**КОНТРАКТ №**

**Оказание услуг по продлению лицензии Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 100-149 Node 1 Year Renewal License**

Идентификационный код закупки

г. Челябинск «\_\_\_»\_\_\_\_\_\_2021 г.

Комитет дорожного хозяйства города Челябинска, именуемый в дальнейшем «Заказчик», в лице Председателя Комитета Кучитарова Рината Галиевича, на основании Положения, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Подрядчик», с другой стороны, вместе именуемые «Стороны» и каждый в отдельности «Сторона», с соблюдением требований Гражданского [кодекса](consultantplus://offline/ref=C36B03DBA536EA525D662381ACE9C394D57D9026D42F5DE9B445103EA5DDE2H) Российской Федерации, на основании пункта 4 части 1 статьи 93 Федерального закона от 05.04.2013 № 44 «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», заключили настоящий Контракт о нижеследующем:

1. **ПРЕДМЕТ КОНТРАКТА**

1.1. Предметом настоящего контракта является**: Оказание услуг по продлению лицензии Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition 100-149 Node 1 Year Renewal License** (далее – антивирусное программное обеспечение, Услуга).

1.2. Исполнитель обладает правом на передачу неисключительных лицензионных прав, установленных Правообладателем в соответствии с требованиями статей 1233, 1235, 1236, 1238 Гражданского кодекса Российской Федерации (Авторизационные письма, партнерские Сертификаты, письма от Дистрибьютора и т.п.), на использование антивирусного программного обеспечения на основании лицензионного договора № 434/ЛК-2015-Л от 01.01.2015 г. между Правообладателем и ООО «МОНТ»; лицензионного договора между ООО «МОНТ» и ООО «БинЕкс»: № RU-66-019014-2021-2-L от 24.03.2021 г..

1.3. Заказчик поручает, а Исполнитель обязуется оказать Услугу в соответствии с техническим заданием (Приложение №1), являющимся неотъемлемой частью настоящего контракта, условиями настоящего контракта, действующим законодательством Российской Федерации, с надлежащим качеством и в сроки, предусмотренные настоящим Контрактом.

1.4. В случае использования технических средств защиты использования антивирусного программного обеспечения, Исполнитель обязуется предоставить Заказчику возможность использования антивирусного программного обеспечения, в том числе путём сообщения ему необходимых ключей доступа и паролей, по адресу, указанному п. 5 Контракта.

**2. ЦЕНА КОНТРАКТА**

2.1. Цена контракта составляет ( ) рубля копеек, **НДС (БЕЗ НДС)**

В случае, если Исполнителем по данному контракту является юридическое лицо или физическое лицо, в том числе зарегистрированное в качестве индивидуального предпринимателя, сумма, подлежащая уплате (цена контракта) заказчиком, уменьшается на размер налогов, сборов и иных обязательных платежей в бюджеты бюджетной системы Российской Федерации, связанных с оплатой контракта, если в соответствии с законодательством Российской Федерации о налогах и сборах такие налоги, сборы и иные обязательные платежи подлежат уплате в бюджеты бюджетной системы Российской Федерации Заказчиком.

2.2. Валютой для установления цены контракта и расчетов с Исполнителем является Российский рубль.

2.3. Источник финансирования: Бюджет города Челябинска.

2.4. Цена Контракта включает в себя: стоимость оказания Услуг, все затраты и издержки необходимые для оказания услуг, а также налоги, сборы и другие обязательные платежи, взимаемые с Исполнителя в связи с исполнением контракта.

2.5. Цена контракта является твердой, определяется на весь срок исполнения контракта и не может изменяться в ходе его исполнения за исключением следующих случаев:

2.5.1. Цена контракта может быть снижена по соглашению Сторон без изменения предусмотренного контрактом объема Услуг, качества оказываемых Услуг и иных условий исполнения контракта;

2.5.2. Настоящий контракт предусматривает право Заказчика по согласованию с Исполнителем в ходе исполнения контракта изменить не более чем на десять процентов объема предусмотренных контрактом Услуг при изменении потребности в таких Услугах.

При выполнении дополнительного объема Услуг Заказчик по согласованию с Исполнителем вправе изменить первоначальную цену контракта пропорционально дополнительному объему таких Услуг, исходя из установленной в контракте цены единицы Услуги, но не более чем на десять процентов цены контракта, а при внесении соответствующих изменений в контракт в связи с сокращением потребности в соответствующем объеме Услуг Стороны обязаны уменьшить цену контракта указанным образом.

**3. ПОРЯДОК РАСЧЕТОВ**

3.1. Оплата за оказание услуг осуществляется по цене, установленной п. 2.1 контракта.

3.2. Оплата за оказанные услуги осуществляется по безналичному расчету путем перечисления Заказчиком денежных средств на расчетный счет Исполнителя, указанный в контракте, на основании выставленного Исполнителем счета или счета-фактуры (при наличии) в течение 30 рабочих дней после подписания Сторонами Акта сдачи-приемки оказанных услуг.

По согласованию с Заказчиком Исполнитель имеет право оформить и осуществить обмен документами о приемке товаров (работ, услуг).

3.3. Обязательство Заказчика по оплате за оказанные Услуги считается исполненным с момента списания денежных средств со счета Заказчика.

**4. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

**4.1. Заказчик вправе:**

4.1.1. Требовать от Исполнителя надлежащего исполнения обязательств в соответствии с условиями контракта.

4.1.2. Требовать от Исполнителя представления надлежащим образом оформленных документов, подтверждающих исполнение обязательств в соответствии с условиями контракта.

4.1.3. Запрашивать у Исполнителя информацию о ходе и состоянии исполнения обязательств Исполнителя по настоящему контракту.

**4.2. Заказчик обязан:**

4.2.1. Выполнять указания и рекомендации Исполнителя относительно функционирования и эксплуатации Продукта.

4.2.2. Своевременно принять и оплатить оказанные Услуги в соответствии с условиями настоящего контракта.

4.2.3. Своевременно предоставлять разъяснения и уточнения по запросам Исполнителя в части оказания Услуг в соответствии с условиями настоящего контракта.

4.2.4. В случае просрочки исполнения Исполнителем обязательств, предусмотренных контрактом, а также в иных случаях ненадлежащего исполнения Исполнителем обязательств, предусмотренных контрактом, направлять Исполнителю требование об уплате в добровольном порядке сумм неустойки, предусмотренных настоящим контрактом, за неисполнение (ненадлежащее исполнение) Исполнителем своих обязательств по настоящему контракту.

4.2.5. В случае неуплаты Исполнителем в добровольном порядке предусмотренных настоящим контрактом сумм неустойки за неисполнение своих обязательств взыскивать их в судебном порядке либо производить оплату по контракту в соответствии с п.9.6 настоящего контракта.

4.2.6. При направлении в суд искового заявления с требованиями о расторжении контракта одновременно заявлять требования об оплате неустойки, рассчитанной в соответствии с положениями законодательства и условиями контракта, если на момент подачи такого заявления имелись основания для взыскания неустойки и такая неустойка не была оплачена в соответствии с п.9.6 настоящего контракта либо отсутствовала возможность для оплаты по контракту в соответствии с п.9.6 настоящего контракта.

4.2.7. Не допускать расторжения контракта по соглашению сторон, если на дату подписания соглашения имелись основания требовать от Исполнителя оплаты неустойки за неисполнение или ненадлежащее исполнение обязательств, предусмотренных контрактом, и Исполнителем такая неустойка не оплачена, в том числе и в порядке, предусмотренном п.9.6 настоящего контракта.

4.2.8. В случае если окончание срока действия контракта повлекло прекращение обязательств Сторон по контракту, но при этом имеются основания требовать от Исполнителя оплаты неустойки за неисполнение или ненадлежащее исполнение обязательств по контракту:

4.2.8.1. В течение 10 дней с даты окончания срока действия контракта направить Исполнителю претензионное письмо с требованием оплаты в течение 30 дней с даты получения претензионного письма неустойки, рассчитанной в соответствии с требованиями законодательства и условиями контракта за весь период просрочки исполнения.

4.2.8.2. При неоплате в установленный срок Исполнителем неустойки не позднее 10 дней с даты истечения срока для оплаты неустойки, указанного в претензионном письме (в случае если оплата по контракту не была произведена в соответствии с п.9.6 настоящего контракта), направить в суд исковое заявление с требованием об оплате неустойки, рассчитанной в соответствии с требованиями законодательства и условиями контракта.

4.2.9. Провести экспертизу для проверки предоставленных Исполнителем результатов оказания Услуг, предусмотренных контрактом, в части их соответствия условиям контракта.

4.2.10. Осуществлять контроль за исполнением Исполнителем условий контракта в соответствии с законодательством Российской Федерации.

**4.3. Исполнитель вправе:**

4.3.1. Требовать подписания в соответствии с условиями контракта Заказчиком акта сдачи-приемки оказанных Услуг по настоящему контракту.

4.3.2. Требовать своевременной оплаты за оказываемые Услуги в соответствии с условиями настоящего контракта.

4.3.3. Направлять Заказчику запросы и получать от него разъяснения и уточнения по вопросам оказания Услуг в рамках настоящего контракта.

**4.4. Исполнитель обязан:**

4.4.1. Оказать Услуги, предусмотренные настоящим контрактом, в соответствии с Техническим заданием и в сроки, установленные в Разделе 5 «Сроки, место и условия оказания Услуг» контракта.

4.4.2. Своевременно представить Заказчику достоверную информацию о ходе исполнения своих обязательств по контракту, в том числе о сложностях, возникших при исполнении контракта.

4.4.3. По окончании оказания Услуг передать результаты оказанных Услуг Заказчику в порядке и в сроки, определенные Разделом 6 «Порядок сдачи-приемки Услуг» настоящего контракта.

4.4.4. Представить Заказчику сведения об изменении своего фактического местонахождения в срок не позднее 5 дней со дня соответствующего изменения. В случае непредставления в установленный срок уведомления об изменении адреса фактическим местонахождением Исполнителя будет считаться адрес, указанный в настоящем контракте.

4.4.5. Гарантировать качество оказанных Услуг.

**5. СРОКИ, МЕСТО И УСЛОВИЯ ОКАЗАНИЯ УСЛУГ**

5.1. Срок оказания Услуг – продление лицензии в течение 15 календарных дней с момента заключения контракта; использование антивирусного программного обеспечения в течение 12 месяцев с момента активации лицензии.

5.2. Место оказания Услуг - 454008, г. Челябинск, Комсомольский пр-т, 4, Комитет дорожного хозяйства города Челябинска,

5.3. Условия оказания Услуг – в соответствии с Техническим заданием (Приложение №1 к настоящему контракту).

1. **ПОРЯДОК СДАЧИ-ПРИЕМКИ УСЛУГ**

6.1. Приемка оказанных Услуг по настоящему контракту на соответствие их требованиям, установленным в настоящем контракте, осуществляется на основании Акта сдачи-приемки оказанных услуг.

6.2. Для проверки оказанных Исполнителем Услуг, предусмотренных контрактом, в части их соответствия условиям контракта Заказчик обязан провести экспертизу. Экспертиза результатов, предусмотренных контрактом, может проводиться Заказчиком своими силами или к ее проведению могут привлекаться эксперты, экспертные организации на основании контрактов, заключенных в соответствии с Федеральным законом № 44-ФЗ.

В случае, если по результатам такой экспертизы установлены нарушения требований контракта, не препятствующие приемке оказанных Услуг, в заключении могут содержаться предложения об устранении данных нарушений, в том числе с указанием срока их устранения.

Заказчик вправе не отказывать в приемке оказанных Услуг в случае выявления несоответствия таких услуг условиям контракта, если выявленное несоответствие не препятствует приемке Услуг и устранено Исполнителем.

6.3. Исправление недостатков, допущенных Исполнителем и выявленных при оказании услуг, осуществляется в срок, согласованный с Заказчиком, и за счет Исполнителя.

6.4. По решению Заказчика для приемки результата услуг по контракту может создаваться приемочная комиссия, которая состоит не менее чем из пяти человек.

В случае привлечения Заказчиком для проведения экспертизы экспертов, экспертных организаций при принятии решения о приемке или об отказе в приемке результата услуг приемочная комиссия должна учитывать отраженные в заключении по результатам указанной экспертизы предложения экспертов, экспертных организаций, привлеченных для ее проведения.

6.5. Заказчик принимает результат услуг по контракту в течение 5 дней со дня получения Акта сдачи-приемки оказанных услуг и направляет Исполнителю подписанный Акт сдачи-приемки оказанных услуг или мотивированный отказ от приемки и подписания Акта сдачи-приемки оказанных услуг с указанием перечня выявленных недостатков, который составляется, в том числе, с учетом отраженного в заключении по результатам экспертизы предложения экспертов, экспертных организаций, если таковые привлекались для ее проведения.

6.6. Исполнитель обязуется своими силами и за свой счет устранить замечания Заказчика в течение 5 рабочих дней с момента получения уведомления об обнаружении факта несоответствия исполненных Исполнителем обязательств условиям настоящего контракта.

6.7. В случае если Акт сдачи-приемки оказанных услуг подписан не уполномоченными лицами, отсутствует расшифровка подписей, акт сдачи-приемки оказанных услуг считается неподписанным, а Услуги непринятыми.

1. **ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА**
   1. Исполнитель гарантирует действительность и полноту объема передаваемого права на использование программного обеспечения в соответствии с Технической частью.

**9. ОТВЕТСТВЕННОСТЬ СТОРОН**

9.1. За неисполнение или ненадлежащее исполнение своих обязательств по Контракту Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

9.2. В случае просрочки исполнения Заказчиком обязательств, предусмотренных Контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Заказчиком обязательств, предусмотренных Контрактом, Исполнитель вправе потребовать уплаты неустоек (штрафов, пеней).

9.2.1. Пеня начисляется за каждый день просрочки исполнения Заказчиком обязательства, предусмотренного Контрактом, начиная со дня, следующего после дня истечения установленного настоящим контрактом срока исполнения обязательства. Такая пеня устанавливается в размере одной трехсотой действующей на дату уплаты пеней ключевой ставки Центрального банка Российской Федерации от не уплаченной в срок суммы.

9.3. В случае просрочки исполнения Исполнителем обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, Исполнитель уплачивает Заказчику неустойку (штраф, пени).

9.3.1. Пеня начисляется за каждый день просрочки исполнения Исполнителем обязательства, предусмотренного контрактом, начиная со дня, следующего после дня истечения установленного контрактом срока исполнения обязательства, и устанавливается контрактом в размере одной трехсотой действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от цены контракта (отдельного этапа исполнения контракта), уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных контрактом (соответствующим отдельным этапом исполнения контракта) и фактически исполненных Исполнителем.

9.3.2. Штрафы начисляются за неисполнение или ненадлежащее исполнение Исполнителем обязательств, предусмотренных Контрактом, за исключением просрочки исполнения Исполнителем обязательств (в том числе гарантийных обязательств), предусмотренных Контрактом. Размер штрафа устанавливается в порядке, установленном постановлением № 1042-ПП РФ от 30.08.2017, в размере:

10 процентов цены Контракта (этапа) в случае, если цена Контракта (этапа) не превышает 3 млн. рублей;

9.3.3. Если закупка осуществляется у субъекта малого предпринимательства, социально ориентированной некоммерческой организации, то за каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, размер штрафа устанавливается в размере 1 процента цены Контракта (этапа), но не более 5000,00 рублей и не менее 1000.00 рублей.

9.4. Общая сумма начисленных штрафов за неисполнение или ненадлежащее исполнение Исполнителем обязательств, предусмотренных Контрактом, не может превышать цену Контракта.

9.5. Общая сумма начисленных штрафов за ненадлежащее исполнение Заказчиком обязательств, предусмотренных Контрактом, не может превышать цену Контракта.

9.6. В случае неисполнения или ненадлежащего исполнения Исполнителем обязательства (в том числе просрочки исполнения обязательства Исполнителем), предусмотренного Контрактом, Заказчик вправе произвести оплату по Контракту за вычетом соответствующего размера неустойки (штраф, пени) или удержать сумму неустойки (штраф, пени) из денежных средств, внесенных в качестве обеспечения исполнения Контракта.

9.7. В случае если Заказчик понес убытки вследствие ненадлежащего исполнения Исполнителем своих обязательств по Контракту, Исполнитель обязан возместить такие убытки Заказчику независимо от уплаты неустойки.

9.8. Уплата неустойки и возмещение убытков, связанных с ненадлежащим исполнением Сторонами своих обязательств по Контракту, не освобождают нарушившую условия контракта Сторону от исполнения взятых на себя обязательств.

9.9. Сторона освобождается от уплаты неустойки (штрафа, пени), если докажет, что неисполнение или ненадлежащее исполнение обязательства, предусмотренного Контрактом, произошло вследствие непреодолимой силы или по вине другой Стороны.

9.10. В случае расторжения контракта в связи с ненадлежащим исполнением Исполнителем своих обязательств (в том числе по соглашению Сторон), последний в течение 5 (пяти) рабочих дней с даты расторжения Контракта или подписания соглашения о расторжении Контракта уплачивает Заказчику неустойку, определенную в соответствии с п. 9.3 настоящего контракта.

**10. КОНФИДЕНЦИАЛЬНОСТЬ**

10.1. Стороны в течение срока действия настоящего контракта, а также в течение трёх лет по окончании его действия, обязуются обеспечить конфиденциальность любой информации и данных, получаемых друг от друга в связи с исполнением настоящего контракта (в том числе персональных данных), за исключением информации и данных, являющихся общедоступными (далее - конфиденциальная информация). Каждая из Сторон обязуется не разглашать конфиденциальную информацию третьим лицам (за исключением Правообладателя) без получения предварительного письменного согласия Стороны, являющейся владельцем конфиденциальной информации.

10.2. Стороны обязуются принимать все разумные меры для защиты конфиденциальной информации друг друга от несанкционированного доступа третьих лиц, в том числе:

- хранить конфиденциальную информацию исключительно в предназначенных для этого местах, исключающих доступ к ней третьих лиц;

- ограничивать доступ к конфиденциальной информации, в том числе для сотрудников, не имеющих служебной необходимости в ознакомлении с данной информацией.

10.3. Стороны гарантируют полное соблюдение всех условий обработки, хранения и использования полученных персональных данных, согласно Федеральному закону от 27.07.2006 № 152‑ФЗ «О персональных данных».

10.4. Стороны обязаны незамедлительно сообщить друг другу о допущенных ими либо ставшим им известным фактах разглашения или угрозы разглашения, незаконном получении или незаконном использовании конфиденциальной информации третьими лицами.

10.5. Стороны не вправе в одностороннем порядке прекращать охрану конфиденциальной информации, предусмотренной настоящим контрактом, в том числе в случае своей реорганизации или ликвидации в соответствии с гражданским законодательством.

10.6. Под разглашением конфиденциальной информации в рамках настоящего контракта понимается действие или бездействие одной из Сторон контракта, в результате которого конфиденциальная информация становится известной третьим лицам в отсутствие согласия на это владельца конфиденциальной информации. При этом форма разглашения конфиденциальной информации третьим лицам (устная, письменная, с использованием технических средств и др.) не имеет значения.

10.7. Не является нарушением конфиденциальности предоставление конфиденциальной информации по законному требованию правоохранительных и иных уполномоченных государственных органов и должностных лиц в случаях и в порядке, предусмотренных применимым законодательством.

10.8. В случае раскрытия конфиденциальной информации указанным органам и/или лицам Сторона, раскрывшая конфиденциальную информацию, письменно уведомляет владельца конфиденциальной информации о факте предоставления такой информации, ее содержании и органе, которому предоставлена конфиденциальная информация, не позднее двух рабочих дней с момента раскрытия конфиденциальной информации.

10.9. В случае неисполнения Сторонами обязательств, предусмотренных настоящим разделом, Сторона, допустившее такое нарушение, обязуется возместить все причиненные этим убытки, в том числе упущенную выгоду, в течение 5 рабочих дней после получения соответствующего письменного требования пострадавшей Стороны.

**12. СРОК ДЕЙСТВИЯ И ПОРЯДОК ИЗМЕНЕНИЯ КОНТРАКТА**

12.1. Контракт вступает в силу с момента его заключения Сторонами и действует по 31.12.2022 г., в части оплаты по контракту - до полного исполнения обязательств принятых Сторонами.

12.2. Изменение положений настоящего контракта возможны в случаях, предусмотренных пунктом 6 статьи 161 Бюджетного кодекса Российской Федерации, при уменьшении ранее доведенных до Заказчика как получателя бюджетных средств лимитов бюджетных обязательств, при этом Заказчик в порядке, предусмотренном ст. 95 Федерального закона № 44-ФЗ, в случае, если не достигнуто соглашение о снижении цены контракта без сокращения объемов Услуг и (или) об изменении сроков исполнения контракта, обеспечивает соглашение с Исполнителем новых условий контракта, в том числе цены и (или) сроков исполнения контракта и (или) объемов Услуг, предусмотренных контрактом.

12.3.Иные изменения и дополнения настоящего контракта возможны по соглашению Сторон в рамках действующего законодательства в сфере осуществления закупок. Все изменения и дополнения оформляются в письменном виде путем подписания Сторонами дополнительных соглашений к контракту. Дополнительные соглашения к контракту являются его неотъемлемой частью и вступают в силу с момента их подписания Сторонами.

**13. ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРОВ**

13.1. В случае возникновения любых противоречий, претензий и разногласий, а также споров, связанных с исполнением настоящего контракта, Стороны предпринимают усилия для урегулирования таких противоречий, претензий и разногласий в добровольном порядке.

13.2. В случае невыполнения Сторонами своих обязательств и не достижения взаимного согласия споры по настоящему контракту разрешаются в Арбитражном суде Челябинской области.

**14. ПОРЯДОК РАСТОРЖЕНИЯ КОНТРАКТА**

14.1. Настоящий контракт может быть расторгнут:

- по соглашению Сторон;

- в судебном порядке;

- в связи с односторонним отказом Заказчика от исполнения Контракта по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения отдельных видов обязательств.

14.2. Заказчик вправе принять решение об одностороннем отказе от исполнения контракта в следующих случаях:

14.2.1. В случае просрочки начала оказания Услуг Исполнителем более чем на 5 дней.

14.2.2. В иных случаях, предусмотренных действующим законодательством.

14.3. Заказчик обязан принять решение об одностороннем отказе от исполнения контракта если в ходе исполнения контракта установлено, что Исполнитель не соответствует установленным документацией о закупке требованиям к участникам закупки или предоставил недостоверную информацию о своем соответствии указанным требованиям, что позволило ему стать победителем определения Исполнителя.

14.4. Расторжение контракта в связи с односторонним отказом Заказчика от исполнения контракта осуществляется в порядке, предусмотренном статьей 95 Федерального закона № 44-ФЗ.

14.5. Расторжение контракта по соглашению сторон производится Сторонами путем подписания соответствующего соглашения о расторжении.

В случае расторжения настоящего контракта по соглашению Сторон Стороны подписывают акт сверки расчётов, отображающий расчеты Сторон за период исполнения контракта до момента его расторжения, а также объём Услуг, фактически оказанных Исполнителем Заказчику.

14.6. Исполнитель не вправе принять решение об одностороннем расторжении настоящего контракта, если Заказчиком не нарушаются условия настоящего контракта.

**16. ПРОЧИЕ УСЛОВИЯ**

16.1. Приложение к контракту является его неотъемлемой частью.

16.2. Все уведомления Сторон, связанные с исполнением настоящего контракта, направляются в письменной форме по почте заказным письмом по фактическому адресу Стороны, указанному в настоящем контракте, а также могут быть направлены с использованием факсимильной связи, электронной почты с последующим предоставлением оригинала или в электронно-цифровой форме, подписанные в таком случае квалифицированной электронной подписью. В случае направления уведомлений с использованием почты уведомления считаются полученными Стороной в день фактического получения, подтвержденного отметкой почты. В случае отправления уведомлений посредством факсимильной связи и электронной почты уведомления считаются полученными Стороной в день их отправки.

16.3. Во всем, что не предусмотрено настоящим контрактом, Стороны руководствуются действующим законодательством Российской Федерации.

**17. ПРИЛОЖЕНИЯ К КОНТРАКТУ**

17.1. Приложение 1. Техническое задание

**18. МЕСТОНАХОЖДЕНИЯ И БАНКОВСКИЕ РЕКВИЗИТЫ СТОРОН**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| ЗАКАЗЧИК | | ПОДРЯДЧИК | | |
| Комитет дорожного хозяйства города Челябинска,  454008, г. Челябинск, Комсомольский пр-т, 4, ИНН 7451227906, КПП 744801001,  ОТДЕЛЕНИЕ ЧЕЛЯБИНСК БАНКА РОССИИ//УФК по Челябинской области г. Челябинск  БИК: 017501500  ЛС 0347100698Б  ОГРН 1067451013882  р/сч 03231643757010006900  к/сч 40102810645370000062  Тел. (351)791-19-67  Факс (351) 796-57-05  E-mail: udh@cheladmin.ru | |  | | |
| Председатель Комитета дорожного хозяйства города Челябинска | |  | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Р.Г. Кучитаров | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| МП | | МП | | |

Приложение № 1

к контракту

№\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Техническое задание**

**Оказание услуг по продлению лицензии Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 100-149 Node 1 Year Renewal License**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**Наименование:** Оказание услуг по продлению неисключительных (лицензионных) прав использования антивирусного программного обеспечения.

Заказчик заявляет ***продление*** неисключительных (лицензионных) прав антивирусного программного обеспечения на уже приобретенный и используемый программный продукт Kaspersky Endpoint Security для бизнеса – Стандартный 100-149, сроком на 1 год. Количество рабочих мест 100 (продлеваемая лицензия №1096-201218-114423-983-97) (Лицензирование количества компонентов защиты рабочих станций и файловых серверов должно быть универсальным и ограничиваться только общим количеством защищаемых объектов). Участник размещения заказа не вправе предложить эквивалент, т.к. предложение другого антивирусного программного обеспечения не обеспечит совместимости с существующим у Заказчика программным обеспечением.

Согласно пп. 1 части 1 статьи 33 ФЗ 44 "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" заказчик заявляет о необходимости предоставления в рамках услуги средств защиты информации, совместимых с существующим у Заказчика программным обеспечением Kaspersky Security Center.

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование | Единица  измерения | Количество |
| 1 | Продление действующей лицензии Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 100-149 Node 1 year Renewal License | шт. | 100 |

# Общие требования

Антивирусные средства должны включать:

* программные средства антивирусной защиты для рабочих станций Windows;
* программные средства антивирусной защиты для рабочих станций MacOS;
* программные средства антивирусной защиты для рабочих станций и серверов Linux;
* программные средства антивирусной защиты для файловых серверов Windows;
* программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов);
* программные средства централизованного управления, мониторинга и обновления;
* обновляемые базы данных сигнатур вредоносных программ и атак;
* эксплуатационную документацию на русском языке.

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке.

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

# Требования к программным средствам антивирусной защиты для рабочих станций Windows

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

* Windows 7 Home / Professional / Enterprise (32 / 64-разрядная);
* Windows 8 Professional / Enterprise (32 / 64-разрядная);
* Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
* Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядная).

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

* + антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
  + антивирусное сканирование по расписанию;
  + антивирусное сканирование подключаемых устройств;
  + эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
  + нейтрализации действий активного заражения;
  + анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
  + анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
  + блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
  + откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
  + ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
  + облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
  + антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
  + защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
  + фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
  + проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
  + блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
  + распознавания и блокировку фишинговых и небезопасных сайтов;
  + встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
  + защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
  + защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
  + контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
  + создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
  + контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
  + управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
  + записи в журнал событий о записи и/или удалении файлов на съемных дисках;
  + назначение приоритета для правил доступа к устройствам с файловой системой;
  + контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
  + защиты от атак типа BadUSB;
  + запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
  + защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
  + управления параметрами Kaspersky Endpoint Security через доверенные программы удаленного администрирования;
  + установки только выбранных компонентов программного средства антивирусной защиты;
  + централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
  + запуска задач по расписанию и/или сразу после запуска приложения;
  + гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
  + ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
  + проверки целостности антивирусной программы;
  + добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
  + импорта и экспорта списков правил и исключений в XML-формат;
  + наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
  + наличие защищенного хранилища для отчетов о работе антивируса;
  + включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
  + интеграции с Windows Defender Security Center;
  + наличие поддержки Antimalware Scan Interface (AMSI);
  + наличие поддержки Windows Subsystem for Linux (WSL);
  + защитить паролем восстановление объектов из резервного хранилища;
  + ограничения сетевого трафика в том случае, если подключение к интернету является лимитным.

# Требования к программным средствам антивирусной защиты для серверов Windows

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

* Windows Small Business Server 2011 Essentials / Standard (64-разрядная);
* Windows MultiPoint Server 2011 (64-разрядная);
* Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная);
* Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядная);
* Windows Server 2012 Foundation / Essentials / Standard (64-разрядная);
* Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная);
* Windows Server 2016 (64-разрядная) (с ограничениями);
* Windows Server 2019 (64-разрядная) (с ограничениями).

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

* антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
* 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.

# Требования к программным средствам антивирусной защиты для рабочих станций Mac

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

* macOS 10.13, 10.14, 10.15 или 11.0;

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

* резидентный антивирусный мониторинг;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* автоматическое обновление антивирусных баз по расписанию;
* резервное копирование зараженных файлов перед их удалением, для возможности восстановления;
* эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
* защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* проверку сетевого трафика, передаваемого через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик);
* контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

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

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

* Ubuntu 16.04 LTS и выше;
* Red Hat® Enterprise Linux® 6.7 и выше;
* CentOS 6.7 и выше;
* Debian GNU / Linux 10;
* Linux Mint 19 и выше;
* Альт Линукс 9 Рабочая станция;
* Гослинукс 6.6;
* Mageia 4.

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

* Ubuntu 18.04 LTS и выше;
* Red Hat Enterprise Linux 8.0 и выше;
* CentOS 8.0 и выше;
* Debian GNU / Linux 10.1 и выше;
* OracleLinux 8 и выше;
* SUSE® Linux Enterprise Server 15 и выше;
* Альт Линукс 9 Образование;
* Amazon Linux AMI;
* Linux Mint 19 и выше;
* Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды);
* Astra Linux Common Edition «Орел» 2.12;
* ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем;
* Гослинукс 7.2;
* AlterOS 7.5 и выше;
* Pardus OS 19.1.

Полный список программных требований доступен в онлайн-справке - <https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU/196583.htm>.

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

# 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 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Windows Server 2008 Core / Standard / Enterprise
* …

64-разрядных операционных систем Microsoft Windows

* Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2008 Core Standard / Enterprise /
* Windows Hyper-V Server 2012;
* Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
* Windows Storage Server 2012 R2;
* Windows Server 2016 Essentials / Standard / Datacenter;
* Windows Hyper-V Server 2016;
* Windows Server 2019 Essentials / Standard / Datacenter;
* Windows Hyper-V Server 2019.
* ...

Полный список программных требований доступен в онлайн-справке - <https://support.kaspersky.com/KSWS/11/ru-RU/155510.htm>.

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

* антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
* защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
* непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
* анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* проверки контейнеров Microsoft Windows;
* защиты от эксплуатирования уязвимостей в памяти процессов;
* должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
* добавлять процессы в список защищаемых;
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
* настройки проверки критических областей сервера в качестве отдельной задачи;
* регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;
* продолжать антивирусное сканирование в фоновом режиме;
* наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
* ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
* интеграции с SIEM системами;
* указания количества рабочих процессов антивируса вручную;
* отключить графический интерфейс;
* наличие удаленной и локальной консоли управления;
* управления параметрами антивируса из командной строки;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;
* контроль устройств, в том числе сетевых карт и модемов;

# Требования к программным средствам антивирусной защиты мобильных устройств

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

* Android 4.2-11.0.
* iOS 10.0-14.0 или iPadOS.

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

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

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

* удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;
* отправки команды блокирования и удаления данных;
* создавать групповые политики безопасности мобильных устройств;
* удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM;
* получать отчеты и статистику о работе мобильных устройств пользователей;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervised mode;
* централизованного управления с помощью единой консоли управления;
* наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari или Game Center, на управляемом устройстве.

# Требования к программным средствам централизованного управления, мониторинга и обновления

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением определенных версий операционных систем, поддерживать установку на виртуальных платформах и функционировать с различными СУБД.

Список программных требований доступен в онлайн-справке - <https://support.kaspersky.com/ksc/12/ru-RU/96255.htm>

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.

# 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 телефону, 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

|  |  |
| --- | --- |
| Председатель Комитета дорожного хозяйства города Челябинска |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Р.Г. Кучитаров | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| МП | МП |