Storage Server 2012 64-разрядная;
* Windows Storage Server 2012 R2 64-разрядная;
* Windows Storage Server 2016 64-разрядная;
* Windows Storage Server 2019 64-разрядная.

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

* VMware vSphere 6.7;
* VMware vSphere 7.0;
* 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;
* Microsoft Hyper-V Server 2022 64-разрядная;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x;
* Parallels Desktop 17;
* 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 (требуются дополнительные действия);
* Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуются дополнительные действия);
* Microsoft Azure SQL Database;
* Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;
* MySQL 5.7 Community 32-разрядная/64-разрядная;
* MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;
* MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;
* MariaDB 10.5.x 32-разрядная/64-разрядная;
* MariaDB 10.4.x 32-разрядная/64-разрядная;
* MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;
* MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
* MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
* MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

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;
* возможность управления развертыванием ОС Windows через консоль управления;
* 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;
* наличие возможности совместного подключения к рабочему столу Windows (Windows Desktop Sharing);
* 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.
* возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами.
* автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
* возможность развернуть Сервер администрирования как систему высокой доступности;
* возможность устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети.

# 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:

* Debian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная;
* Debian GNU/Linux 10.х (Buster) 32-разрядная/64-разрядная;
* Debian GNU/Linux 9.х (Stretch) 32-разрядная/64-разрядная;
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
* Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная;
* CentOS 7.x 64-разрядная;
* Red Hat Enterprise Linux Server 8.x 64-разрядная;
* Red Hat Enterprise Linux Server 7.x 64-разрядная;
* SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная;
* SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная;
* Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Astra Linux Special Edition 1.6 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Astra Linux Common Edition 2.12 64-разрядная;
* Альт Сервер 10 64-разрядная;
* Альт Сервер 9.2 64-разрядная;
* Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
* Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная;
* Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная;
* Oracle Linux 7 64-разрядная;
* Oracle Linux 8 64-разрядная;
* РЕД ОС 7.3 Сервер 64-разрядная;
* РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

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

* VMware vSphere 6.7.
* VMware vSphere 7.0;
* 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;
* Microsoft Hyper-V Server 2022 64-разрядная;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x;
* Parallels Desktop 17;
* Виртуальная машина на основе Kernel. Поддерживает следующие операционные системы:
* Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
* Альт Сервер 10 64-разрядная;
* Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Debian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная;
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
* РЕД ОС 7.3 Сервер 64-разрядная;
* РЕД ОС 7.3 Сертифицированная редакция 64-разрядная

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

* MySQL 5.7 Community 32-разрядная/64-разрядная;
* MySQL 8.0 32-разрядная/64-разрядная;
* MariaDB 10.5.x 32-разрядная/64-разрядная;
* MariaDB 10.4.x 32-разрядная/64-разрядная;
* MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;
* MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
* MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

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;
* возможность обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;
* возможность с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;
* возможность использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули.

# 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 модулю предотвращения утечек данных:

|  |  |
| --- | --- |
| **Состав системы:** | Серверная часть должна содержать в составе: модуль опроса агентов, модуль оповещений, модуль формирования отчетов; сервер индексации и контекстного поиска; клиентский модуль (агент), консоль администрирования, консоль просмотра данных (консоль специалиста безопасности). |
| **Описание и требуемый функционал:** | Программа должна состоять из следующих частей - пользовательской части (агента), серверной части, консоли администрирования и консоли просмотра данных.  Агентская часть программы должна устанавливаться на контролируемый компьютер и производить сбор и накопление информации о действиях пользователя. Временное хранение накопленных данных должно осуществляться на контролируемом ПК в каталоге с защитой доступа в зашифрованных файлах. По запросу серверной части эти данные должны пересылаться на сервер, а на контролируемом ПК очищаться.  Частота сбора данных должна настраиваться. Обмен между агентом и сервером должен производиться в зашифрованном виде. Также должна быть возможность установления пароль на доступ сервера к агентам.  Серверная часть программы должна работать под ОС Windows без необходимости применять средства виртуализации.  Комплекс должен обеспечивать функционал:  - Регистрировать нажатия клавиш на клавиатуре.  - Делать снимки экранов мониторов (скриншоты) через заданный промежуток времени и по смене окон программ. Также иметь возможность выполнения снимков в черно-белом режиме и с возможностью изменения качества выполняемых снимков.  - Иметь возможность для отдельных программ настроить частоту выполнения скриншотов, отличающуюся от основной. - Запоминать запуск и закрытие программ, иметь функцию блокировки запуска запрещенных программ.  - Перехватывать e-mail полученные/отправленные по протоколам POP3/POP3S, SMTP/SMTPS, IMAP.  - Сохранять копию текстовой переписки в Skype, а также голосовых сообщений.  - Сохранять текст, копируемый в буфер обмена.  - Запоминать сообщения, отправляемые в соц. сетях, и файлы, выкладываемые в интернет.  - Запоминать запросы в поисковых системах (yandex, google)  - Осуществлять мониторинг файловой системы: создание, удаление, переименование, изменение файлов.  - Перехватывать посещённые сайты.  - Отслеживать включение/выключение компьютера, вход/выход пользователей в windows.  - Определять подключение и отключение USB носителей информации и иметь возможность выполнения «теневой копии» скопированных на данный носитель файлов.  - Иметь функцию блокировки клиентов облачных дисков и выполнения «теневой копии» файлов, копируемых на облачные диски.  - Иметь функцию блокировки подключения таких классов устройств, как USB накопители, CD/DVD Rom, флоппи - дисководы.  - Вести список разрешенных USB накопителей, подключение которых к контролируемым компьютерам разрешать. Подключение остальных USB накопителей блокировать.  - Запоминать установку и удаление программ.  - Запоминать информацию об отправленных на печать документах и сохранять сам образ напечатанного документа в формате pdf.  - Отслеживать работу с общими ресурсами компьютера  - Иметь возможность "активного оповещения" администратора о таких событиях на контролируемых компьютерах, как подключение/отключение USB носителей информации, установка/удаление программ, копирование файлов на съемный накопитель, отправку письма через браузер.  - Оповещать администратора об изменении состава комплектующих контролируемого компьютера (CPU, оперативная память, жесткие диски);  - Иметь функцию обнаружения нестандартной активности пользователей. - Иметь возможность формирования отчетов, в т.ч. по расписанию.  - Иметь возможность оповещения специалиста безопасности о нарушениях установленных в программе правил безопасности: напрямую на консоль просмотра данных, на e-mail, на мессенджер Telegram.  - Иметь функцию полнотекстового поиска ключевых фраз по всем собранным с контролируемых компьютеров данным, в том числе по файлам теневой копии, вложениям почты, распечатанным на принтер документам.  - Иметь функцию поиска регулярных выражений в собранных данных (номеров телефонов, паспортных данных, ИНН и т.д.)  - иметь функцию «конфиденциального каталога», внутри которого можно работать с файлами только в заданных программах. При этом разрешать изменение файлов внутри данного каталога, но запрещать их копирование наружу данного каталога. Опционально запрещать печать таких документов на принтер или копирование в буфер обмена.  - Вся собранная с контролируемых компьютеров информация должна храниться централизованно в базе данных на сервере.  - Должна быть возможность удалённого управление настройками агента, возможность удалённо запустить/остановить мониторинг.  - Возможность удаленной установки/удаления агентов: как средствами консоли администрирования, так и средствами групповых политик при помощи инсталляционного пакета msi.  - Информация от агента должна передаваться по сети до модуля сбора в зашифрованном виде.  - Возможность отправки текстовых сообщений на компьютер пользователя.  Лицензирование системы должно происходить по количеству компьютеров, за которыми ведется наблюдение в один момент времени. Т.е. должна быть возможность одни компьютеры с мониторинга снимать, и вместо них ставить на мониторинг другие, так, чтобы при этом не требовалось расширение лицензии. Лицензия должна предоставляться на бессрочный период. |
| **Требование по используемой СУБД** | Хранение собранных данных должно осуществляться на сервере в базе данных под управлением бесплатной СУБД Firebird. |
| **Требования к консоли администрирования** | Консоль администрирования должна позволять производить дистанционную установку/удаление агентов, а также их настройку (какие виды информации накапливать на контролируемом ПК). Также с ее помощью должна производиться настройка доступа специалистов безопасности к накопленным данным. Для каждого специалиста безопасности (его учетной записи, созданной в административной части программы) должна быть возможность указать с каких конкретно компьютеров данный специалист может просматривать данные и какие именно данные. В консоли администрирования должна быть возможность производить задание правил безопасности:  - Список запрещенных для использования приложений и выбор, производить ли блокировку запуска таких программ.  - Список запрещенных веб сайтов  - Список запрещенных файлов, действия с которыми являются нарушением безопасности  - Ключевые слова для поиска в переписке.  - Правила выявления подозрительной активности  Также через консоль администрирования должна быть возможность производить подписку учетных записей специалистов безопасности на оповещения о нарушении заданных политик безопасности.  Вход и в консоль администрирования должен осуществляться после обязательной авторизации.  Консоль администрирования должна быть реализована классическим приложением Windows, без необходимости использовать браузер. |
| **Требования к консоли просмотра данных** | Данная консоль должна позволять авторизованным пользователям осуществлять просмотр собранных данных. При этом каждому пользователю должна предоставляться только та информация и по тем контролируемым компьютерам, к которым ему разрешен доступ.  Консоль просмотра данных должна содержать в своем составе мастер отчетов, позволяющий сформировать как отчеты по текущим данным, так и аналитические отчеты, содержащие статистику использования контролируемых компьютеров, программ, посещения веб сайтов, использования принтеров, переписки через программы обмена сообщениями.  При нарушении заданных политик безопасности, сообщение об этом должно отображается в специальном окне.  Вход и в консоль просмотра данных должен осуществляться после обязательной авторизации.  Консоль просмотра данных должна быть реализована классическим приложением Windows, без необходимости использовать браузер. |
| **Требование к системе оповещения** | Оповещение специалистов безопасности о нарушении заданных политик безопасности должно производиться напрямую в консоль просмотра данных, на e-mail и/или на мессенджер Telegram. |
| **Требования к подсистеме отчетов** | Комплекс должен содержать в своем составе планировщик отчетов, позволяющий настроить выполнение групп отчетов по выбранным компьютерам за заданные промежутки времени по расписанию. Должен обеспечивать при необходимости отправку сформированных отчетов на e-mail. |
| **Язык интерфейса** | Программа должна иметь русскоязычный интерфейс |
| **Технические требования:** | 1. Серверы:  Центральный процессор: 2-х ядерный с частотой ядра 3,2 ГГц или выше;  Оперативная память: не менее 4 ГБ (рекомендуется 8 ГБ)  Жесткий диск: не менее 300 ГБ. Свободное место на диске требуется из расчета 600 МБ на каждый контролируемый компьютер для хранения данных за 30 дней.  Поддерживаемые операционные системы: Windows 2008/7/8.1/10/2012/2016 (32- или 64-разрядный выпуск)  Открытые порты TCP/IP: входящие - 7657, 3050, 6587; исходящий – 47658.  2. Контролируемые рабочие станции:  Центральный процессор: с частотой 2,4 ГГц или выше  Оперативная память: не менее 1 ГБ (рекомендуется от 2 ГБ)  Жесткий диск: не менее 200 МБ свободного пространства на диске.  Поддерживаемые операционные системы: Windows XP/2003/2008/Vista/7/8.1/10 (32- или 64-разрядный выпуск)  Сеть: Локальная сеть от 100 Мбит, обслуживающая все рабочие станции и сервер.  Открытые порты TCP/IP: входящий – 47658; исходящий - 7657. |

# Приложение № 2 к техническому заданию

# Характеристики

Продление действующей лицензии на антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса – Расширенный на срок 1 год с учётом имеющейся у Заказчика лицензии № 1B08-220427-011616-833-1407

Комплектация:

- ключевой файл для активации программного обеспечения;

Страна происхождения программного обеспечения: Российская Федерация

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 / Ultimate / Enterprise Service Pack 1 и выше;
* Windows 8 Professional / Enterprise (32 / 64-разрядная);
* Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
* Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise;
* Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise

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 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;
  + наличие инструмента мониторинга сети по протоколам TCP и UDP;
  + возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
  + возможность установки ограничение длительности выполнения задачи;
  + возможность ставить задачи проверки в очередь, если проверка уже выполняется.
  + 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;
  + возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий)
  + возможность создавать служебную учетную запись агента аутентификации при шифровании диска;
  + поддержка стороннего поставщика учетных данных ADSelfService Plus для работы SSO при полнодисковом шифровании.

# 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), Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2;
* Windows MultiPoint Server 2011 (64-разрядная);
* Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;
* Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2016 Essentials / Standard / Datacenter;
* Windows Server 2019 Essentials / Standard / Datacenter;
* Windows Server 2022.

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;
* поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов.
* возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
* возможность установки ограничения длительности выполнения задачи;
* возможность ставить задачи проверки в очередь, если проверка уже выполняется.

# 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 10.14 - 12;

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;
* возможность установки расширений из командной строки с помощью новой команды kav;
* возможность задавать исключения при проверке указанных областей на уровне перехватов файловых операций;
* возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены.

# 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:

* CentOS 6.7 и выше.
* Debian GNU/Linux 10.1 и выше.
* Debian GNU/Linux 11.
* Mageia 4.
* Red Hat Enterprise Linux 6.7 и выше.
* Альт 8 СП Рабочая Станция.
* Альт 8 СП Сервер.
* Альт Образование 10.
* Альт Рабочая Станция 10.

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

* AlmaLinux OS 8 и выше.
* AlmaLinux OS 9 и выше.
* AlterOS 7.5 и выше.
* Amazon Linux 2.
* Astra Linux Common Edition 2.12.
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
* Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
* CentOS 6.7 и выше.
* CentOS 7.2 и выше.
* CentOS Stream 9.
* Debian GNU/Linux 10.1 и выше.
* Debian GNU/Linux 11.
* EMIAS 1.0.
* EulerOS 2.0 SP5.
* LinuxMint 19.2 и выше.
* LinuxMint 20.3 и выше.
* openSUSE Leap 15.0 и выше.
* Oracle Linux 7.3 и выше.
* Oracle Linux 8.0 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.
* Red Hat Enterprise Linux 9.
* Rocky Linux 8.5 и выше.
* SUSE Linux Enterprise Server 12.5 и выше.
* SUSE Linux Enterprise Server 15 и выше.
* Ubuntu 20.04 LTS.
* Ubuntu 22.04 LTS.
* Альт 8 СП Рабочая станция.
* Альт 8 СП Сервер.
* Альт Образование 10.
* Альт Рабочая Станция 10.
* Альт Сервер 10.
* Атлант, сборка Alcyone, версия 2022.02.
* Гослинукс 7.17.
* Гослинукс 7.2.
* РЕД ОС 7.3.
* РОСА "Кобальт" 7.9.
* РОСА "Хром" 12.
* ОСОН "ОСНова".

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

* Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
* EulerOS 2.0 SP8.
* SUSE Linux Enterprise Server 15 SP3.
* Ubuntu 20.04 LTS.
* Альт 8 СП Сервер.
* РЕД ОС 7.3.

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;
* получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация);
* создание файлов трассировки при запуске программы;
* получение информации обо всех исполняемых файлах программ, установленных на компьютерах;
* проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;
* сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий.

# 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 Server 2022;
* 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;
* включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов.
* 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 5.0–13 (включая Android 12L, исключая Go Edition);
* iOS 10–16 или iPadOS 13–15;

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 Enterprise 2015 LTSB 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 2019 LTSC 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 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 11 Home 64-разрядная;
* Microsoft Windows 11 Pro 64-разрядная;
* Microsoft Windows 11 Enterprise 64-разрядная;
* Microsoft Windows 11 Education 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 2008 R2 with Standard Service Pack 1 и выше 64-разрядная;
* Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;
* Windows Server 2012 Server Core 64-разрядная;
* Windows Server 2012 Datacenter 64-разрядная;
* Windows Server 2012 Essentials 64-разрядная;
* Windows Server 2012 Foundation 64-разрядная;
* Windows Server 2012 Standard 64-разрядная;
* Windows Server 2012 R2 Server Core 64-разрядная;
* Windows Server 2012 R2 Datacenter 64-разрядная;
* Windows Server 2012 R2 Essentials 64-разрядная;
* Windows Server 2012 R2 Foundation 64-разрядная;
* Windows Server 2012 R2 Standard 64-разрядная;
* Windows Server 2016 Datacenter (LTSB) 64-разрядная;
* Windows Server 2016 Standard (LTSB) 64-разрядная;
* Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
* Windows Server 2019 Standard 64-разрядная;
* Windows Server 2019 Datacenter 64-разрядная;
* Windows Server 2019 Core 64-разрядная;
* Windows Server 2022 Standard 64-разрядная;
* Windows Server 2022 Datacenter 64-разрядная;
* Windows Server 2022 Core 64-разрядная;
* Windows Storage Server 2012 64-разрядная;
* Windows Storage Server 2012 R2 64-разрядная;
* Windows Storage Server 2016 64-разрядная;
* Windows Storage Server 2019 64-разрядная.

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

* VMware vSphere 6.7;
* VMware vSphere 7.0;
* 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;
* Microsoft Hyper-V Server 2022 64-разрядная;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x;
* Parallels Desktop 17;
* 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 (требуются дополнительные действия);
* Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуются дополнительные действия);
* Microsoft Azure SQL Database;
* Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;
* MySQL 5.7 Community 32-разрядная/64-разрядная;
* MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;
* MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;
* MariaDB 10.5.x 32-разрядная/64-разрядная;
* MariaDB 10.4.x 32-разрядная/64-разрядная;
* MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;
* MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
* MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
* MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

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;
* возможность управления развертыванием ОС Windows через консоль управления;
* 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;
* наличие возможности совместного подключения к рабочему столу Windows (Windows Desktop Sharing);
* 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.
* возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами.
* автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
* возможность развернуть Сервер администрирования как систему высокой доступности;
* возможность устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети.

# 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:

* Debian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная;
* Debian GNU/Linux 10.х (Buster) 32-разрядная/64-разрядная;
* Debian GNU/Linux 9.х (Stretch) 32-разрядная/64-разрядная;
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
* Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная;
* CentOS 7.x 64-разрядная;
* Red Hat Enterprise Linux Server 8.x 64-разрядная;
* Red Hat Enterprise Linux Server 7.x 64-разрядная;
* SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная;
* SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная;
* Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Astra Linux Special Edition 1.6 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Astra Linux Common Edition 2.12 64-разрядная;
* Альт Сервер 10 64-разрядная;
* Альт Сервер 9.2 64-разрядная;
* Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
* Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная;
* Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная;
* Oracle Linux 7 64-разрядная;
* Oracle Linux 8 64-разрядная;
* РЕД ОС 7.3 Сервер 64-разрядная;
* РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

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

* VMware vSphere 6.7.
* VMware vSphere 7.0;
* 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;
* Microsoft Hyper-V Server 2022 64-разрядная;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x;
* Parallels Desktop 17;
* Виртуальная машина на основе Kernel. Поддерживает следующие операционные системы:
* Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
* Альт Сервер 10 64-разрядная;
* Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Debian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная;
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
* РЕД ОС 7.3 Сервер 64-разрядная;
* РЕД ОС 7.3 Сертифицированная редакция 64-разрядная

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

* MySQL 5.7 Community 32-разрядная/64-разрядная;
* MySQL 8.0 32-разрядная/64-разрядная;
* MariaDB 10.5.x 32-разрядная/64-разрядная;
* MariaDB 10.4.x 32-разрядная/64-разрядная;
* MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;
* MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
* MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

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;
* возможность обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;
* возможность с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;
* возможность использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули.

# 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.

1. Данная Форма заполняется и подписывается всеми физическими лицом, чьи персональные данные предоставляются в составе заявки на участие в настоящем запросе котировок и приложениях к ней, а также документах, входящих в состав заявки Участника. Предоставленные персональные данные должны соответствовать действующему законодательству РФ «О персональных данных». Отсутствие настоящего документа не является основанием для отклонения Заявки. [↑](#footnote-ref-1)