**Сублицензионный договор № \_\_\_\_\_\_**

**о предоставлении права использования**

**программного обеспечения**

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

**Частное учреждение здравоохранения «Центральная клиническая больница «РЖД-Медицина»**, именуемое в дальнейшем **«Сублицензиат»,** в лице директора Акчуриной Инны Майильевны, действующей на основании Устава, с одной стороны, и **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, именуемое в дальнейшем **«Лицензиат»**, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, вместе именуемые «Стороны», заключили настоящий Договор о нижеследующем:

1. **ПРЕДМЕТ ДОГОВОРА**

1.1. Лицензиат, с согласия Лицензиара, обязуется предоставить Сублицензиату право использования объекта интеллектуальной собственности - программное обеспечение Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition, (далее - Программное обеспечение) в порядке, предусмотренном настоящим Договором, а Сублицензиат обязуется уплатить Лицензиату обусловленное настоящим Договором вознаграждение.

1.2. Лицензиат гарантирует, что обладает правами на предоставление Сублицензиату права использования Программного обеспечения на условиях настоящего Договора на законном основании, что подтверждается: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1.3. В целях идентификации Объекта интеллектуальной собственности Лицензиат передает Сублицензиату в *1 (одном) экземпляре* Программное обеспечение, согласно Требованиям к Программному обеспечению (Приложение № 1 к настоящему Договору), в электронном виде в формате электронного лицензионного сертификата и ключа активации по Универсальному передаточному документу (далее - УПД)

1.4. Срок действия предоставляемых прав на использование Программного обеспечения составляет: 12 месяцев с даты подписания сторонами передаточного документа, указанного в п.1.3 договора.

**2. ПРАВА, ПЕРЕДАВАЕМЫЕ ЛИЦЕНЗИАТУ**

2.1. Сублицензия, выдаваемая Сублицензиату по настоящему Договору, является простой (неисключительной). За Лицензиатом сохраняется право выдачи сублицензий другим лицам.

2.1.1. Лицензиату предоставляется право использования Программного обеспечения следующими способами: неисключительное право на воспроизведение Программного обеспечения, ограниченное правом инсталляции, копирования и запуска Программного обеспечения в соответствии с лицензионным соглашением для конечного пользователя, на территории России. При этом право на использование Программного обеспечения, в отношении которого предоставляется простая (неисключительная) лицензия, ограничено пределами, предусмотренными лицензионным соглашением для конечного пользователя..

2.2. По настоящему Договору использование Лицензиатом Программного обеспечения допускается на территории: РФ.

2.3. Сублицензиат не вправе заключать с третьими лицами субсублицензионные договоры на передачу прав на Программное обеспечение, без дополнительного согласия Лицензиара.

**3. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

3.1. Лицензиат обязуется:

3.1.1. Передать Сублицензиату Программное обеспечение в состоянии, позволяющем его использование на условиях настоящего Договора, в течение: *10 (десяти) рабочих дней с момента заключения настоящего Договора.*

3.1.2. Передать Сублицензиату экземпляр Программного обеспечения *в формате электронного лицензионного сертификата и ключа активации,* содержащем программу для установки, а также техническую документацию к Программному обеспечению.

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

3.2. Лицензиат вправе:

3.2.1. Требовать своевременного получения вознаграждения в порядке и размере, установленных настоящим Договором.

3.3. Сублицензиат обязуется:

3.3.1. Выплатить Лицензиату вознаграждение за предоставление (передачу) 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 Лицензиатом коммерческой и технической информации.

3.4. Сублицензиат вправе:

3.4.2. Отказаться от исполнения настоящего Договора, если Лицензиат в нарушение условий настоящего Договора отказывается передать Сублицензиату право на использование Программного обеспечения по настоящему Договору, *а также потребовать возврата уплаченной денежной суммы.*

3.4.3. Расторгнуть настоящий Договор в одностороннем внесудебном порядке в случае нарушения Лицензиатом требований п.3.1.3. настоящего Договора.

**4. ВОЗНАГРАЖДЕНИЕ И СРОК ОПЛАТЫ**

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

4.2. Оплата по настоящему Договору осуществляется Сублицензиатом в безналичной форме, путем перечисления денежных средств на расчетный счет Лицензиата указанный в разделе 13 настоящего Договора, в следующем порядке:

*Оплата вознаграждения по настоящему Договору производится Сублицензиатом в течение 40 календарных дней после подписания Сторонами УПД согласно п.1.3 договора*

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

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. В случае нарушения Лицензиатом сроков передачи права пользования на Программное обеспечение и (или) документации на право пользования, Лицензиат выплачивает Сублицензиату неустойку в размере 0,1% от размера вознаграждения, указанного в п.4.1. за каждый день просрочки.

5.3. Лицензиат 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. Стороны обязуются в течение срока действия настоящего Договора и в течение 5 (пяти) лет после его прекращения обеспечить охрану полученной от другой Стороны информации конфиденциального характера и не использовать эту информацию для целей, не связанных с выполнением обязательств по настоящему Договору.

6.2 Информация конфиденциального характера, передаваемая Сторонами друг другу, должна иметь реквизиты, свидетельствующие о ее конфиденциальности.

6.3. Каждая из Сторон обязуется не передавать оригиналы или копии документов, полученных друг от друга в связи с настоящим Договором, третьим лицам без предварительного письменного согласия другой Стороны.

6.4. Стороны обязуются в течение срока действия настоящего Договора и в течение 5 (пяти) лет после его прекращения обеспечить охрану полученной ими друг от друга информации конфиденциального характера и не использовать эту информацию для целей, не связанных с выполнением обязательств по настоящему Договору.

6.5. Стороны обязуются соблюдать конфиденциальность персональных данных, обрабатываемых ими при выполнении настоящего Договора, и принимать меры по обеспечению безопасности персональных данных при их обработке, предусмотренные статьей 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

**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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**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 Сублицензиата о нарушениях каких-либо положений пункта 9.1. настоящего Договора: телефон: (499) 181-24-52, e-mail: omts@rzd-med.ru, официальный сайт [www.ckb2rzd.ru](http://www.ckb2rzd.ru) (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 *в течении 12(двенадцати) месяцев с даты заключения настоящего Договора.*

**11. НАЛОГОВАЯ ОГОВОРКА**

11.1.Лицензиат гарантирует, что:

зарегистрирован в ЕГРЮЛ/ЕГРИП надлежащим образом;

*его исполнительный орган находится и осуществляет функции управления по месту регистрации юридического лица, и в нем нет дисквалифицированных лиц* - *данный абзац не добавляется в договор, если Лицензиатом является индивидуальный предприниматель*;

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 Сублицензиату* – *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 Лицензиат нарушит гарантии (любую одну, несколько или все вместе), указанные в пункте 11.1. настоящего Договора, и это повлечет:

предъявление налоговыми органами требований к Сублицензиату 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 Лицензиата услуги, имущественные права, являющиеся предметом настоящего Договора, требований к Сублицензиату 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 Лицензиат обязуется возместить Сублицензиату убытки, который последний понес вследствие таких нарушений.

11.3. Лицензиат в соответствии со ст. 406.1. Гражданского кодекса Российской Федерации, возмещает Сублицензиату 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 Лицензиата 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 Сублицензиата, второй - у Лицензиата.

12.7. К настоящему Договору прилагаются:

12.7.1. Требование к программному обеспечению (Приложение № 1).

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

|  |  |
| --- | --- |
| **Сублицензиат:****ЧУЗ «ЦКБ «РЖД-Медицина»**Место нахождения: 129128, г. Москва, ул. Будайская, д. 2ИНН 7716511464КПП 771601001ОГРН 1047796593525Р/с 40703 810 9 01300 000612АО «АЛЬФА-БАНК»К/с 30101 810 2 000 000 00593БИК 044525593E-mail: dogovor\_ckb@mail.ruДиректор\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / И.М. Акчурина/М.П. | **Лицензиат:**Место нахождения: ИНН:КПП:ОГРН:К/С:Банк БИК: Р/С:Электронная почта: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **/\_\_\_\_\_\_\_\_\_\_/** |

Приложение № 1

к Сублицензионному договору

№ \_\_\_ от "\_\_" \_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

**Требование к программному обеспечению**

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

Функциональные требования:

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:

oWindows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 и выше;

oWindows 8 Professional / Enterprise (32 / 64-разрядная);

oWindows 8.1 Professional / Enterprise (32 / 64-разрядная);

oWindows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise;

oWindows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise.

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

•антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;

•антивирусное сканирование по расписанию;

•антивирусное сканирование подключаемых устройств;

•эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;

•нейтрализации действий активного заражения;

 •анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;

•анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;

•блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;

•откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;

•ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;

•облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

•антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;

•защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;

•фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;

•проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;

•блокировку баннеров и всплывающих окон на загружаемых Web-страницах;

•распознавания и блокировку фишинговых и небезопасных сайтов;

•встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;

•защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;

•защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;

•контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;

•создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;

•контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;

•управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;

•записи в журнал событий о записи и/или удалении файлов на съемных дисках;

•назначение приоритета для правил доступа к устройствам с файловой системой;

•контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;

•защиты от атак типа BadUSB;

•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 через доверенные программы удаленного администрирования;

•установки только выбранных компонентов программного средства антивирусной защиты;

•централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

•запуска задач по расписанию и/или сразу после запуска приложения;

•гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

•ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

•проверки целостности антивирусной программы;

•добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;

•импорта и экспорта списков правил и исключений в XML-формат;

•наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;

•наличие защищенного хранилища для отчетов о работе антивируса;

•включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;

•интеграции с Windows Defender Security Center;

•наличие поддержки Antimalware Scan Interface (AMSI);

•наличие поддержки Windows Subsystem for Linux (WSL);

•защитить паролем восстановление объектов из резервного хранилища;

•ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;

•наличие инструмента мониторинга сети по протоколам TCP и UDP;

•возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;

•возможность установки ограничение длительности выполнения задачи;

•возможность ставить задачи проверки в очередь, если проверка уже выполняется.

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:

oWindows Small Business Server 2011 Essentials / Standard (64-разрядная), Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2;

oWindows MultiPoint Server 2011 (64-разрядная);

oWindows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;

oWindows Server 2012 Foundation / Essentials / Standard / Datacenter;

oWindows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;

oWindows Server 2016 Essentials / Standard / Datacenter;

oWindows Server 2019 Essentials / Standard / Datacenter;

oWindows Server 2022.

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

•антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;

•антивирусное сканирование по расписанию;

•антивирусное сканирование подключаемых устройств;

•эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;

•нейтрализации действий активного заражения;

•анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;

•анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;

•блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;

•откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;

•облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

•антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;

•встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;

•защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;

•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;

•возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;

•возможность установки ограничения длительности выполнения задачи;

•возможность ставить задачи проверки в очередь, если проверка уже выполняется.

Требования к программным средствам антивирусной защиты для рабочих станций Mac

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

omacOS 10.14 - 12;

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

•резидентный антивирусный мониторинг;

•облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

•автоматическое обновление антивирусных баз по расписанию;

•резервное копирование зараженных файлов перед их удалением, для возможности восстановления;

•эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;

•защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;

•блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;

•проверку сетевого трафика, передаваемого через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик);

•контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к

 определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем

•ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

•централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

•возможность установки расширений из командной строки с помощью новой команды kav;

•возможность задавать исключения при проверке указанных областей на уровне перехватов файловых операций;

•возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены.

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

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

oCentOS 6.7 и выше.

oDebian GNU/Linux 10.1 и выше.

oDebian GNU/Linux 11.

oMageia 4.

oRed Hat Enterprise Linux 6.7 и выше.

oАльт 8 СП Рабочая Станция.

oАльт 8 СП Сервер.

oАльт Образование 10.

oАльт Рабочая Станция 10.

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

oAlmaLinux OS 8 и выше.

oAlmaLinux OS 9 и выше.

oAlterOS 7.5 и выше.

oAmazon Linux 2.

oAstra Linux Common Edition 2.12.

oAstra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).

oAstra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).

oAstra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).

oAstra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).

oCentOS 6.7 и выше.

oCentOS 7.2 и выше.

oCentOS Stream 9.

oDebian GNU/Linux 10.1 и выше.

oDebian GNU/Linux 11.

oEMIAS 1.0.

oEulerOS 2.0 SP5.

oLinuxMint 19.2 и выше.

oLinuxMint 20.3 и выше.

oopenSUSE Leap 15.0 и выше.

oOracle Linux 7.3 и выше.

oOracle Linux 8.0 и выше.

oRed Hat Enterprise Linux 6.7 и выше.

oRed Hat Enterprise Linux 7.2 и выше.

oRed Hat Enterprise Linux 8.0 и выше.

oRed Hat Enterprise Linux 9.

 oRocky Linux 8.5 и выше.

oSUSE Linux Enterprise Server 12.5 и выше.

oSUSE Linux Enterprise Server 15 и выше.

oUbuntu 20.04 LTS.

oUbuntu 22.04 LTS.

oАльт 8 СП Рабочая станция.

oАльт 8 СП Сервер.

oАльт Образование 10.

oАльт Рабочая Станция 10.

oАльт Сервер 10.

oАтлант, сборка Alcyone, версия 2022.02.

oГослинукс 7.17.

oГослинукс 7.2.

oРЕД ОС 7.3.

oРОСА "Кобальт" 7.9.

oРОСА "Хром" 12.

oОСОН "ОСНова".

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

oAstra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).

oEulerOS 2.0 SP8.

oSUSE Linux Enterprise Server 15 SP3.

oUbuntu 20.04 LTS.

oАльт 8 СП Сервер.

oРЕД ОС 7.3.

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

•резидентного антивирусного мониторинга;

•облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

•проверку ресурсов доступных по SMB / NFS;

•возможность проверки памяти ядра;

•эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

•антивирусное сканирование по команде пользователя или администратора и по расписанию;

•антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;

•проверку сообщений электронной почты в текстовом формате (Plain text);

•наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);

•защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;

•включения опции блокирования файлов во время проверки;

•помещение подозрительных и поврежденных объектов на карантин;

•перехвата и проверки файловых операций на уровне SAMBA;

•управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;

•запуск задач по расписанию и/или сразу после загрузки операционной системы;

•экспортировать и сохранять отчеты в форматах HTML и CSV;

•гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

•сохранение копии зараженного объекта в резервном хранилище перед

лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;

•управления через пользовательский графический интерфейс без root прав;

•централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;

•управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;

•проверки съемных дисков;

•отслеживания во входящем сетевом трафике активности, характерной для сетевых атак

•проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым;

•получения данных о действиях программ на компьютере пользователя;

•создание файлов трассировки при запуске программы;

•получение информации обо всех исполняемых файлах программ, установленных на компьютерах;

•проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;

•сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий.

Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows

Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

32-разрядных операционных систем Microsoft Windows

oWindows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

oWindows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

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

oWindows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше.

64-разрядных операционных систем Microsoft Windows

oWindows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

oWindows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

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

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

oMicrosoft Small Business Server 2008 Standard / Premium SP2 или выше;

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

oWindows Server 2008 R2 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;

oWindows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше;

oMicrosoft Small Business Server 2011 Essentials / Standard SP1 или выше;

oMicrosoft Windows MultiPoint Server 2011 Standard / Premium;

oWindows Server 2012 Foundation / Essentials / Standard / Datacenter;

oWindows Server 2012 Core Foundation / Essentials / Standard / Datacenter;

oMicrosoft MultiPoint Server 2012 Standard / Premium;

 oWindows Storage Server 2012;

oWindows Hyper-V Server 2012;

oWindows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;

oWindows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;

oWindows Storage Server 2012 R2;

oWindows Hyper-V Server 2012 R2;

oWindows Server 2016 Essentials / Standard / Datacenter;

oWindows Server 2016 MultiPoint;

oWindows Server 2016 Core Standard / Datacenter;

oMicrosoft Windows MultiPoint Server 2016;

oWindows Storage Server 2016;

oWindows Hyper-V Server 2016;

oWindows Server 2019 Essentials / Standard / Datacenter;

oWindows Server 2019 Core;

oWindows Storage Server 2019;

oWindows Hyper-V Server 2019;

oWindows Server 2022;

oWindows 10 Enterprise multi-session.

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

•антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;

•антивирусное сканирование по команде пользователя или администратора и по расписанию;

•запуск задач по расписанию и/или сразу после загрузки операционной системы;

•облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;

•антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;

•защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;

•непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.

•анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;

•проверки контейнеров Microsoft Windows;

•защиты от эксплуатирования уязвимостей в памяти процессов;

•должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;

•добавлять процессы в список защищаемых;

•ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

•проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;

•настройки проверки критических областей сервера в качестве отдельной задачи;

•регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;

•продолжать антивирусное сканирование в фоновом режиме;

 •наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);

•ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;

•интеграции с SIEM системами;

•указания количества рабочих процессов антивируса вручную;

•отключить графический интерфейс;

•наличие удаленной и локальной консоли управления;

•управления параметрами антивируса из командной строки;

•централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

•управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;

•защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;

•включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов.

Требования к программным средствам антивирусной защиты мобильных устройств

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

oAndroid 5.0–13 (включая Android 12L, исключая Go Edition);

oiOS 10–16 или iPadOS 13–15;

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

•постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;

•проверка файловой системы устройства по требованию и по расписанию;

•мгновенная проверка устанавливаемых приложений

•блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;

•наличие хранилища для изолирования зараженных объектов;

•обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;

•блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;

•поддержка белых списков разрешенных приложений;

•блокировка системных приложений, в рамках контроля запуска приложений;

•отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM);

•заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;

•указать параметры подключения к wi-fi сетям;

•указать обязательные к установке приложения;

•блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);

•создания списка правил на основе которых будет осуществляться

проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;

•поддержка технологий Samsung KNOX1 и KNOX2.

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

•удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;

•отправки команды блокирования и удаления данных;

•создавать групповые политики безопасности мобильных устройств;

•удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM;

•получать отчеты и статистику о работе мобильных устройств пользователей;

•блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervised mode;

•централизованного управления с помощью единой консоли управления;

•наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari или Game Center, на управляемом устройстве.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

oMicrosoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

 oMicrosoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

oMicrosoft Windows 11 Home 64-разрядная;

oMicrosoft Windows 11 Pro 64-разрядная;

oMicrosoft Windows 11 Enterprise 64-разрядная;

oMicrosoft Windows 11 Education 64-разрядная;

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

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

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

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

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

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

oWindows Server 2008 R2 with Standard Service Pack 1 и выше 64-разрядная;

oWindows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;

oWindows Server 2012 Server Core 64-разрядная;

oWindows Server 2012 Datacenter 64-разрядная;

oWindows Server 2012 Essentials 64-разрядная;

oWindows Server 2012 Foundation 64-разрядная;

oWindows Server 2012 Standard 64-разрядная;

oWindows Server 2012 R2 Server Core 64-разрядная;

oWindows Server 2012 R2 Datacenter 64-разрядная;

oWindows Server 2012 R2 Essentials 64-разрядная;

oWindows Server 2012 R2 Foundation 64-разрядная;

oWindows Server 2012 R2 Standard 64-разрядная;

oWindows Server 2016 Datacenter (LTSB) 64-разрядная;

oWindows Server 2016 Standard (LTSB) 64-разрядная;

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

oWindows Server 2019 Standard 64-разрядная;

oWindows Server 2019 Datacenter 64-разрядная;

oWindows Server 2019 Core 64-разрядная;

oWindows Server 2022 Standard 64-разрядная;

oWindows Server 2022 Datacenter 64-разрядная;

oWindows Server 2022 Core 64-разрядная;

oWindows Storage Server 2012 64-разрядная;

 oWindows Storage Server 2012 R2 64-разрядная;

oWindows Storage Server 2016 64-разрядная;

oWindows Storage Server 2019 64-разрядная.

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

oVMware vSphere 6.7;

oVMware vSphere 7.0;

oVMware Workstation 16 Pro;

oMicrosoft Hyper-V Server 2012 64-разрядная;

oMicrosoft Hyper-V Server 2012 R2 64-разрядная;

oMicrosoft Hyper-V Server 2016 64-разрядная;

oMicrosoft Hyper-V Server 2019 64-разрядная;

oMicrosoft Hyper-V Server 2022 64-разрядная;

oCitrix XenServer 7.1 LTSR;

oCitrix XenServer 8.x;

oParallels Desktop 17;

oOracle VM VirtualBox 6.x.

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

oMicrosoft SQL Server 2012 Express 64-разрядная;

oMicrosoft SQL Server 2014 Express 64-разрядная;

oMicrosoft SQL Server 2016 Express 64-разрядная;

oMicrosoft SQL Server 2017 Express 64-разрядная;

oMicrosoft SQL Server 2019 Express 64-разрядная;

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

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

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

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

oMicrosoft SQL Server 2019 (все редакции) для Windows 64-разрядная (требуются дополнительные действия);

oMicrosoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуются дополнительные действия);

oMicrosoft Azure SQL Database;

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

oMySQL 5.7 Community 32-разрядная/64-разрядная;

oMySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;

oMySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;

oMariaDB 10.5.x 32-разрядная/64-разрядная;

oMariaDB 10.4.x 32-разрядная/64-разрядная;

oMariaDB 10.3.22 и выше 32-разрядная/64-разрядная;

oMariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;

oMariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;

oMariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

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

•выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;

•чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;

•настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;

•автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD;

•централизованные установка, обновление и удаление программных средств антивирусной защиты;

•централизованная настройка, администрирование;

•просмотр отчетов и статистической информации по работе средств защиты;

•централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;

•сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;

•наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;

•указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;

•иерархии триггеров, по которым происходит перераспределение;

•тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;

•доставка обновлений на рабочие места пользователей сразу после их получения;

•распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;

•построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;

•создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;

•поддержка мультиарендности (multi-tenancy) для серверов управления;

•обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;

•доступ к облачным серверам производителя антивирусного ПО через сервер управления;

•автоматическое распространение лицензии на клиентские компьютеры;

•инвентаризация установленного ПО и оборудования на компьютерах пользователей;

•наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;

•функция управления мобильными устройствами через сервер Exchange ActiveSync;

•функция управления мобильными устройствами через сервер iOS MDM;

•отправки SMS-оповещений о заданных событиях;

•централизованная установка сертификатов на управляемые мобильные устройства;

•указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;

•указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;

•построение графических отчетов по событиям антивирусной защиты,

данным инвентаризации, данным лицензирования установленных программ;

•наличие преднастроенных стандартных отчетов о работе системы;

•экспорт отчетов в файлы форматов PDF и XML;

•централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;

•создание внутренних учетных записей для аутентификации на сервере управления;

•создание резервной копии системы управления встроенными средствами системы управления;

•поддержка Windows Failover Clustering;

•поддержка интеграции с Windows сервисом Certificate Authority;

•наличие портала самообслуживания пользователей;

•портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;

•наличие системы контроля возникновения вирусных эпидемий;

•установки в облачной инфраструктуре Microsoft Azure и Google Cloud;

•интеграции по OpenAPI;

•управления антивирусной защитой с использованием WEB консоли;

•двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;

•использования дополнительной аутентификация после изменения параметров учетной записи пользователя.

•возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами;

•возможность развернуть сервер администрирования как систему высокой доступности.

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

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

oDebian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная;

oDebian GNU/Linux 10.х (Buster) 32-разрядная/64-разрядная;

oDebian GNU/Linux 9.х (Stretch) 32-разрядная/64-разрядная;

oUbuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;

oUbuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная;

oCentOS 7.x 64-разрядная;

oRed Hat Enterprise Linux Server 8.x 64-разрядная;

oRed Hat Enterprise Linux Server 7.x 64-разрядная;

oSUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная;

oSUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная;

oAstra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;

oAstra Linux Special Edition 1.6 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;

oAstra Linux Common Edition 2.12 64-разрядная;

oАльт Сервер 10 64-разрядная;

oАльт Сервер 9.2 64-разрядная;

oАльт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;

oАльт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная;

oАльт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная;

oOracle Linux 7 64-разрядная;

oOracle Linux 8 64-разрядная;

oРЕД ОС 7.3 Сервер 64-разрядная;

oРЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

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

oVMware vSphere 6.7.

oVMware vSphere 7.0;

oVMware Workstation 16 Pro;

oMicrosoft Hyper-V Server 2012 64-разрядная;

oMicrosoft Hyper-V Server 2012 R2 64-разрядная;

oMicrosoft Hyper-V Server 2016 64-разрядная;

oMicrosoft Hyper-V Server 2019 64-разрядная;

oMicrosoft Hyper-V Server 2022 64-разрядная;

oCitrix XenServer 7.1 LTSR;

oCitrix XenServer 8.x;

oParallels Desktop 17;

oВиртуальная машина на основе Kernel. Поддерживает следующие операционные системы:

oАльт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;

oАльт Сервер 10 64-разрядная;

oAstra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;

oDebian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная;

oUbuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;

oРЕД ОС 7.3 Сервер 64-разрядная;

oРЕД ОС 7.3 Сертифицированная редакция 64-разрядная

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

oMySQL 5.7 Community 32-разрядная/64-разрядная;

oMySQL 8.0 32-разрядная/64-разрядная;

oMariaDB 10.5.x 32-разрядная/64-разрядная;

oMariaDB 10.4.x 32-разрядная/64-разрядная;

oMariaDB 10.3.22 и выше 32-разрядная/64-разрядная;

oMariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;

oMariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

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

•централизованные установка, обновление и удаление программных средств антивирусной защиты;

•централизованная настройка, администрирование;

•просмотр отчетов и статистической информации по работе средств защиты;

•сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;

•иерархии триггеров, по которым происходит перераспределение;

•доставка обновлений на рабочие места пользователей сразу после их получения;

•распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;

•построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;

•создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;

•поддержка мультиарендности (multi-tenancy) для серверов управления;

 •обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;

•доступ к облачным серверам производителя антивирусного ПО через сервер управления;

•автоматическое распространение лицензии на клиентские компьютеры;

•наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;

•построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ;

•наличие преднастроенных стандартных отчетов о работе системы;

•экспорт отчетов в файлы форматов PDF и XML;

•централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;

•создание внутренних учетных записей для аутентификации на сервере управления;

•создание резервной копии системы управления встроенными средствами системы управления;

•наличие системы контроля возникновения вирусных эпидемий;

•управления антивирусной защитой с использованием WEB консоли;

•возможность обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;

•возможность с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;

•возможность использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули.

Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

•создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток;

•множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;

•проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к эксплуатационной документации

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

•«Руководство пользователя (администратора)»

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

•Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по электронной почте и через Интернет.

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

|  |  |
| --- | --- |
| **от Сублицензиата:****Директор** | **от Лицензиата:** |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **/И.М. Акчурина/** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **/\_\_\_\_\_\_\_\_\_\_/**