**ЛИЦЕНЗИОННЫЙ (СУБЛИЦЕНЗИОННЫЙ) ДОГОВОР № 22161207003/37**

**о предоставлении права использования программного обеспечения Kaspersky Endpoint Security для бизнеса – Стандартный**

**для ЧУЗ «РЖД-Медицина г. Калининград»**

г. Калининград «\_\_\_»\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, именуемое в дальнейшем **«Лицензиар (Сублицензиар)** в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ с одной стороны, и Частное учреждение здравоохранения «Больница «РЖД-Медицина» города Калининград» (ЧУЗ «РЖД-Медицина» г. Калининград»), именуемое в дальнейшем **«Лицензиат»**, в лице, Главного врача Сиглаевой Людмилы Михайловны, действующего на основании Устава, с другой стороны, вместе именуемые «Стороны», заключили настоящий Договор о нижеследующем:

**1. ПРЕДМЕТ ДОГОВОРА**

1.1. Лицензиар (Сублицензиар) обязуется предоставить Лицензиату право использования объекта интеллектуальной собственности - **программное обеспечение Kaspersky Endpoint Security для бизнеса – Стандартный**, (далее - Программное обеспечение) в порядке, предусмотренном настоящим Договором, а Лицензиат обязуется уплатить Лицензиару (Сублицензиару) обусловленное настоящим Договором вознаграждение.

1.2. Лицензиар (Сублицензиар) гарантирует, что является правообладателем неисключительного права на Программное обеспечение.

1.3. Принадлежность исключительного права на Объект интеллектуальной собственности Лицензиару (Сублицензиару) подтверждается: лицензионным сертификатом, подтверждающим, что Лицензиар (Сублицензиар) является авторизированным партнером АО «Лаборатория Касперского» и вправе распространять программные продукты и сервисы (услуги), разработанные АО «Лаборатория Касперского».

1.4. В целях идентификации Объекта интеллектуальной собственности Лицензиар (Сублицензиар) передает Лицензиату в *1* (одном) экземпляре ключи и сертификат продлеваемой лицензии, согласно Требованиям к Программному обеспечению (Приложение № 1 к настоящему Договору), в электронном виде по Акту приемки-передачи объекта интеллектуальной собственности по форме, согласованной в Приложении № 2 к настоящему Договору.

Лицензиар (Сублицензиар) передает Лицензиату Программное обеспечение в электронном виде, по адресу электронной почты: it\_rzd\_klgd@mail.ru в срок: не позднее 30 (тридцати) календарных дней в полном объеме с момента заключения договора.

1.5. Срок действия предоставляемых прав на использование Программного обеспечения составляет: не менее 24 месяцев.

**2. ПРАВА, ПЕРЕДАВАЕМЫЕ ЛИЦЕНЗИАТУ**

2.1. Лицензиату предоставляется право использования Программного обеспечения:

- без сохранения за Лицензиаром (Сублицензиаром) права выдавать лицензии другим лицам (исключительная лицензия).

2.1.1. Лицензиату предоставляется право использования Программного обеспечения следующими способами: в электронном виде, по адресу электронной почты: it\_rzd\_klgd@mail.ru.

2.2. По настоящему Договору использование Лицензиатом Программного обеспечения допускается на территории всего мира.

2.3. Лицензиат вправе заключать сублицензионный договор без дополнительного получения письменного одобрения по каждому такому факту.

2.4. Лицензиат обязан предоставить Лицензиару (Сублицензиару), по первому требованию (требование должно быть оформлено в письменном виде), в течение 5 (пяти) рабочих дней со дня направления такого требования, отчет в письменном виде о результатах использования объекта интеллектуальной собственности или средства индивидуализации, согласно условиям настоящего Договора.

**3. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

3.1. Лицензиар (Сублицензиар) обязуется:

3.1.1. Передать Лицензиату Программное обеспечение, свободным от прав третьих лиц, в состоянии, позволяющем его использование на условиях настоящего Договора, в течение десяти дней с момента заключения настоящего Договора.

3.1.2. Передать Лицензиату экземпляр Программного обеспечения  *в электронном виде*, содержащем ключи в форматах .txt, .key, а так же лицензионный сертификат к Программному обеспечению.

3.1.3. Предоставлять информацию об изменениях в составе владельцев Лицензиара (Сублицензиара), включая реального приобретателя выгоды, и (или) в исполнительных органах Лицензиар (Сублицензиар)а не позднее, чем через 5 (пять) календарных дней после таких изменений.

3.2. Лицензиар (Сублицензиар) вправе:

3.2.1. В случае нарушения Лицензиатом условий (способов) использования прав на Программное обеспечение по настоящему Договору, лишить Лицензиата лицензии на использование прав на Программное обеспечение.

3.2.2. Настоящий Договор предоставляет Лицензиату право на использование Программного обеспечения с сохранением за Лицензиаром (Сублицензиаром) права выдачи лицензий другим лицам. Лицензиат может использовать экземпляр Программного обеспечения только в пределах тех прав и теми способами, которые предусмотрены настоящим Договором.

3.3. Лицензиат обязуется:

3.3.1. Выплатить Лицензиару (Сублицензиару) вознаграждение за предоставление (передачу) Лицензиату прав на использование Программного обеспечения в порядке и сроки, установленные настоящим Договором.

3.3.2. Использовать Программное обеспечение исключительно способами, предусмотренными настоящим Договором.

3.3.3. Строго придерживаться и не нарушать условий настоящего Договора, а также обеспечить конфиденциальность полученной при сотрудничестве с Лицензиаром (Сублицензиаром) коммерческой и технической информации.

3.4. Лицензиат вправе:

3.4.1. Предоставить право использования Программного обеспечения в соответствии с настоящим Договором другому лицу.

3.4.2. Отказаться от исполнения настоящего Договора, если Лицензиар (Сублицензиар) в нарушение условий настоящего Договора отказывается передать Лицензиату право на использование Программного обеспечения по настоящему Договору.

**4.** **ВОЗНАГРАЖДЕНИЕ И СРОК ОПЛАТЫ**

4.1. Вознаграждение Лицензиара (Сублицензиара), за предоставление Лицензиату прав на использование Программного обеспечения по Договору составляет: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) рублей \_\_\_ копеек (НДС не облагается на основании пп. 26 п. 2 ст. 149 НК Российской Федерации).

п.4.2. Оплата вознаграждения по настоящему Договору производится Лицензиатом в течение 30 (тридцати) дней после подписания Сторонами Акта приемки-передачи объекта интеллектуальной собственности.

4.3. Датой исполнения обязательства Лицензиата по оплате считается дата списания денежных средств с расчетного счета Лицензиата.

4.4. Проценты на сумму оплаты по настоящему Договору не начисляются и не уплачиваются.

**5. ОТВЕТСТВЕННОСТЬ СТОРОН**

5.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

5.2. Использование Лицензиатом Программного обеспечения способом, не предусмотренным настоящим Договором, либо по прекращении действия настоящего Договора, либо иным образом за пределами прав, предоставленных Лицензиату по настоящему Договору, влечет ответственность за нарушение исключительного права на результат интеллектуальной деятельности, установленную законодательством.

5.3. При существенном нарушении Лицензиатом обязанности уплатить Лицензиару (Сублицензиару) в установленный срок вознаграждение за предоставление лицензии Лицензиар (Сублицензиар) может в одностороннем порядке отказаться от настоящего Договора и потребовать возмещения убытков, причиненных расторжением настоящего Договора.

5.4. Лицензиар (Сублицензиар) несет ответственность за несвоевременную передачу права пользования и (или) Документации на право пользования, возникшую не по вине Лицензиата. В случае совершения обозначенного в настоящем пункте Договора нарушения настоящего Договора Лицензиар (Сублицензиар) выплачивает неустойку в размере 1/365 ключевой ставки Центрального банка Российской Федерации от размера вознаграждения указанного в п.4.1. за каждый день просрочки.

5.5. Лицензиар (Сублицензиар) несет ответственность за качество предоставленных материальных носителей, содержащих экземпляры ПО (если ПО предоставляется на материальных носителях), а также за наличие Документации на русском языке.

**6. КОНФИДЕНЦИАЛЬНОСТЬ**

6.1. Условия настоящего Договора и дополнительных соглашений к нему, а также все материалы и (или) сведения, принадлежащие Лицензиару (Сублицензиару) в отношении Программного обеспечения, ставшие известными Лицензиату, конфиденциальны и не подлежат разглашению.

6.2. Лицензиат обязан сохранять конфиденциальность сведений, касающихся Программного обеспечения и иных прав Лицензиара (Сублицензиара), в течение всего срока действия настоящего Договора.

6.3. Лицензиар (Сублицензиар) имеет право с момента заключения настоящего Договора и в течение срока его действия в любой момент потребовать от Лицензиата заключения отдельного соглашения о неразглашении конфиденциальной информации, касающейся предмета настоящего Договора, а Лицензиат обязан заключить его и соблюдать условия.

**7. РАЗРЕШЕНИЕ СПОРОВ**

7.1. Все споры, возникающие при исполнении настоящего Договора, решаются Сторонами путем переговоров, которые могут проводиться в том числе, путем отправления писем по почте, обмена факсимильными сообщениями.

7.2. Если Стороны не придут к соглашению путем переговоров, все споры рассматриваются в претензионном порядке. Срок рассмотрения претензии – три недели с даты получения претензии.

7.3. В случае если споры не урегулированы Сторонами путем переговоров и в претензионном порядке, то они передаются заинтересованной Стороной в Арбитражный суд Калининградской области.

**8. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ**

8.1. Ни одна из Сторон не несет ответственности перед другой Стороной за неисполнение или ненадлежащее исполнение обязательств по настоящему Договору, обусловленное действием обстоятельств непреодолимой силы, то есть чрезвычайных и не предотвратимых обстоятельств, в том числе в условиях объявленной или фактической войны, гражданскими волнениями, эпидемиями, блокадами, эмбарго, пожарами, землетрясениями, наводнениями и другими природными стихийными бедствиями, а также изданием актов государственных органов.

8.2. Свидетельство, выданное торгово-промышленной палатой или иным компетентным органом, является достаточным подтверждением наличия и продолжительности действия обстоятельств непреодолимой силы.

8.3. Сторона, которая не исполняет свои обязательства вследствие действия обстоятельств непреодолимой силы, должна, по возможности, в трехдневный срок известить другую Сторону о таких обстоятельствах и их влиянии на исполнение обязательств по настоящему Договору.

8.4. Если обстоятельства непреодолимой силы действуют на протяжении 3 (трех) последовательных месяцев для обеих Сторон, настоящий Договор может быть расторгнут по инициативе любой из Сторон, при этом инициирующая Сторона обязана произвести расчеты с другой Стороной по фактически исполненному до наступления форс-мажорных обстоятельств после прекращения форс-мажорных обстоятельств.

**9.АНТИКОРРУПЦИОННАЯ ОГОВОРКА**

9.1. При исполнении своих обязательств по настоящему Договору Стороны, их аффилированные лица, работники или посредники не выплачивают, не предлагают выплатить и не разрешают выплату каких-либо денежных средств или ценностей, прямо или косвенно, любым лицам для оказания влияния на действия или решения этих лиц с целью получить какие-либо неправомерные преимущества или для достижения иных неправомерных целей.

При исполнении своих обязательств по настоящему Договору Стороны, их аффилированные лица, работники или посредники не осуществляют действия, квалифицируемые применимым для целей настоящего Договора законодательством как дача/получение взятки, коммерческий подкуп, а также иные действия, нарушающие требования применимого законодательства и международных актов о противодействии коррупции.

9.2. В случае возникновения у Стороны подозрений, что произошло или может произойти нарушение каких-либо положений [пункта 9.1](#p283) настоящего Договора, соответствующая Сторона обязуется уведомить об этом другую Сторону в письменной форме. В письменном уведомлении Сторона обязана сослаться на факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений [пункта 9.1](#p283) настоящего Договора другой Стороной, ее аффилированными лицами, работниками или посредниками.

Каналы уведомления Лицензиата о нарушениях каких-либо положений пункта 9.1. настоящего Договора: (4012)601-353, RailwayHospital@mail.ru.

Каналы уведомления Лицензиара (Сублицензиара) о нарушениях каких-либо положений пункта 9.1. настоящего Договора: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, официальный сайт \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (для заполнения специальной формы).

Сторона, получившая уведомление о нарушении каких-либо положений [пункта 9.1](#p283). настоящего Договора, обязана рассмотреть уведомление и сообщить другой Стороне об итогах его рассмотрения в течение 20 (двадцати) рабочих дней с даты получения письменного уведомления.

9.3. Стороны гарантируют осуществление надлежащего разбирательства по фактам нарушения положений [пункта 9.1](#p283). настоящего Договора с соблюдением принципов конфиденциальности и применение эффективных мер по предотвращению возможных конфликтных ситуаций. Стороны гарантируют отсутствие негативных последствий как для уведомившей Стороны в целом, так и для конкретных работников уведомившей Стороны, сообщивших о факте нарушений.

9.4. В случае подтверждения факта нарушения одной Стороной положений [пункта 9.1](#p283). настоящего Договора и/или неполучения другой Стороной информации об итогах рассмотрения уведомления о нарушении в соответствии с [пунктом 9.2](#p285). настоящего Договора, другая Сторона имеет право расторгнуть настоящий Договор в одностороннем внесудебном порядке путем направления письменного уведомления не позднее чем за 60 (шестьдесят) календарных дней до даты прекращения действия настоящего Договора.

**10. СРОК ДЕЙСТВИЯ ДОГОВОРА**

Настоящий Договор вступает в силу с момента его подписания и действует до «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ года включительно.

**11. НАЛОГОВАЯ ОГОВОРКА**

11.1.Лицензиар (Сублицензиар) гарантирует, что:

зарегистрирован в ЕГРЮЛ надлежащим образом;

его исполнительный орган находится и осуществляет функции управления по месту регистрации юридического лица, и в нем нет дисквалифицированных лиц;

располагает персоналом, имуществом и материальными ресурсами, необходимыми для выполнения своих обязательств по настоящему Договору, а в случае привлечения подрядных организаций (соисполнителей) принимает все меры должной осмотрительности, чтобы подрядные организации (соисполнители) соответствовали данному требованию;

располагает лицензиями, необходимыми для осуществления деятельности и исполнения обязательств по настоящему Договору, если осуществляемая по настоящему Договору деятельность является лицензируемой;

является членом саморегулируемой организации, если осуществляемая по настоящему Договору деятельность требует членства в саморегулируемой организации;

ведет бухгалтерский учет и составляет бухгалтерскую отчетность в соответствии с законодательством Российской Федерации и нормативными правовыми актами по бухгалтерскому учету, представляет годовую бухгалтерскую отчетность в налоговый орган;

ведет налоговый учет и составляет налоговую отчетность в соответствии с законодательством Российской Федерации, субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления, своевременно и в полном объеме представляет налоговую отчетность в налоговые органы;

не допускает искажения сведений о фактах хозяйственной жизни (совокупности таких фактов) и объектах налогообложения в первичных документах, бухгалтерском и налоговом учете, в бухгалтерской и налоговой отчетности, а также не отражает в бухгалтерском и налоговом учете, в бухгалтерской и налоговой отчетности факты хозяйственной жизни выборочно, игнорируя те из них, которые непосредственно не связаны с получением налоговой выгоды;

своевременно и в полном объеме уплачивает налоги, сборы и страховые взносы;

отражает в налоговой отчетности по НДС все суммы НДС, предъявленные Лицензиату – *данный абзац исключается в случае освобождения от уплаты НДС при заключении настоящего Договора;*

лица, подписывающие от его имени первичные документы и счета-фактуры, имеют на это все необходимые полномочия и доверенности.

11.2. Если Лицензиар (Сублицензиар) нарушит гарантии (любую одну, несколько или все вместе), указанные в пункте 11.1. настоящего Договора, и это повлечет:

предъявление налоговыми органами требований к Лицензиату об уплате налогов, сборов, страховых взносов, штрафов, пеней, отказ в возможности признать расходы для целей налогообложения прибыли или включить НДС в состав налоговых вычетов и(или)

предъявление третьими лицами, купившими у Лицензиара (Сублицензиара) услуги, имущественные права, являющиеся предметом настоящего Договора, требований к Лицензиату о возмещении убытков в виде начисленных по решению налогового органа налогов, сборов, страховых взносов, пеней, штрафов, а также возникших из-за отказа в возможности признать расходы для целей налогообложения прибыли или включить НДС в состав налоговых вычетов, то Лицензиар (Сублицензиар) обязуется возместить Лицензиату убытки, который последний понес вследствие таких нарушений.

11.3. Лицензиар (Сублицензиар) в соответствии со ст. 406.1. Гражданского кодекса Российской Федерации, возмещает Лицензиату все убытки последнего, возникшие в случаях, указанных в пункте 11.2. настоящего Договора. При этом факт оспаривания или не оспаривания налоговых доначислений в налоговом органе, в том числе вышестоящем, или в суде, а также факт оспаривания или не оспаривания в суде претензий третьих лиц не влияет на обязанность Исполнителя возместить имущественные потери.

**12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

12.1. Во всем остальном, что не предусмотрено настоящим Договором, Стороны будут руководствоваться действующим законодательством Российской Федерации.

12.2. Любые изменения и дополнения к настоящему Договору действительны при условии, если они совершены в письменной форме и подписаны Сторонами или надлежаще уполномоченными на то представителями Сторон.

12.3. Стороны обязуются своевременно извещать друг друга об изменении своих реквизитов.

12.4. Все уведомления, сообщения, согласования в рамках исполнения настоящего Договора могут быть направлены другой Стороне по электронному адресу, указанному в реквизитах настоящего Договора. Документы, направляемые в отсканированном виде, содержащие печать и подпись Стороны, в последующем должны быть направлены в оригинале по адресу указанному получателем в реквизитах Договора. В любом из случаев, срок получения такого документа, письма, уведомления, начинает течь с момента направления электронного сообщения. Сторона, указавшая неверный электронный адрес или не указавшая его вообще, не вправе ссылаться на несвоевременное получение уведомления, сообщения и прочей письменной документации от другой Стороны. В этом случае, уведомления, сообщения и прочая переписка будет считаться принятыми к исполнению другой Стороной с даты отправления электронного письма.

12.5. Все уведомления и сообщения в рамках настоящего Договора должны направляться Сторонами друг другу в письменной форме.

12.6. Настоящий Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, из которых один находится у Лицензиара (Сублицензиара), второй - у Лицензиата.

12.7. К настоящему Договору прилагаются:

12.7.1. Требование к программному обеспечению (Приложение № 1)

12.7.2. Форма Акта приемки-передачи объекта интеллектуальной собственности на электронном носителе (Приложение №2).

**13. АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН**

|  |  |
| --- | --- |
| **Лицензиар (Сублицензиар)**Место нахождения: ИНН:КПП:ОГРН:К/С:Банк БИК: Р/С:Электронная почта: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **/\_\_\_\_\_\_\_\_\_\_/** | **Лицензиат****Частное учреждение здравоохранения «Больница «РЖД-Медицина» города Калининград»** ОГРН 1043900824604, ИНН 3908029088, КПП 390601001,ОКПО 73707902, Местонахождение: 236005, Калининградская обл., город Калининград, улица Летняя, д.1, р/с: 40703810820380004163 в Филиале «Центральный» Банка ВТБ (ПАО) в г. Москве к/с 30101810145250000411, БИК 044525411Тел/Факс: 8 (4012) 60-13-53, 60-19-50Еmail: RailwayHospital@mail.ruГлавный врачЧУЗ «РЖД-Медицина» г. Калининград» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Сиглаева Л.М./ |

Приложение № 1

к Договору о предоставлении права использования

программного обеспечения

№ 22161207003/37 от "\_\_" \_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

**Требование к программному обеспечению**

|  |  |
| --- | --- |
| г. Калининград  | "\_\_" \_\_\_\_\_\_\_\_ 20\_\_ г. |

1. **Наименование и описание объекта закупки (функциональные, технические и качественные характеристики, эксплуатационные характеристики объекта закупки), объем и условия оказания услуг, требования к качеству услуг:**

 **1.1. Наименование объекта закупки:** оказание услуг по продлению лицензии Kaspersky Endpoint Security для бизнеса – Стандартный

 **1.2. Описание услуг, объем и условия оказания услуг, требования к качеству услуг:**

|  |  |
| --- | --- |
| **Наименование**  | Продление лицензии пользователя (передача неисключительных прав на использование программ для ЭВМ) ЧУЗ "РЖД-МЕДИЦИНА" Г. КАЛИНИНГРАД"№26FE-180910-144526-7-1559, лицензия на 2 года, программное обеспечение Kaspersky Endpoint Security для бизнеса – Стандартный 50-99 NodeRenewal 2 yearKL4863RAQDR \* |
| **Количество закупаемых товаров, объем работ, услуг** | Лицензия на 70 рабочих мест |
| **Место поставки** | 236005, КАЛИНИНГРАДСКАЯ ОБЛ, КАЛИНИНГРАД Г, ЛЕТНЯЯ УЛ, 1 |
| **Срок (периодичность) передачи неисключительных лицензионных прав** | Поставщик передает неисключительные лицензионные права Заказчику в срок не позднее 30 (тридцати) календарных дней в полном объеме с момента заключения государственного контракта. |
| **Условия поставки товара** | Датой передачи неисключительных лицензионных прав, считается дата подписания Акта приема передачи неисключительных прав, **без претензий**. |
| **Требования по объему и сроку гарантий качества товаров** | Поставщик гарантирует работу ключа на программный продукт в течение 24 месяцев при соблюдении условий лицензионного соглашения. Гарантийные обязательства вступают в силу с момента приема передачи неисключительных прав заказчику. |

\* данное программное обеспечение (далее ПО) не сопровождается словами «или эквивалент», так как необходимо обеспечить взаимодействие указанного ПО с базами данных и другим ПО, которые используются Заказчиком.

**1.3. Технические требования к системе антивирусной защиты: KasperskyEndpointSecurity для бизнеса – Стандартный**

# **Общие требования**

Антивирусные средства должны включать:

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

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

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

# **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;
* возможность 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 (ActiveDirectory 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 ActiveDirectory;
* возможность управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (ActiveDirectory или локальных пользователей/групп), в рамках контроля устройств;
* записи в журнал событий о записи и/или удалении файлов на съемных дисках;
* 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 ActiveDirectory;
* 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;
* 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 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;
* возможность проверки целостности антивирусной программы;
* возможность 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;
* возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей;
* возможностьинтеграциис Windows Defender Security Center;
* наличиеподдержки Antimalware Scan Interface (AMSI);
* наличиеподдержки Windows Subsystem for Linux (WSL);
* возможность защитить паролем восстановление объектов из резервного хранилища.

# **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 2008 Standard / Premium (64-разрядная);
* Windows Small Business Server 2011 Essentials / Standard (64-разрядная);
* Windows MultiPoint Server 2011 (64-разрядная);
* Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная);
* Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядная);
* Windows Server 2012 Foundation / Essentials / Standard (64-разрядная);
* Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная);
* WindowsServer 2016 (64-разрядная) (с ограничениями);
* WindowsServer 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;
* ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
* облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (ActiveDirectory 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;
* 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;
* возможность проверки целостности антивирусной программы;
* возможность 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;
* возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей;
* возможностьинтеграциис Windows Defender Security Center;
* наличиеподдержки Antimalware Scan Interface (AMSI);
* наличиеподдержки Windows Subsystem for Linux (WSL);
* возможность защитить паролем восстановление объектов из резервного хранилища.

# **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 Catalina 10.15;
* macOSMojave 10.14;
* macOSHighSierra 10.13;
* macOSSierra 10.12.

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, GoogleChrome 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 Linux**

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

* Ubuntu 16.04 LTS;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 и выше;
* Debian GNU / Linux 8.6- 8.х;
* Debian GNU / Linux 9.4 – 9.х;
* LinuxMint 18.2 – 18.х;
* LinuxMint 19 (последняя версия);
* Альт Линукс СПТ 7.0.6;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* Лотос;
* Гослинукс 6.6.

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

* Ubuntu 16.04 LTS;
* Ubuntu 18.04 LTS;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 – 6.х;
* CentOS 7.2 – 7.х;
* Debian GNU / Linux 8.6- 8.х;
* Debian GNU / Linux 9.4 – 9.х;
* OracleLinux 7.3 и выше;
* SUSE LinuxEnterpriseServer 15;
* openSUSE 15;
* Альт Линукс СПТ 7.0.6 ;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* AmazonLinux AMI;
* LinuxMint 18.2 и выше;
* LinuxMint 19 (последняя версия);
* Micro Focus Open Enterprise Server 2018;
* AstraLinuxSpecialEdition 1.5 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* AstraLinuxSpecialEdition 1.6 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* Циркон 36КТ;
* Циркон 36СТ;
* ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем;
* ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем;
* ЕМИАС 1.0;
* Гослинукс 6.6;
* Лотос;
* РЕД ОС 7.2.

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;
* 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 (Plaintext);
* наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
* защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
* помещение подозрительных и поврежденных объектов на карантин;
* проверку почтовых баз приложений Microsoft Outlook на наличие вредоносных объектов;
* возможность перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
* возможность управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

**Требования к программным средствам антивирусной защиты 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 спакетомобновлений SP2 иливыше;
* Windows Server 2003 R2 Standard / Enterprise / Datacenter спакетомобновлений SP2 иливыше;
* Windows Server 2008 Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше;
* Windows Server 2008 Core / Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше.

**64-разрядныхоперационныхсистем Microsoft Windows**

* Windows Server 2003 Standard / Enterprise / Datacenter с пакетомобновлений SP2 иливыше;
* Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетомобновлений SP2 иливыше;
* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* Windows Server 2008 Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* Microsoft Small Business Server 2008 Standard / Premium;
* Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* WindowsHyper-VServer 2008 R2 с пакетом обновлений SP1 или выше;
* Microsoft Small Business Server 2011 Essentials / Standard;
* Microsoft Windows MultiPoint™ Server 2011 Standard / Premium;
* Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
* Microsoft Windows MultiPoint Server 2012 Standard / Premium;
* Windows Storage Server 2012;
* Windows Hyper-V Server 2012;
* Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
* Windows Storage Server 2012 R2;
* Windows Hyper-V Server 2012 R2;
* Windows Server 2016 Essentials / Standard / Datacenter;
* Windows Server 2016 MultiPoint;
* Windows Server 2016 Core Standard / Datacenter;
* Microsoft Windows MultiPoint Server 2016;
* Windows Storage Server 2016;
* Windows Hyper-V Server 2016;
* Windows Server 2019 Essentials / Standard / Datacenter;
* Windows Server 2019 Core;
* Windows Storage Server 2019;
* Windows Hyper-V Server 2019.

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 WindowsScriptTechnologies (или ActiveScripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
* анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* возможность проверки контейнеров Microsoft Windows;
* защиты от эксплуатирования уязвимостей в памяти процессов;
* должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
* возможность 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;
* возможность продолжать антивирусное сканирование в фоновом режиме;
* наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
* ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
* возможность интеграции с SIEM системами;
* возможность указания количества рабочих процессов антивируса вручную;
* возможность отключить графический интерфейс;
* наличие удаленной и локальной консоли управления;
* управления параметрами антивируса из командной строки;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил.

**Требования к программным средствам антивирусной защиты для файловых серверов Linux**

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

* Ubuntu 16.04 LTS;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 и выше;
* Debian GNU / Linux 8.6 – 8.х;
* Debian GNU / Linux 9.4 - 9.х;
* LinuxMint 18.2 и выше;
* LinuxMint 19 (последняя версия);
* Альт Линукс СПТ 7.0.6;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* Лотос;
* Гослинукс 6.6.

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

* Ubuntu 16.04 LTS;
* Ubuntu 18.04 LTS;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 – 6.х;
* CentOS 7.2 – 7.х;
* Debian GNU / Linux 8.6 – 8.х;
* Debian GNU / Linux 9.4 - 9.х;
* OracleLinux 7.3 и выше;
* SUSE LinuxEnterpriseServer 15;
* openSUSE 15;
* Альт Линукс СПТ 7.0.6;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* AmazonLinux AMI;
* LinuxMint 18.2 и выше;
* LinuxMint 19 (последняя версия);
* Micro Focus Open Enterprise Server 2018;
* AstraLinuxSpecialEdition 1.5 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* AstraLinuxSpecialEdition 1.6 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* Циркон 36КТ;
* Циркон 36СТ;
* ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем;
* ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем;
* ЕМИАС 1.0;
* Гослинукс 6.6;
* Лотос;
* РЕД ОС 7.2.

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;
* 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 (Plaintext);
* наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
* защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
* помещение подозрительных и поврежденных объектов на карантин;
* проверку почтовых баз приложений Microsoft Outlook
* возможность перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию;
* возможность управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

# Требования к программным средствам антивирусной защиты мобильных устройств

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

* Android 4.4– 10.0;
* AppleiOS 10.0 – 12.

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
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* поддержка белых списков разрешенных сайтов;
* наличие хранилища для изолирования зараженных объектов;
* обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;
* блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;
* поддержка белых списков разрешенных приложений;
* блокировка системных приложений, в рамках контроля запуска приложений;
* возможность отправки команд и push уведомлений через сервис FirebaseCloudMessaging (FCM);
* базовая поддержка AndroidforWork;
* возможность заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
* возможность указать параметры подключения к wi-fi сетям;
* возможность указать обязательные к установке приложения;
* возможность блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factoryreset);
* возможность 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 AppleiOS должны быть реализованы следующие функциональные возможности:

* возможность удаленной настройки параметров iOSMDM-устройств с помощью групповых политик;
* возможность отправки команды блокирования и удаления данных;
* возможность создавать групповые политики безопасности мобильных устройств;
* удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу ExchangeActiveSync\ iOSMDM;
* 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 supervisedmode;
* возможность централизованного управления с помощью единой консоли управления.

# **Требования к программным средствам централизованного управления, мониторинга и обновления**

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

* Microsoft Windows 7 32-разрядная / 64-разрядная;
* Microsoft Windows 8 32 разрядная / 64-разрядная;
* Microsoft Windows 8;1 32-разрядная / 64-разрядная;
* Microsoft Windows 10 32-разрядная / 64-разрядная;
* Windows Server 2008, 2008 R232-разрядная / 64-разрядная;
* Windows Server 2012, 2012 R264-разрядная;
* Windows Server 2016 64-разрядная;
* WindowsServer 2019 Standard, Datacenter.

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

* VMware vSphere 5.5, 6;
* VMware Workstation 12.x Pro;
* Microsoft Hyper-V Server 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2;
* Microsoft Virtual PC 2007 (6.0.156.0);
* Citrix XenServer 6.2, 6.5, 7;
* Parallels Desktop 11 для Mac;
* OracleVMVirtualBox 4.0.4-70112 (поддерживаются гостевые операционные системы Windows).

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

* Microsoft SQL Server 2008 Express 32-разрядная;
* Microsoft SQL 2008 R2 Express 64-разрядная;
* Microsoft SQL 2012 Express, 2014 Express 64-разрядная;
* MicrosoftSQLServer 2008 (все редакции) 32-разрядная / 64-разрядная;
* MicrosoftSQLServer 2008 R2 (все редакции) 64-разрядная;
* Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная;
* MicrosoftSQLServer 2012 (все редакции) 64-разрядная;
* MicrosoftSQLServer 2014 (все редакции) 64-разрядная;
* MicrosoftSQLServer 2016 (все редакции) 64-разрядная;
* Microsoft SQL Server 2017 (для Windows) 64-разрядная;
* Microsoft Azure SQL Database;
* MySQL 5.5 32-разрядная / 64-разрядная (не поддерживаются версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5);
* MySQL Enterprise 5.5 32-разрядная / 64-разрядная;
* MySQL 5.6 32-разрядная / 64-разрядная;
* MySQL Enterprise 5.6 32-разрядная / 64-разрядная;
* MySQL 5.7 32-разрядная / 64-разрядная;
* MySQLEnterprise 5.7 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;
* возможность чтения информации из ActiveDirectory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
* возможность настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OUAD;
* автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OUAD;
* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* 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;
* возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
* возможность 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 ExchangeActiveSync;
* функция управления мобильными устройствами через сервер iOSMDM;
* возможность отправки SMS-оповещений о заданных событиях;
* централизованная установка сертификатов на управляемые мобильные устройства;
* возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
* возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
* построение графических отчетов 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;
* поддержкаинтеграции с Windows сервисом Certificate Authority;
* наличие веб-консоли управления приложением;
* наличие портала самообслуживания пользователей;
* портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
* наличие системы контроля возникновения вирусных эпидемий;
* возможность установки в облачной инфраструктуре Microsoft Azure;
* возможность интеграции по OpenAPI;
* возможность 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 пользователей программных продуктов.

|  |  |
| --- | --- |
| **от Лицензиата** | **от Лицензиара (Сублицензиара)** |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **/\_\_\_\_\_\_\_\_\_\_/** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **/\_\_\_\_\_\_\_\_\_\_/**

Приложение № 2

к Договору о предоставлении права использования

программного обеспечения

№ 22161207003/37 от "\_\_" \_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

*ФОРМА*

**АКТ ПРИЕМКИ-ПЕРЕДАЧИ**

**ОБЪЕКТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ**

***НА ЭЛЕКТРОННОМ НОСИТЕЛЕ***

|  |  |
| --- | --- |
| г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  | "\_\_" \_\_\_\_\_\_\_\_ 20\_\_ г. |
|  |  |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,** именуемое в дальнейшем **«Лицензиар» (Сублицензиар)** в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ с одной стороны, и

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, именуемое в дальнейшем **«Лицензиат»**, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании Устава, с другой стороны, вместе именуемые «Стороны»составили настоящий Акт приемки-передачи объекта интеллектуальной собственности на материальном носителе (далее - Акт) к Договору о предоставлении права использования программного обеспечения № \_\_\_ от "\_\_\_" \_\_\_\_\_\_\_\_\_ 20\_\_ г. (далее - Договор) о нижеследующем:

1.Лицензиар (Сублицензиар) передает объект интеллектуальной собственности: программы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_на материальном носителе в электронном виде \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в количестве *1 (один)* экземпляр, а Лицензиат принимает объект интеллектуальной собственности на материальном носителе.

2. Лицензиар (Сублицензиар) передает Лицензиату *исключительные/неисключительные* права на объект интеллектуальной собственности: программы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в объеме, указанном в пункте 1.1. Договора.

3.  Индивидуальная характеристика объекта интеллектуальной собственности: программное обеспечение.

4. Материальный носитель объекта интеллектуальной собственности осмотрен Лицензиатом и принят в исправном состоянии.

 5. Акт составлен в двух экземплярах, по одному для Лицензиар (Сублицензиар)а и Лицензиата.

**от Лицензиата от Лицензиара (Сублицензиара)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **/\_\_\_\_\_\_\_\_\_\_/** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **/\_\_\_\_\_\_\_\_\_\_/**