СУБЛИЦЕНЗИОННЫЙ ДОГОВОР № 140/10/2023ЦПН
на оказание услуг по продлению и подключению неисключительных (пользовательских) прав на использование программного обеспечения – универсальная лицензия антивирусной защиты (рабочие станции / файловые сервера / мобильные устройства) с функциями расширенного системного администрирования и шифрования данных на 12 месяцев

(Идентификационный код закупки № 231770403237977040100101530012620244)

г. Москва « 02» октября 2023 г.

Федеральное государственное бюджетное учреждение «Национальный медицинский исследовательский центр психиатрии и наркологии имени В.П. Сербского» Министерства здравоохранения Российской Федерации (ФГБУ «НМИЦ ПН им. В.П. Сербского» Минздрава России), именуемое в дальнейшем «Сублицензиат», в лице в лице в лице заместителя генерального директора по финансово-экономическим вопросам Юрасовой Марии Андреевны, действующего на основании доверенности от 21.11.2022 г. №01-22/5167, с одной стороны, и **Общество с ограниченной ответственностью "СОФТЕКС" (ООО «СОФТЕКС»)**, именуемое в дальнейшем «Лицензиат», в лице генерального директора Дорофеева Дмитрия Олеговича, действующего на основании Устава, с другой стороны, по отдельности именуемые «Сторона», вместе именуемые «Стороны», с соблюдением требований Федерального закона от 05.04.2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – Закон № 44-ФЗ) и на основании Протокола подведения итогов определения поставщика (подрядчика, исполнителя) от «21» сентября 2023 г. № 0373100113723000140, заключили настоящий Договор (далее - Договор) о нижеследующем::

1. ПРЕДМЕТ ДОГОВОРА

1.1. По настоящему Договору Лицензиат, являясь правообладателем либо имея от правообладателя соответствующие полномочия: (Сертификат PIN SF55RU01)[1], обязуется оказать услуги по продлению и подключению (передаче) неисключительных (пользовательских) прав на использование программного обеспечения – универсальная лицензия антивирусной защиты (рабочие станции / файловые сервера / мобильные устройства) с функциями расширенного системного администрирования и шифрования данных на 12 месяцев Сублицензиату на условиях простой (неисключительной) лицензии, неисключительных прав на использование антивирусного программного обеспечения (далее – Услуги). Наименование, технические характеристики, количественные данные, права на использование которых предоставляются (передаются) Сублицензиату, определяются Техническим заданием (Приложение № 1 к настоящему Договору).

1.2. Право использования антивирусного программного обеспечения включает в себя право на воспроизведение соответствующих программ на территории Российской Федерации, ограниченное инсталляцией, копированием и запуском. Право использования предоставляется Сублицензиату на срок действия исключительного права с ограничениями, включая способы использования программ, установленными настоящим Договором.

1.3. Сублицензиат обязуется принять передаваемые права, соответствующие условиям Договора, и оплатить Лицензиату вознаграждение в порядке и на условиях, определенных настоящим Договором.

[1] *Указываются наименования и реквизиты документов, подтверждающих правообладание или согласие правообладателя на предоставление Сублицензиату прав на использование антивирусного программного обеспечения*

1.4. Лицензиат гарантирует, что он обладает всеми законными основаниями для предоставления Сублицензиату права использования антивирусного программного обеспечения по настоящему Договору.

1.5. Лицензиат подтверждает, что права на использование антивирусного программного обеспечения не заложены, не арестованы, не являются предметом исков третьих лиц и являются лицензионным продуктом.

2. Цена Договора и порядок оплаты

2.1. Размер вознаграждения Лицензиата по настоящему Договору определен в Расчете цены договора (Приложение № 2 к настоящему Договору) и составляет **895 555,72 (Восемьсот девяносто пять тысяч пятьсот пятьдесят пять) рублей 72 копейки**.

Вознаграждение по настоящему Договору не подлежит обложению НДС в соответствии с пп. 26 п. 2. ст. 149 Налогового кодекса Российской Федерации.

Суммы, подлежащие уплате Сублицензиатом юридическому лицу или физическому лицу, в том числе зарегистрированному в качестве индивидуального предпринимателя, уменьшаются на размер налогов, сборов и иных обязательных платежей в бюджеты бюджетной системы Российской Федерации, связанных с оплатой Договора, если в соответствии с законодательством Российской Федерации о налогах и сборах такие налоги, сборы и иные обязательные платежи подлежат уплате в бюджеты бюджетной системы Российской Федерации Заказчиком.

2.2. Цена Договора является твердой, определяется на весь срок исполнения Договора, за исключением случаев, установленных Федеральным законом от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – Закон № 44-ФЗ) и Договором.

Источник финансирования: субсидии на выполнение государственного задания.

2.3. В цену настоящего Договора входят все затраты, издержки и иные расходы Лицензиата, связанные с надлежащим исполнением Договора, а также сумма всех расходов Лицензиата, прямо и/или косвенно связанных с исполнение обязательств по Договору, в том числе лицензионное вознаграждение Лицензиату, расходы на страхование, уплату таможенных пошлин, налогов и других обязательных платежей, финансовых рисков, инфляционных ожиданий и других расходов, связанных с исполнением Договора.

2.4. Оплата по Договору осуществляется по факту передачи неисключительных прав на использование антивирусного программного обеспечения в течение 7 (Семи) рабочих дней с даты подписания Сублицензиатом с помощью электронной подписи в единой информационной системе в сфере закупок (далее – ЕИС) документа о приемке в соответствии с п. 3.1.1, п.4.3 и п.4.3.1 настоящего Договора на основании счета, выставленного Лицензиатом.

Авансовый платеж не предусмотрен.

2.5. Оплата вознаграждения производится в рублях Российской Федерации по безналичному расчету платежными поручениями путём перечисления указанной суммы на расчётный счёт Лицензиата, указанный в разделе 13 настоящего Договора.

2.6. Датой оплаты считается дата списания денежных средств с лицевого счета Сублицензиата в адрес расчётного счёта Лицензиата.

3. Права и обязанности Сторон

3.1. **Лицензиат обязан:**

3.1.1. В срок не позднее 14 (четырнадцати) календарных дней с даты заключения настоящего Договора предоставить Сублицензиату неисключительные права на использование антивирусного программного обеспечения, в том числе путём сообщения ему необходимых ключей доступа и паролей, согласно Техническому заданию (Приложение № 1 к настоящему Договору) и направить Сублицензиату с использованием ЕИС документ о приемке в соответствии с п. 4.3 настоящего Договора, включающий Акт приема-передачи неисключительных прав на использование антивирусного программного обеспечения.

3.1.2. Выставить Сублицензиату счет на оплату в соответствии с разделом 2 настоящего Договора.

3.1.3. В случае принятия решения об одностороннем отказе от исполнения Договора разместить его в ЕИС и направить Сублицензиату в порядке, предусмотренном ст. 95 Закона № 44-ФЗ.

3.2. **Лицензиат имеет право:**

3.2.1. Требовать надлежащего исполнения Сублицензиатом условий настоящего Договора.

3.2.2. Проверять соблюдение Сублицензиатом условий настоящего Договора.

3.2.3. Требовать своевременной оплаты надлежащим образом оказанных и принятых Сублицензиатом Услуг на условиях, установленных Договором.

3.2.4. Принять решение об одностороннем отказе от исполнения настоящего Договора в соответствии с гражданским законодательством.

3.2.5. Требовать возмещения убытков, уплаты неустоек (штрафов, пеней) в соответствии с разделом 5 Договора.

3.2.6. Лицензиат обладает иными правами и обязанностями, предусмотренными настоящим Договором, Гражданским кодексом Российской Федерации и иными нормативными правовыми актами Российской Федерации.

3.3. **Сублицензиат обязан:**

3.3.1. Принять неисключительные права на использование антивирусного программного обеспечения согласно условиям по Акту предоставления прав.

3.3.2. Провести экспертизу переданных неисключительных прав на использование антивирусного программного обеспечения в целях проверки их соответствия условиям Договора в соответствии с Законом № 44-ФЗ.

3.3.3. Обеспечить своевременную оплату вознаграждения по Договору согласно разделу 2 Договора.

3.3.4. Принять решение об одностороннем отказе от исполнения Договора в случае, если в ходе исполнения Договора установлено, что Лицензиат и (или) передаваемые неисключительные права на использование антивирусного программного обеспечения не соответствуют установленным извещением об осуществлении закупки и (или) документацией о закупке требованиям к участникам закупки и (или) передаваемым правам на использование антивирусного программного обеспечения или представил недостоверную информацию о своем соответствии и (или) соответствии передаваемых неисключительных прав на использование антивирусного программного обеспечения таким требованиям, что позволило ему стать победителем определения поставщика (подрядчика, исполнителя).

3.3.5. Соблюдать условия лицензионного соглашения.

3.3.6. Не распространять антивирусное программное обеспечение.

Под распространением антивирусного программного обеспечения понимается предоставление доступа третьим лицам к воспроизведенным в любой форме компонентам программного обеспечения, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем или фактического предоставления.

3.3.7. Требовать уплаты неустоек (штрафов, пеней) в соответствии с разделом 5 Договора.

3.3.8. Сублицензиат не обязан предоставлять Лицензиату отчёт об использовании антивирусным программным обеспечением, права на использование которых передаются по настоящему Договору.

3.4. **Сублицензиат имеет право:**

3.4.1. Требовать от Лицензиата надлежащего исполнения обязательств по Договору.

3.4.2. Требовать от Лицензиата своевременного предоставления надлежащим образом оформленных документов, предусмотренных Договором, счетов, счетов-фактур (если на Лицензиата законодательством о налогах и сборах возложена обязанность по составлению и выставлению счетов-фактур) и документа о приемке.

3.4.3. В любое время проверять ход оказания и качество Услуг, оказываемых Лицензиатом, не вмешиваясь в его оперативно-хозяйственную деятельность.

3.4.4. Требовать от Лицензиата своевременного устранения недостатков, выявленных в ходе приемки.

3.4.5. Требовать возмещения убытков в соответствии с разделом 5 Договора, причиненных по вине Лицензиата.

3.4.6. Получать информацию об оказываемых Лицензиатом Услугах, о реквизитах, режиме работы Лицензиата.

3.4.7. Предъявлять письменные претензии в случае ненадлежащего исполнения Лицензиатом своих обязательств.

3.4.8. Принять решение об одностороннем отказе от исполнения Договора в соответствии с гражданским законодательством и Законом № 44-ФЗ.

3.4.9. Сублицензиат обладает иными правами и обязанностями, предусмотренными настоящим Договором, Гражданским кодексом Российской Федерации и иными нормативными правовыми актами Российской Федерации.

4. Условия предоставления неисключительных прав

4.1. Неисключительные права на использование антивирусного программного обеспечения предоставляются в электронном виде и/или на бумажном носителе, осуществляется силами и за счёт средств Лицензиата. Передача прав на использование антивирусного программного обеспечения сопровождается передачей Заказчику оформленных в соответствии с законодательством Российской Федерации сертификатов, соглашений, свидетельств, подтверждающих предоставление неисключительных прав на использование антивирусного программного обеспечения.

В случае предоставления неисключительных прав на использование антивирусного программного обеспечения на бумажном носителе, права передаются по предварительному согласованию с Сублицензиатом и уточнением количества, адреса передачи, а также в согласованное время с Сублицензиатом, в срок не превышающий 14 (четырнадцати) календарных дней с даты заключения настоящего Договора.

Права передаются по следующим адресам Сублицензиата:

г. Москва, Кропоткинский пер., д.23.

г. Москва, ул. Потешная, д. 3, стр. 10,11

г. Москва, ул. Ставропольская д.27, стр.7

г. Москва, Малый Могильцевский пер., д.3

Срок активации неисключительных прав (лицензии) на использование антивирусного программного обеспечения должен составлять 12 (двенадцать) месяцев с даты передачи Лицензиатом неисключительных прав (лицензии) на использование антивирусного программного обеспечения.

4.2. В течение 2 (двух) рабочих дней, следующих за днем передачи неисключительных прав на использование антивирусного программного обеспечения, Лицензиат обязан сформировать с использованием единой информационной системы (далее – ЕИС), подписать усиленной электронной подписью лица, имеющего право действовать от имени Лицензиата, и размещает в ЕИС документ о приемке.

4.3. Документ о приемке должен содержать:

а) включенные в договор идентификационный код закупки, наименование, место нахождения Сублицензиата, наименование объекта закупки, место поставки товара, выполнения работы, оказания услуги, информацию о Лицензиате, единицу измерения поставленного товара (при осуществлении закупки товара, в том числе поставляемого заказчику при выполнении закупаемых работ, оказании закупаемых услуг), выполненной работы, оказанной услуги;

б) наименование поставленного товара, выполненной работы, оказанной услуги;

в) наименование страны происхождения поставленного товара (при осуществлении закупки товара, в том числе поставляемого заказчику при выполнении закупаемых работ, оказании закупаемых услуг);

г) информацию о количестве поставленного товара (при осуществлении закупки товара, в том числе поставляемого Сублицензиату при выполнении закупаемых работ, оказании закупаемых услуг);

д) информацию об объеме выполненной работы, оказанной услуги (при необходимости);

е) стоимость исполненных Лицензиатом обязательств, предусмотренных договором, с указанием цены за единицу поставленного товара (при осуществлении закупки товара, в том числе поставляемого Сублицензиату при выполнении закупаемых работ, оказании закупаемых услуг), выполненной работы, оказанной услуги;

ж) иную информацию с учетом требований, установленных в соответствии с частью 3 статьи 5 Закона № 44-ФЗ.

4.3.1. К документу о приемке, предусмотренному п. 4.3 Договора, могут прилагаться документы, которые считаются его неотъемлемой частью, в том числе, к документу о приемке прилагается Акт приема-передачи неисключительных прав на использование антивирусного программного обеспечения. При этом в случае, если информация, содержащаяся в прилагаемых документах, не соответствует информации, содержащейся в документе о приемке, приоритет имеет предусмотренная п. 4.3 Договора информация, содержащаяся в документе о приемке.

4.4. Электронные документы о приемке в рамках исполнения настоящего Договора, сформированные в ЕИС в электронной форме и подписанные усиленной квалифицированной электронной подписью по правилам Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», признаются электронными документами, равнозначными документам на бумажном носителе, подписанными собственноручными подписями.

4.5. Документы о приемке, сформированные Лицензиатом в ЕИС в электронной форме и подписанные усиленной квалифицированной электронной подписью, должны соответствовать документам, представляемым Лицензиатом Сублицензиату на дату предоставления неисключительных прав на использование антивирусного программного обеспечения.

4.6. Документ о приемке, подписанный Лицензиатом, не позднее одного часа с момента его размещения в ЕИС автоматически с использованием ЕИС направляется Сублицензиату. Датой поступления Сублицензиату документа о приемке, подписанного Лицензиатом, считается дата размещения в соответствии с п. 4.2, 4.3, 4.3.1. настоящего Договора такого документа в ЕИС в соответствии с часовой зоной, в которой расположен Сублицензиат.

4.7. Проверка наименования, комплектации, иных данных, касающихся предоставляемых неисключительных прав на использование антивирусного программного обеспечения, осуществляется Сублицензиатом в момент передачи указанных прав.

4.8. Сублицензиат в течение 20 (двадцати) рабочих дней с момента передачи неисключительных прав на использование антивирусного программного обеспечения и предоставления Лицензиатом документа о приемке в соответствии с п. 4.2, 4.3, 4.3.1. осуществляет действия, направленные на установление соответствия (несоответствия), передаваемых неисключительных прав на использование антивирусного программного обеспечения и представленных Лицензиатом документов, необходимых для осуществления приемки, условиям Договора. Указанные действия включают:

1) Проверку номенклатуры и комплектности передаваемых неисключительных прав на использование антивирусного программного обеспечения.

2) Проверку соблюдения требований по упаковке и маркировке.

3) Контроль работоспособности антивирусного программного обеспечения, права использования которых предоставляются по настоящему Договору, на соответствие Техническому заданию (Приложение №1 к настоящему Договору) и технической документации правообладателей.

4) Контроль оформления гарантийных обязательств (если гарантийные обязательства предусмотрены Договором).

4.9. По результатам приемки Сублицензиат:

а) подписывает усиленной электронной подписью лица, имеющего право действовать от имени Сублицензиата, и размещает в ЕИС документ о приемке;

б) формирует с использованием ЕИС, подписывает усиленной электронной подписью лица, имеющего право действовать от имени Сублицензиата, и размещает в ЕИС мотивированный отказ от подписания документа о приемке с указанием причин такого отказа.

4.10. В случае приемки предоставляемых неисключительных прав на использование антивирусного программного обеспечения приемочной комиссией не позднее 20 (двадцати) рабочих дней, следующих за днем поступления Сублицензиату документа о приемке в соответствии с пунктом 4.8 настоящего Договора:

а) члены приемочной комиссии подписывают усиленными электронными подписями поступивший документ о приемке или формируют с использованием ЕИС, подписывают усиленными электронными подписями мотивированный отказ от подписания документа о приемке с указанием причин такого отказа. При этом, если приемочная комиссия включает членов, не являющихся работниками заказчика, допускается осуществлять подписание документа о приемке, составление мотивированного отказа от подписания документа о приемке, подписание такого отказа без использования усиленных электронных подписей и ЕИС;

б) после подписания членами приемочной комиссии в соответствии с подпунктом "а" настоящего пункта документа о приемке или мотивированного отказа от подписания документа о приемке Сублицензиат подписывает документ о приемке или мотивированный отказ от подписания документа о приемке усиленной электронной подписью лица, имеющего право действовать от имени Сублицензиата, и размещает его в ЕИС. Если члены приемочной комиссии в соответствии с подпунктом "а" настоящего пункта не использовали усиленные электронные подписи и ЕИС, Сублицензиат прилагает подписанные ими документы в форме электронных образов бумажных документов.

4.11. При выявлении несоответствий в передаваемых неисключительных прав на использование антивирусного программного обеспечения (наименования, количества, качества), препятствующих их приемке, Сублицензиат в срок, установленный в пунктах 4.8 или 4.10 Договора, отказывает в приемке передаваемых неисключительных прав на использование антивирусного программного обеспечения, направляя Лицензиату мотивированный отказ от подписания документа о приемке с перечнем выявленных недостатков.

Сублицензиат вправе потребовать от Лицензиата произвести замену передаваемых неисключительных прав на использование антивирусного программного обеспечения, не соответствующих условиям Договора, без каких-либо дополнительных затрат со стороны Сублицензиата. Лицензиат обязан заменить передаваемые неисключительные права на использование антивирусного программного обеспечения в течение 5 (пяти) рабочих дней, следующих за днем непринятия прав.

Сублицензиат вправе не отказывать в приемке передаваемых неисключительных прав на использование антивирусного программного обеспечения в случае выявления несоответствия прав условиям Договора, если выявленное несоответствие не препятствует приемке этих прав и устранено Лицензиатом.

4.12. Документ о приемке, мотивированный отказ от подписания документа о приемке не позднее одного часа с момента размещения в ЕИС в соответствии с пунктами 4.9 или 4.10 настоящего Договора направляются автоматически с использованием ЕИС Лицензиату. Датой поступления Лицензиату документа о приемке, мотивированного отказа от подписания документа о приемке считается дата размещения в соответствии с указанными пунктами таких документа о приемке, мотивированного отказа от подписания документа о приемке в ЕИС в соответствии с часовой зоной, в которой расположен Лицензиат.

4.13. В случае получения в соответствии с подп. «б» п. 4.9 или подп. «б» п. 4.10 Договора мотивированного отказа от подписания документа о приемке Лицензиат вправе устранить причины, указанные в таком мотивированном отказе, в согласованный Сторонами срок без дополнительной оплаты и направить Сублицензиату документ о приемке в порядке, предусмотренном настоящим разделом Договора.

4.14. Неисключительные права на использование антивирусного программного обеспечения считаются предоставленными Сублицензиату, и Сублицензиат вправе начать использование неисключительных прав на использование антивирусного программного обеспечения с даты предоставления неисключительных прав на использование антивирусного программного обеспечения, но не ранее даты начала срока действия неисключительных прав на использование антивирусного программного обеспечения, установленной в соответствии с Техническим заданием (Приложение № 1 к настоящему Договору).

4.15. В случае если Лицензиат получит достоверную информацию о нарушении Сублицензиатом требований законодательства или любых лицензионных соглашений, или правил лицензионного использования неисключительных прав на использование антивирусного программного обеспечения, Сублицензиат соглашается приостановить и (или) прекратить использование неисключительных прав на использование антивирусного программного обеспечения с момента получения соответствующего письменного уведомления Лицензиата.

4.16. Если третье лицо предъявит Сублицензиату иск о неправомерности использования неисключительных прав на использование антивирусного программного обеспечения, предоставленные по Договору, Сублицензиат будет обязан привлечь Лицензиата к участию в деле, а Лицензиат обязан вступить в это дело на стороне Сублицензиата. Непривлечение Сублицензиатом Лицензиата к участию в деле не освобождает Лицензиата от ответственности перед Сублицензиатом.

4.17. Внесение исправлений в документ о приемке, оформленный в соответствии с разделом 4 настоящего Договора, осуществляется путем формирования, подписания усиленными электронными подписями лиц, имеющих право действовать от имени Лицензиата, Сублицензиата, и размещения в ЕИС исправленного документа о приемке. Срок внесения Лицензиатом исправлений в документ о приемке составляет не более 5 (пяти) рабочих дней с даты получения уведомления от Сублицензиатом с использованием ЕИС.

5. Ответственность Сторон

5.1. За неисполнение или ненадлежащее исполнение своих обязательств, установленных Договором, Стороны несут ответственность в соответствии с законодательством Российской Федерации и настоящим Договором.

В случае полного (частичного) неисполнения условий Договора одной из Сторон эта Сторона обязана возместить другой Стороне причиненные убытки в части, непокрытой неустойкой.

5.2. В случае просрочки исполнения Сублицензиатом обязательств, предусмотренных Договором, а также в иных случаях неисполнения или ненадлежащего исполнения Сублицензиатом обязательств, предусмотренных Договором, Лицензиат вправе потребовать уплаты неустоек (штрафов, пеней).

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

5.4. За каждый факт неисполнения Сублицензиатом обязательств, предусмотренных Договором, за исключением просрочки исполнения обязательств, предусмотренных

Договором, штраф устанавливается в размере 1000,00 (Одна тысяча) рублей 00 копеек (Постановление Правительства Российской Федерации от 30 августа 2017 г. № 1042).

5.5. Общая сумма начисленных штрафов за ненадлежащее исполнение Сублицензиатом обязательств, предусмотренных Договором, не может превышать цену Договора.

5.6. Сублицензиат освобождается от уплаты неустойки (штрафа, пени), если докажет, что неисполнение или ненадлежащее исполнение обязательства, предусмотренного Договором, произошло вследствие непреодолимой силы или по вине другой Стороны, или по основаниям, связанными с уменьшением в установленном порядке средств бюджета Сублицензиата, выделенных для финансирования работ (услуг, поставки товаров).

5.7. В случае просрочки исполнения Лицензиатом обязательств (в том числе гарантийного обязательства), предусмотренных Договором, а также в иных случаях неисполнения или ненадлежащего исполнения Лицензиатом обязательств, предусмотренных Договором, Сублицензиат направляет Лицензиату требование об уплате неустоек (штрафов, пеней), а Лицензиат обязан уплатить неустойки (штрафы, пени).

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

5.9. За каждый факт неисполнения или ненадлежащего исполнения Лицензиатом обязательств, предусмотренных Договором, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Договором, начисляются штрафы. Штраф устанавливается в размере 1 (Одного) процента от цены Договора (этапа), но не более 5 000,00 (Пяти тысяч) рублей 00 копеек и не менее 1 000,00 (Одной тысячи) рублей 00 копеек (Постановление Правительства Российской Федерации от 30 августа 2017 г. № 1042).

5.10. За каждый факт неисполнения или ненадлежащего исполнения Лицензиатом обязательства, предусмотренного Договором, которое не имеет стоимостного выражения, штраф устанавливается (при наличии в Договоре таких обязательств) в размере 1000,00 (Одна тысяча) рублей 00 копеек (Постановление Правительства Российской Федерации от 30 августа 2017 г. № 1042).

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

5.12. Общая сумма начисленных штрафов за неисполнение или ненадлежащее исполнение Лицензиатом обязательств, предусмотренных Договором, не может превышать цену Договора.

5.13. В случае применения судебными органами (иными соответствующими органами, в том числе административными органами), юридическими лицами, физическими лицами имущественных санкций (взысканий) к Сублицензиату, если они явились результатом нарушения Лицензиатом своих обязанностей по Договору или совершения Лицензиатом иных действий, влекущих применение к Сублицензиату имущественных санкций, Лицензиат компенсирует Сублицензиату убытки в размере взысканных санкций.

5.14. Уплата неустоек (штрафа, пени) не освобождает Стороны от исполнения обязательств по Договору.

5.15. Лицензиат обязан в установленные Договором сроки безвозмездно устранять недостатки оказанных Услуг, обнаруженные Сублицензиатом и (или) Лицензиатом в период оказания Услуг.

5.16. Сублицензиат вправе удержать суммы неисполненных Лицензиатом требований об уплате неустоек (штрафов, пеней), предъявленных Сублицензиатом в соответствии с Законом № 44-ФЗ, из суммы, подлежащей оплате Лицензиату.

5.17. Меры ответственности Сторон, не предусмотренные настоящим Договором, принимаются в соответствии с нормами законодательства Российской Федерации.

5.18. В случае обмена документами при применении мер ответственности и совершении иных действий в связи с нарушением Лицензиатом или Сублицензиатом условий Договора такой обмен осуществляется с использованием ЕИС путем направления электронных уведомлений. Такие уведомления формируются с использованием ЕИС, подписываются усиленной электронной подписью лица, имеющего право действовать от имени Сублицензиата, Лицензиата, и размещаются в ЕИС без размещения на официальном сайте.

6. Обстоятельства непреодолимой силы

6.1. Стороны не несут ответственности за полное или частичное неисполнение предусмотренных настоящим Договором обязательств, если такое неисполнение связано с обстоятельствами непреодолимой силы. К таким обстоятельствам, в частности, Стороны относят: стихийные бедствия; природные и промышленные катастрофы; террористические акты; военные действия; гражданские беспорядки; принятие органами государственной власти или органами местного самоуправления актов, содержащих запреты или ограничения в отношении деятельности Сторон по настоящему Договору, иные обстоятельства, которые не могут быть заранее предвидены или предотвращены Сторонами и делают невозможным исполнение обязательств Сторон по Договору.

6.2. Сторона, для которой создалась невозможность исполнения обязательств по настоящему Договору вследствие обстоятельств непреодолимой силы, не позднее трех дней с момента их наступления в письменной форме извещает другую Сторону с приложением документов, удостоверяющих факт наступления указанных обстоятельств.

6.3. Если обстоятельство непреодолимой силы непосредственно повлияло на исполнение обязательств в срок, установленный в настоящем Договоре, срок исполнения обязательств отодвигается соразмерно времени действия соответствующего обстоятельства, но не более чем на один месяц.

6.4. Если обстоятельства непреодолимой силы будут действовать свыше одного месяца, то каждая из Сторон вправе расторгнуть настоящий Договор, и в этом случае ни одна из Сторон не вправе требовать возмещения убытков.

6.5. Доказательством наличия обстоятельств непреодолимой силы и их продолжительности является соответствующее письменное свидетельство органов государственной власти Российской Федерации или Торгово-промышленной палаты Российской Федерации.

7. Порядок разрешения споров.

7.1. Все споры и разногласия между Сторонами, возникшие в результате исполнения Сторонами настоящего Договора, разрешаются в претензионном порядке.

7.2. Претензия одной Стороны должна быть рассмотрена другой Стороной в срок, не позднее, чем 10 (десять) календарных дней с момента получения претензии.

7.3. В случае неурегулирования споров и разногласий в претензионном порядке, спор подлежит разрешению в Арбитражном суде г. Москвы.

7.4. Во всем остальном, что не предусмотрено настоящим Договором, Стороны руководствуются действующим законодательством Российской Федерации.

8. Срок действия Договора. Порядок изменения и расторжения Договора

8.1. Настоящий Договор вступает в силу с даты его подписания и действует по **29.12.2023 года. (включительно),** а в части осуществления расчетов по Договору

и ответственности Сторон, предусмотренной Разделом 5 Договора, - до полного исполнения Сторонами взаимных обязательств. Окончание срока действия Договора не влечет прекращения неисполненных обязательств Сторон по Договору, в том числе гарантийных обязательств Исполнителя.

8.2. Изменение существенных условий настоящего Договора при его исполнении не допускается, за исключением случаев, предусмотренных Законом № 44-ФЗ.

8.3. Внесение изменений и дополнений, не противоречащих законодательству Российской Федерации, в условия Договора осуществляется путем заключения Сторонами в письменной форме дополнительных соглашений к Договору, которые являются его неотъемлемой частью.

8.4. В случае, предусмотренном Бюджетным кодексом Российской Федерации, при уменьшении ранее доведенных до Сублицензиата субсидий федерального бюджета, Сторонами осуществляется согласование изменения условий Договора.

8.5. При исполнении настоящего Договора не допускается перемена Лицензиата, за исключением случая, когда новый лицензиат является правопреемником Лицензиата по Договору вследствие реорганизации юридического лица в форме преобразования, слияния или присоединения.

Передача прав и обязанностей по Договору правопреемнику Лицензиата осуществляется путем заключения соответствующего дополнительного соглашения к Договору.

8.6. Расторжение Договора допускается по соглашению Сторон, по решению суда или в связи с односторонним отказом Стороны от исполнения Договора по основаниям, предусмотренным гражданским законодательством Российской Федерации и Законом № 44-ФЗ.

8.7. Сублицензиат вправе в одностороннем внесудебном порядке отказаться от исполнения Договора и расторгнуть его путем направления уведомления Лицензиату в случаях:

8.7.1. неисполнения Лицензиатом обязательств, предусмотренных настоящим Договором;

8.7.2. задержки Лицензиатом передачи неисключительных прав на использование антивирусного программного обеспечения более чем на 5 (пять) календарных дней по причинам, не зависящим от Сублицензиата;

8.7.3. ненадлежащего выполнения/невыполнения иных обязательств Лицензиатом по Договору;

8.7.4. в случае введения процедуры несостоятельности (банкротства) в отношении Лицензиата;

8.7.5. в случае если по каким-либо причинам обеспечение исполнения настоящего Договора перестало быть действительным, и Лицензиат не предоставил Сублицензиату иное (новое) надлежащее обеспечение исполнения настоящего Договора в сроки, установленные п. 9.9 настоящего Договора;

8.7.6. по иным основаниям, предусмотренным действующим законодательством Российской Федерации.

8.8. Договор будет считаться расторгнутым по основаниям, предусмотренным пунктом 8.7 настоящего Договора, по истечении 10 (десяти) календарных дней с даты надлежащего уведомления Лицензиата.

При этом Лицензиат обязан возместить все убытки Сублицензиату, связанные с односторонним расторжением Договора. Убытки Лицензиата, возникшие по основаниям, указанным в пункте 8.7 настоящего Договора, возмещению не подлежат.

8.9. Сублицензиат обязан принять решение об одностороннем отказе от исполнения настоящего Договора в связи с нарушением Лицензиатом существенных условий настоящего Договора в порядке, предусмотренном ст. 95 Закона № 44-ФЗ.

8.10. В реестр недобросовестных поставщиков включается информация о Лицензиате, не исполнившим или ненадлежащим образом исполнившим обязательства, предусмотренные Договором.

8.11. В случае прекращения финансирования Сублицензиата настоящий Договор подлежит расторжению по соглашению Сторон.

9. Обеспечение исполнения Договора

9.1. Размер обеспечения Договора устанавливается в размере 30% цены Договора, что составляет 268 666,72 руб..

В целях обеспечения исполнения обязательств по настоящему Договору Лицензиат представляет Сублицензиату обеспечение исполнения Договора в форме независимой гарантии, выданной организациями, перечисленными в части 1 статьи 45 Закона № 44-ФЗ, и соответствующей требованиям статьи 45 Закона № 44-ФЗ, или в форме внесения денежных средств на указанный Сублицензиатом счет, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими Сублицензиату[2].

9.2. В случае непредоставления участником закупки, с которым заключается Договор, обеспечения исполнения Договора в срок, установленный для заключения Договора, такой участник считается уклонившимся от заключения Договора.

9.3. В случае внесения Лицензиатом денежных средств в качестве обеспечения исполнения настоящего Договора, их возврат осуществляется Сублицензиатом в течение 15 (Пятнадцати) дней после выполнения Лицензиатом обязательств по договору.

9.4. Независимая гарантия, предоставленная в качестве обеспечения исполнения Договора, должна содержать условие об обязанности гаранта уплатить Сублицензиату (бенефициару) денежную сумму по независимой гарантии не позднее десяти рабочих дней со дня, следующего за днем получения гарантом требования Сублицензиата (бенефициара), соответствующего условиям такой независимой гарантии, при отсутствии предусмотренных Гражданским кодексом Российской Федерации оснований для отказа в удовлетворении этого требования. Срок действия независимой гарантии должен превышать срок исполнения обязательств не менее чем на один месяц.

9.5. В случае неисполнения/некачественного исполнения Лицензиатом обязательств по настоящему Договору из суммы обеспечения исполнения Договора Сублицензиатом может быть удержана сумма денежных средств, рассчитанных в соответствии с условиями Договора. В этом случае в адрес Лицензиата в течение 5 (пяти) рабочих дней со дня удержания Сублицензиатом направляется соответствующее уведомление об удержании, уменьшении денежных средств, внесенных в качестве обеспечения исполнения обязательств по Договору. При возврате суммы обеспечения исполнения Договора Лицензиат не вправе требовать от Сублицензиата удержанные денежные средства.

9.6. В ходе исполнения Договора Лицензиат вправе изменить способ обеспечения исполнения Договора и (или) предоставить Сублицензиату взамен ранее предоставленного обеспечения исполнения Договора новое обеспечение исполнения Договора, размер которого может быть уменьшен в порядке и случаях, которые предусмотрены пунктами 9.7 и 9.8 Договора.

9.7. Размер обеспечения исполнения Договора уменьшается посредством направления Сублицензиатом информации об исполнении Лицензиатом обязательств по исполнению Договора или об исполнении им отдельного этапа исполнения Договора и стоимости исполненных обязательств для включения в реестр контрактов, предусмотренный статьей 103 Закона № 44-ФЗ (далее - реестр контрактов). Уменьшение размера обеспечения исполнения Договора производится пропорционально стоимости исполненных обязательств, приемка и оплата которых осуществлены в порядке и сроки, которые предусмотрены Договором. В случае если обеспечение исполнения Договора осуществляется путем предоставления независимой гарантии, требование Сублицензиата об уплате денежных сумм по этой гарантии может быть предъявлено в размере не более размера обеспечения исполнения Договора, рассчитанного Сублицензиатом на основании

[2] Способ обеспечения исполнения договора, срок действия независимой гарантии определяются участником аукциона, с которым заключается договор, самостоятельно в соответствии с требованиями Закона № 44-ФЗ.

информации об исполнении Договора, размещенной в реестре контрактов. В случае, если обеспечение исполнения Договора осуществляется путем внесения денежных средств на счет, указанный Сублицензиатом, по заявлению Лицензиата ему возвращаются Сублицензиатом в установленный в пункте 9.3 Договора срок денежные средства в сумме, на которую уменьшен размер обеспечения исполнения Договора, рассчитанный Заказчиком на основании информации об исполнении Договора, размещенной в реестре контрактов.

9.8. Предусмотренное пунктами 9.6 и 9.7 Договора уменьшение размера обеспечения исполнения Договора осуществляется при условии отсутствия неисполненных Лицензиатом требований об уплате неустоек (штрафов, пеней), предъявленных Сублицензиатом в соответствии с разделом 5 Договора, а также приемки Сублицензиатом поставленных товаров, выполненных работ, оказанных услуг, результатов отдельного этапа исполнения Договора в объеме выплаченного аванса (если Договором предусмотрена выплата аванса) либо в объеме, превышающем выплаченный аванс (если в соответствии с законодательством Российской Федерации расчеты по Договору в части выплаты аванса подлежат казначейскому сопровождению). Такое уменьшение не допускается в случаях, определенных Правительством Российской Федерации в соответствии с частью 7.3 статьи 96 Закона № 44-ФЗ.

9.9. В случае отзыва в соответствии с законодательством Российской Федерации у банка, предоставившего независимую гарантию в качестве обеспечения исполнения Договора, лицензии на осуществление банковских операций, Лицензиат обязан предоставить новое обеспечение исполнения Договора не позднее одного месяца со дня надлежащего уведомления Сублицензиатом Лицензиата о необходимости предоставить соответствующее обеспечение. Размер такого обеспечения может быть уменьшен в порядке и случаях, которые предусмотрены статьей 96 Закона № 44-ФЗ. За каждый день просрочки исполнения Лицензиатом обязательства, предусмотренного настоящим пунктом Договора, начисляется пеня в размере, определенном в порядке, установленном пунктом 5.8 настоящего Договора.

9.10. Положения настоящего раздела Договора не применяются в случае заключения Договора с участником закупки, который является казенным учреждением.

9.11. Участник закупки, с которым заключается договор по результатам определения поставщика (подрядчика, исполнителя) в соответствии с пунктом 1 части 1 статьи 30 Закона № 44-ФЗ, освобождается от предоставления обеспечения исполнения Договора, в том числе с учетом положений статьи 37 Закона № 44-ФЗ, в случае предоставления таким участником закупки информации, содержащейся в реестре контрактов, заключенных заказчиками, и подтверждающей исполнение таким участником (без учета правопреемства) в течение трех лет до даты подачи заявки на участие в закупке трех контрактов, исполненных без применения к такому участнику неустоек (штрафов, пеней). Такая информация представляется участником закупки до заключения Договора в случаях, установленных Законом № 44-ФЗ для предоставления обеспечения исполнения контракта. При этом сумма цен таких контрактов должна составлять не менее начальной (максимальной) цены договора, указанной в извещении об осуществлении закупки и документации о закупке.

10. Конфиденциальность

10.1. Заключив Договор, Стороны могут получить доступ к информации, являющейся конфиденциальной информацией другой Стороны. К конфиденциальной информации относится вся информация, чётко обозначенная Сторонами как конфиденциальная.

10.2. Каждая из Сторон обязуется не раскрывать и не разглашать третьим лицам в общем или в частности факты или информацию, полученные ей от другой Стороны в соответствии с Договором, использовать конфиденциальную информацию другой Стороны только в целях выполнения Договора, кроме случаев, предусмотренных законодательством Российской Федерации. Обязанности по соблюдению конфиденциальности остаются в силе после прекращения действия Договора в течение трех лет.

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

11. Исключительные права третьих лиц

11.1. Лицензиат гарантирует, что исполнение его обязательств по Договору не повлечёт нарушения исключительных прав (авторских прав, патентов, лицензий и т.п.) третьих лиц, которые могут быть препятствием для использования результатов оказываемых услуг и документации Сублицензиатом на территории Российской Федерации.

11.2. В случае возникновения претензий или исков, предъявленных Сублицензиату со стороны третьих лиц, вызванных нарушением на территории Российской Федерации их исключительных прав (авторских прав, патентов, лицензий и т.п.) в связи с выполнением Лицензиатом обязательств по Договору, Сублицензиат:

- немедленно информирует об этом Лицензиата;
- проведет предварительные переговоры с третьей стороной;
- обеспечит возможность Лицензиату провести любые мероприятия по урегулированию претензий, исков и судебных разбирательств.

11.3. Лицензиат обязуется урегулировать такие претензии своими силами и за свой счёт, а также возместить Сублицензиату все убытки, вызванные нарушением Лицензиатом исключительных прав (авторских прав, патентов, лицензий и т.п.) третьих лиц на территории Российской Федерации.

11.4. По просьбе Лицензиата урегулирование таких претензий может осуществить Сублицензиат, в этом случае Лицензиат оплатит Сублицензиату все обоснованные расходы, связанные с урегулированием вышеуказанных нарушений, а также возместить Сублицензиату все убытки, вызванные нарушением Лицензиатом исключительных прав (авторских прав, патентов, лицензий и т.п.) третьих лиц.

12. Прочие условия.

12.1. Гарантия качества, устранение недостатков и дефектов предоставляется Лицензиатом в течение всего срока действия лицензии.

12.2. . Ответственным лицом за исполнение условий Договора от Сублицензиата представлен: **Алексеев Андрей Александрович, тел. +7 (495) 637-23-64 .**

Ответственным лицом за исполнение условий Договора от Лицензиата представлен **Дорофеев Дмитрий Олегович, тел. +7(385) 250-20-44.**

12.3. Вопросы, не урегулированные Договором, разрешаются в порядке, установленном действующим законодательством Российской Федерации.

12.4. Ни одна из Сторон не имеет права передавать третьему лицу права и обязательства по настоящему Договору без письменного согласия другой Стороны.

12.5. Все предусмотренные Договором заявления, извещения отправляются Сторонами посредством факсимильной связи по номерам, указанным в Договоре, и почтовыми отправлениями по адресам, указанным в Договоре в качестве почтовых адресов и впоследствии вручаются уполномоченному представителю Стороны-получателя.

12.6. Все документы, исходящие от Стороны по Договору и отправляемые в рамках исполнения Договора, должны быть подписаны уполномоченным лицом Стороны-отправителя.

12.7. Любое уведомление, запрос или согласие, выдача которых необходима в связи с настоящим Договором, оформляется в письменном виде и направляется одной Стороной другой Стороне любым доступным способом связи.

12.8. Договор остается в силе в случае изменения адресов, банковских реквизитов Сторон, изменения учредительных документов и организационно-правовой формы Сторон.

В случае их изменения Стороны обязаны в течение 10 (десяти) рабочих дней уведомить об этом друг друга в письменной форме.

12.9. Договор составлен в форме электронного документа, подписанного усиленными электронными подписями Сторон.

12.10. К настоящему Договору прилагаются и являются его неотъемлемой частью:

- Техническое задание (Приложение № 1);
- Расчет цены договора (Приложение № 2).

13. Адреса, реквизиты и подписи Сторон

Сублицензиат:
ФГБУ «НМИЦ ПН им. В.П. Сербского» Минздрава России

Юридический адрес:
119034, г. Москва, Кропоткинский пер., д.23
Фактический адрес : 119034, г. Москва, Кропоткинский пер., д. 23
Почтовый адрес: 119034, г. Москва, Кропоткинский пер., д. 23

ИНН 7704032379
ОГРН 1027700267737
КПП 770401001

ГУ Банка России по ЦФО//УФК
по г. Москве г. Москва
Казначейский счет
03214643000000017300
Единый казначейский счет (корр. сч.)
40102810545370000003
л/сч 20736X58400
(X - заглавная латиницей)
БИК 004525988
ОКТМО 45383000
ОКОПФ 75103
Дата поставки на учет
в налоговом органе: 13.02.1995
Телефон: (495) 637-40-00
Адрес эл.почты: info@serbsky.ru

От Сублицензиата :
ФГБУ «НМИЦ ПН им. В.П. Сербского» Минздрава России
Заместитель генерального директора
по финансово-экономическим вопросам

_____ / М.А. Юрасова/

М.П.

Лицензиат:
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "СОФТЕКС"

ИНН: 2225171231 КПП: 222501001
Тип поставщика: Юридическое лицо (РФ)
Юридический адрес: 656049, Российская Федерация, КРАЙ АЛТАЙСКИЙ, Г. БАРНАУЛ, УЛ. ПАРТИЗАНСКАЯ, Д. 132, ПОМЕЩ. Н21
Почтовый адрес: 656049, КРАЙ АЛТАЙСКИЙ22, Г БАРНАУЛ, УЛ ПАРТИЗАНСКАЯ, ДОМ 132, ПОМЕЩЕНИЕ Н21
Телефон: 73852502044
E-Mail: tender@softexgroup.ru
Банковские реквизиты: АЛТАЙСКОЕ ОТДЕЛЕНИЕ N8644 ПАО СБЕРБАНК
БИК: 040173604
Рас/с: 40702810902000015087
Кор/с: 30101810200000000604

От Лицензиата:
ООО "СОФТЕКС"
Генеральный директор

_____ /Д.О. Дорофеев/

М.П. (при наличии)

Приложение №1
к Сублицензионному договору
от «02» октября 2023г. № 140/10/2023ЦПН

Техническое задание
на оказание услуг по продлению и подключению неисключительных (пользовательских) прав на использование программного обеспечения –
универсальная лицензия антивирусной защиты (рабочие станции / файловые сервера / мобильные устройства) с функциями расширенного системного администрирования и шифрования данных на 12 месяцев

1. Место оказания услуг:
г. Москва, Кропоткинский пер., д.23.
г. Москва, ул. Потешная, д. 3, стр. 10,11
г. Москва, ул. Ставропольская д.27, стр.7
г. Москва, Малый Могильцевский пер., д.3

2. Условия оказания услуг: Доставка лицензии на бумажном и электронном носителе осуществляется силами и за счёт средств Исполнителя.
3. **Срок оказания услуг по продлению и подключению неисключительных (пользовательских) прав на использование программного обеспечения** - в течение 14 (четырнадцати) календарных дней с даты заключения Контракта.
4. Антивирусное программное обеспечение будет предоставлять Заказчику защиту информации корпоративной сети на **12 месяцев на 800 защищаемых объектов**. Лицензирование количества компонентов защиты рабочих станций и файловых серверов будет универсальным и ограничиваться только общим количеством защищаемых объектов в течение срока действия лицензионного соглашения. **Антивирусное программное обеспечение будет производить шифрование данных и включать модуль расширенного системного администрирования.**
Согласно Постановлению Правительства РФ от 16.11.2015 №1236 программное обеспечение будет включено в Единый реестр российских программ для электронных вычислительных машин и баз данных https://reestr.digital.gov.ru/reestr/

№ п/п	Наименование по ОКПД 2	Наименование объекта поставки	Единица измерения	Объем услуги (количество защищаемых объектов)
1.	Системы и средства обеспечения безопасности информации (программные, программно-аппаратные и аппаратные), такие как СЗИ НСД, защиты от утечек, антивирусной защиты и другие ОКПД2: 26.20.40.142	**Оказание услуг по продлению и подключению неисключительных (пользовательских) прав на использование программного обеспечения – универсальная лицензия антивирусной защиты (рабочие станции / файловые сервера / мобильные устройства) с функциями расширенного системного администрирования и шифрования данных на 12 месяцев** **Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License** **Страна происхождения: Россия** **Товарный знак/производитель: АО «Лаборатория Касперского»**	условная единица*	800

* за 1 условную единицу принято продление и подключение 1 лицензии

Заказчик имеет действующие соглашение № 1CE2-220901-040542-046-526от правообладателя АО «Лаборатория Касперского» на 760 (диапазон 500-999) защищаемых объектов (рабочие станции / файловые сервера / мобильные устройства). Срок окончания действия лицензионного ключа – 17.09.2023г.

Согласно пп. 1 части 1 статьи 33 ФЗ 44 "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" заказчику будут предоставлены в рамках услуги средства защиты информации, совместимые с существующим у Заказчика программным обеспечением KasperskyEndpointSecurity и KasperskySecurityCenter.

С целью принятия исчерпывающих мер по обеспечению антивирусной защиты информации к программному обеспечению, Исполнитель предоставит Заказчику право на:

- Использование новых версий антивирусного программного обеспечения и отдельных его модулей по мере их выхода (через сеть интернет).
- Использование услуг технической поддержки (по телефону и через сеть интернет).
- Доступ к информационным и вспомогательным ресурсам правообладателя программного обеспечения, в том числе к антивирусным базам данных, содержащие описания сигнатур угроз и сетевых атак, а также методы борьбы с ними.

5. Общие характеристики

5.1. Характеристики Антивирусных средств (будут включать):

- **Программные средства антивирусной защиты для рабочих станций Windows**;
- **Программные средства антивирусной защиты для файловых серверов Windows;**
- **Программные средства антивирусной защиты для рабочих станций MacOS**;
- **Программные средства антивирусной защиты для рабочих станций и серверов Linux**;
- **Программные средства антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows**;
- **Программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов)**;
- **Программные средства централизованного управления, мониторинга и обновления**;
- **Программные средства автоматизированного поиска и закрытия уязвимостей в установленных приложениях;**
- **Программные средства инвентаризации установленного программного обеспечения и оборудования;**
- **Программные средства шифрования данных;**
- **Обновляемые базы данных сигнатур вредоносных программ и атак;**
- **Эксплуатационную документацию на русском языке;**
- **Техническую поддержку;**
- **Универсальную лицензию антивирусной защиты для рабочих станций, файловых серверов, мобильных устройств с возможностью изменения соотношения защищаемых объектов в течение срока действия лицензионного соглашения в рамках приобретаемого числа лицензий.**

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

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

5.2 Характеристики программных средств антивирусной защиты для рабочих станций Windows

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

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 ивыше;
- Windows 8 Professional / Enterprise (32 / 64-разрядная);
- Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
- Windows 10 Home / Pro / Pro длярабочихстанций / Education / Enterprise;
- Windows 11 Home / Pro / Pro длярабочихстанций / Education / Enterprise.

В программном средстве антивирусной защиты будут 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 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 и 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 и 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, с возможностью настройки доверенных ресурсов и работой в режиме блокировки и 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 и разрешающих установку и запуск программ для всех и для определенных групп пользователей (Active Directory и локальных пользователей/групп), компонент будет контролировать приложения как по пути нахождения программы, метаданным, сертификату и его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент будет работать в режиме черного и белого списка, а также в режиме сбора статистики и блокировки;
- контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и 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 MTP устройствами и настройки правил доступа к устройствам этого типа для всех и для групп пользователей (Active Directory и локальных пользователей/групп), в рамках контроля устройств;
- записи в журнал событий о записи и 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 и разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
- защиты от атак типа BadUSB;
- защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
- управления параметрами через доверенные программы удаленного администрирования;
- установки только выбранных компонентов программного средства антивирусной защиты;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
- запуска задач по расписанию и 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 и 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 набором возможностей;
- интеграциис Windows Defender Security Center;
- наличиеподдержки Antimalware Scan Interface (AMSI);
- наличиеподдержки Windows Subsystem for Linux (WSL);
- защитить паролем восстановление объектов из резервного хранилища;
- ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
- наличие инструмента мониторинга сети по протоколам TCP и UDP;
- возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
- возможность установки ограничение длительности выполнения задачи;
- возможность ставить задачи проверки в очередь, если проверка уже выполняется;
- запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
- полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии SingleSignOn, поддержка UEFI-систем;
- восстановления зашифрованного содержимого в случае сбоев загрузочного агента и файлов ОС, поддержка UEFI-систем;
- поддержка двухфакторной аутентификации при полнодисковом шифровании;
- шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению);
- наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы за пределами организации с помощью пароля;
- шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;
- возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);
- возможность создавать служебную учетную запись агента аутентификации при шифровании диска;

• поддержка стороннего поставщика учетных данных ADSelfServicePlus для работы SSO при полнодисковом шифровании.

5.3 Характеристики программных средств антивирусной защиты для серверов Windows

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

• Windows Small Business Server 2011 Essentials / Standard (64-разрядная), Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживаетсятолькосустановленным Service Pack 1 для Microsoft Windows Server 2008 R2;
• Windows MultiPoint Server 2011 (64-разрядная);
• Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 ивыше;
• Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
• Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
• Windows Server 2016 Essentials / Standard / Datacenter;
• Windows Server 2019 Essentials / Standard / Datacenter;
• Windows Server 2022.

В программном средстве антивирусной защиты будут 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 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 и файлу;
• антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
• встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
• защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
• защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников и 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 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 и 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 набором возможностей;
- интеграциис Windows Defender Security Center;
- наличиеподдержки Antimalware Scan Interface (AMSI);
- наличиеподдержки Windows Subsystem for Linux (WSL);
- защитить паролем восстановление объектов из резервного хранилища;
- импорта и экспорта списков правил и исключений в XML-формат;
- ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
- создания специальных правил, запрещающих и разрешающих установку и запуск программ для всех и для определенных групп пользователей (Active Directory и локальных пользователей/групп), компонент будет контролировать приложения как по пути нахождения программы, метаданным, сертификату и его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент будет работать в режиме черного и белого списка, а также в режиме сбора статистики и блокировки;
- формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);
- запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
- поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов;
- возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
- возможность установки ограничения длительности выполнения задачи;
- возможность ставить задачи проверки в очередь, если проверка уже выполняется.

5.4 Характеристики программных средств антивирусной защиты для рабочих станций и серверов Linux

Программные средства антивирусной защиты для рабочих станций Linux будут функционировать на компьютерах, работающих под управлением 32-битных операционных систем следующих версий:
- CentOS 6.7 и выше.
- Debian GNU/Linux 10.1 и выше.
- Debian GNU/Linux 11.
- Mageia 4.
- Red Hat Enterprise Linux 6.7 ивыше.
- Альт 8 СП Рабочая Станция.
- Альт 8 СП Сервер.
- Альт Образование 10.
- Альт Рабочая Станция 10.

Программные средства антивирусной защиты для рабочих станций Linux будут функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий:
- AlmaLinux OS 8 и выше.
- AlmaLinux OS 9 и выше.
- AlterOS 7.5 ивыше.
- Amazon Linux 2.
- Astra Linux Common Edition 2.12.
- Astra Linux Special Edition РУСБ.10015-01 (очередноеобновление 1.5).
- Astra Linux Special Edition РУСБ.10015-01 (очередноеобновление 1.6).
- Astra Linux Special Edition РУСБ.10015-01 (очередноеобновление 1.7).
- AstraLinuxSpecialEditionРУСБ.10015-16 (исполнение 1) (очередноеобновление 1.6).

- CentOS 6.7 и выше.
- CentOS 7.2 и выше.
- CentOS Stream 9.
- Debian GNU/Linux 10.1 ивыше.
- Debian GNU/Linux 11.
- EMIAS 1.0.
- EulerOS 2.0 SP5.
- LinuxMint 19.2 ивыше.
- LinuxMint 20.3 ивыше.
- openSUSE Leap 15.0 ивыше.
- Oracle Linux 7.3 ивыше.
- Oracle Linux 8.0 ивыше.
- Red Hat Enterprise Linux 6.7 ивыше.
- Red Hat Enterprise Linux 7.2 ивыше.
- Red Hat Enterprise Linux 8.0 ивыше.
- Red Hat Enterprise Linux 9.
- Rocky Linux 8.5 ивыше.
- SUSE Linux Enterprise Server 12.5 ивыше.
- SUSE Linux Enterprise Server 15 ивыше.
- Ubuntu 20.04 LTS.
- Ubuntu 22.04 LTS.
- Альт 8 СПРабочаястанция.
- Альт 8 СП Сервер.
- Альт Образование 10.
- Альт Рабочая Станция 10.
- Альт Сервер 10.
- Атлант, сборка Alcyone, версия 2022.02.
- Гослинукс 7.17.
- Гослинукс 7.2.
- РЕД ОС 7.3.
- РОСА "Кобальт" 7.9.
- РОСА "Хром" 12.
- ОСОН "ОСНова".

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

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

В программном средстве антивирусной защиты будут 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 и файлу;
- проверку ресурсов доступных по SMB / NFS;
- возможность проверки памяти ядра;
- эвристический анализатор, позволяющий эффективно распознавать и блокировать неизвестные вредоносные программы;
- антивирусное сканирование по команде пользователя и 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;
- 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 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 и веб-консоли;
- управления доступом пользователей к установленным и 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 и фишинговым;
- получения данных о действиях программ на компьютере пользователя;
- получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация);
- создание файлов трассировки при запуске программы;
- получение информации обо всех исполняемых файлах программ, установленных на компьютерах;
- проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;
- сохранение резервных копий файлов перед лечением и удалением и восстановление файлов из резервных копий.

5.5 Характеристики программных средств антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows

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

32-разрядных операционных систем Microsoft Windows

- WindowsServer 2003 Standard / Enterprise / Datacenterспакетомобновлений SP2 и выше;
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter спакетомобновлений SP2 и выше;
- Windows Server 2008 Standard / Enterprise / Datacenter спакетомобновлений SP2 и выше;
- Windows Server 2008 Core Standard / Enterprise / Datacenter спакетомобновлений SP2 и выше.

64-разрядныхоперационныхсистем Microsoft Windows

- Windows Server 2003 Standard / Enterprise / Datacenter спакетомобновлений SP2 и выше;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter спакетомобновлений SP2 и выше;
- Windows Server 2008 Core Standard / Enterprise / Datacenter спакетомобновлений SP2 и выше;
- Windows Server 2008 Standard / Enterprise / Datacenter спакетомобновлений SP2 и выше;
- Microsoft Small Business Server 2008 Standard / Premium SP2 и выше;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter спакетомобновлений SP1 и выше;
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter спакетомобновлений SP1 и выше;
- Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 и выше;
- Microsoft Small Business Server 2011 Essentials / Standard SP1 и выше;

- Microsoft Windows MultiPoint Server 2011 Standard / Premium;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
- Microsoft MultiPoint Server 2012 Standard / Premium;
- Windows Storage Server 2012;
- Windows Hyper-V Server 2012;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Hyper-V Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2016 MultiPoint;
- Windows Server 2016 Core Standard / Datacenter;
- Microsoft Windows MultiPoint Server 2016;
- Windows Storage Server 2016;
- Windows Hyper-V Server 2016;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2019 Core;
- Windows Storage Server 2019;
- Windows Hyper-V Server 2019;
- Windows Server 2022;
- Windows 10 Enterprisemulti-session.

В программном средстве антивирусной защиты будут 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 и администратора и по расписанию;
- запуск задач по расписанию и 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 и 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 MicrosoftWindowsScriptTechnologies (и 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;
- проверки контейнеров Microsoft Windows;
- защиты от эксплуатирования уязвимостей в памяти процессов;
- будет возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не будут 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 и неквалифицированных пользователей, а также запрещающий и 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 и выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов;
- контроль устройств, в том числе сетевых карт и модемов;
- веб-контроль;
- защита от почтовых угроз (плагин для Outlook);
- защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика будет осуществляться с помощью драйвера перехвата и с помощью его перенаправления;
- создания специальных правил, запрещающих и разрешающих установку и запуск программ для всех и для определенных групп пользователей (Active Directory и локальных пользователей/групп);
- создания специальных правил будет контролировать приложения по пути нахождения программы, метаданным, сертификату и его отпечатку, контрольной сумме;
- создания специальных правил будет работать в режиме черного и белого списка, а также в режиме сбора статистики и блокировки, будет иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
- осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
- осуществление контроля работы с сетью Интернет, в том числе включение явного запрета и разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем;
- информирование администратора о подключении внешних устройств;
- наличие механизмов автоматической генерации правил для контроля устройств и приложений.

5.6. Характеристики программных средств антивирусной защиты мобильных устройств

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

- Android 5.0–13 (включая Android 12L, исключая Go Edition);
- iOS 10–16 и iPadOS 13–15;

В программном средстве антивирусной защиты смартфонов для ОС Android будут 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 FirebaseCloudMessaging (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 (factoryreset);
- 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 будут 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 ExchangeActiveSync\ 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 supervisedmode;
- централизованного управления с помощью единой консоли управления;
- наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari и Game Center, на управляемом устройстве.

5.7. Характеристики программных средств централизованного управления, мониторинга и обновления на базе ОС Windows

Программные средства централизованного управления, мониторинга и обновления будут функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
- Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro длярабочихстанций RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H2 32-разрядная/64-разрядная;

- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 11 Home 64-разрядная;
- Microsoft Windows 11 Pro 64-разрядная;
- Microsoft Windows 11 Enterprise 64-разрядная;
- Microsoft Windows 11 Education 64-разрядная;
- Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная;
- Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 8 Pro 32-разрядная/64-разрядная;
- Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 7 Professional Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 R2 with Standard Service Pack 1 ивыше 64-разрядная;
- Windows Server 2008 R2 Service Pack 1 (всередакции) 64-разрядная;
- Windows Server 2012 Server Core 64-разрядная;
- Windows Server 2012 Datacenter 64-разрядная;
- Windows Server 2012 Essentials 64-разрядная;
- Windows Server 2012 Foundation 64-разрядная;
- Windows Server 2012 Standard 64-разрядная;
- Windows Server 2012 R2 Server Core 64-разрядная;
- Windows Server 2012 R2 Datacenter 64-разрядная;
- Windows Server 2012 R2 Essentials 64-разрядная;
- Windows Server 2012 R2 Foundation 64-разрядная;
- Windows Server 2012 R2 Standard 64-разрядная;
- Windows Server 2016 Datacenter (LTSB) 64-разрядная;
- Windows Server 2016 Standard (LTSB) 64-разрядная;
- Windows Server 2016 (вариантустановки Server Core) (LTSB) 64-разрядная;
- Windows Server 2019 Standard 64-разрядная;
- Windows Server 2019 Datacenter 64-разрядная;
- Windows Server 2019 Core 64-разрядная;
- Windows Server 2022 Standard 64-разрядная;
- Windows Server 2022 Datacenter 64-разрядная;
- Windows Server 2022 Core 64-разрядная;
- Windows Storage Server 2012 64-разрядная;
- Windows Storage Server 2012 R2 64-разрядная;
- Windows Storage Server 2016 64-разрядная;
- Windows Storage Server 2019 64-разрядная.

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

- VMware vSphere 6.7;
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper-V Server 2012 64-разрядная;

- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная;
- Microsoft Hyper-V Server 2019 64-разрядная;
- Microsoft Hyper-V Server 2022 64-разрядная;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- Parallels Desktop 17;
- Oracle VM VirtualBox 6.x.

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

- Microsoft SQL Server 2012 Express 64-разрядная;
- Microsoft SQL Server 2014 Express 64-разрядная;
- Microsoft SQL Server 2016 Express 64-разрядная;
- Microsoft SQL Server 2017 Express 64-разрядная;
- Microsoft SQL Server 2019 Express 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;
- Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная;
- Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная (дополнительные действия);
- Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (дополнительные действия);
- MicrosoftAzureSQLDatabase;
- Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;
- MySQL 5.7 Community 32-разрядная/64-разрядная;
- MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;
- MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;
- MariaDB 10.5.x 32-разрядная/64-разрядная;
- MariaDB 10.4.x 32-разрядная/64-разрядная;
- MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;
- MariaDBServer 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
- MariaDBGaleraCluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
- MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

В программном средстве антивирусной защиты будут 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 и 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 ExchangeActiveSync;
- 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;
- поддержкаинтеграциис Windows сервисом Certificate Authority;
- наличие портала самообслуживания пользователей;
- портал самообслуживания будет 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 MicrosoftAzure и GoogleCloud;
- интеграции по OpenAPI;
- управления антивирусной защитой с использованием WEB консоли;
- возможность управления развертыванием ОС Windows через консоль управления;
- наличие преднастроенных ролей пользователей средств централизованного управления;
- будет реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей;
- возможность подключения по RDP и штатными средствами из консоли управления;

- наличие возможности совместного подключения к рабочему столу Windows (WindowsDesktopSharing);
- пользователю будет выводиться запрос на разрешение дистанционного подключения;
- наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической и виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (baremetal);
- будет обеспечена возможность добавления наборов драйверов в ранее созданный образ;
- возможность запускать скрипты и устанавливать дополнительное ПО в автоматическом режиме после установки ОС;
- возможность импортировать образ операционной системы из дистрибутивов (WIM);
- наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией и превышении срока действия лицензии;
- автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры;
- поддержка функциональности управления шифрованием данных;
- возможность интеграции с SIEM системами и передача событий в формате syslog и CEF\ LEEF
- двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;
- использования дополнительной аутентификация после изменения параметров учетной записи пользователя;
- возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами;
- автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
- возможность развернуть Сервер администрирования как систему высокой доступности;
- возможность устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети.

5.8 Характеристики программных средств централизованного управления, мониторинга и обновления на базе ОС Linux

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

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

- Oracle Linux 8 64-разрядная;
- РЕД ОС 7.3 Сервер 64-разрядная;
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

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

- VMware vSphere 6.7.
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper-V Server 2012 64-разрядная;
- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная;
- Microsoft Hyper-V Server 2019 64-разрядная;
- Microsoft Hyper-V Server 2022 64-разрядная;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- ParallelsDesktop 17;
- Виртуальная машина на основе Kernel. Поддерживает следующие операционные системы:
- Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
- Альт Сервер 10 64-разрядная;
- Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
- Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная;
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
- РЕД ОС 7.3 Сервер 64-разрядная;
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная

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

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

В программном средстве антивирусной защиты будут 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.

5.9. Характеристики обновления антивирусных баз

Обновляемые антивирусные базы данных будут обеспечивать реализацию следующих функциональных возможностей:
• создания правил обновления антивирусных баз 24 раза 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.

5.10. Характеристики эксплуатационной документации

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, будет включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:
• «Руководство пользователя (администратора)»
Документация, поставляемая с антивирусными средствами, будет детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

5.11. Характеристики технической поддержки

Техническая поддержка антивирусного программного обеспечения будет:
• 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 будет на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.

5.12. Характеристики поставки антивирусного программного обеспечения и сертификатов соответствия

Исполнитель подтверждает передачу неисключительных прав на использование антивирусного программного обеспечения путём предоставления:
• Лицензионного соглашения между заказчиком и компанией разработчиком антивирусного программного обеспечения, подтверждающее право на использование и поддержку антивирусного

программного обеспечения в течение указанного срока и количества. Лицензия для рабочих станций / файловых серверов / мобильных устройств будет универсальной и обеспечивать возможность изменения соотношения защищаемых объектов в течение срока действия лицензионного соглашения в рамках приобретаемого числа лицензий.

6. Гарантии

6.1. Гарантия качества оказанных Услуг и устранение недостатков и дефектов оказанных Услуг предоставляется Исполнителем на 12 (двенадцать) месяцев с даты заключения Контракта.

От Сублицензиата :	
ФГБУ «НМИЦ ПН им. В.П. Сербского» Минздрава России	От Лицензиата: ООО "СОФТЕКС"
Заместитель генерального директора по финансово-экономическим вопросам	Генеральный директор
_____ / М.А. Юрасова/	_____ /Д.О. Дорофеев/
М.П.	М.П. (при наличии)

Приложение № 2
к Сублицензионному договору
от «02» октября 2023г. № 140/10/2023ЦПН

Расчет цены Договора

№ п/п	Наименование по КТРУ/ОКПД2	Наименование	Ед. изм.	Кол-во	Цена за единицу, НДС не облагается	Сумма, НДС не облагается	Ставка НДС
1.	Системы и средства обеспечения безопасности информации (программные, программно-аппаратные и аппаратные), такие как СЗИ НСД, защиты от утечек, антивирусной защиты и другие, ОКПД2: 26.20.40.142	Оказание услуг по продлению и подключению неисключительных (пользовательских) прав на использование программного обеспечения – универсальная лицензия антивирусной защиты (рабочие станции / файловые сервера / мобильные устройства) с функциями расширенного системного администрирования и шифрования данных на 12 месяцев Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License **Страна происхождения:** Россия **Товарный знак/производитель:** АО «Лаборатория Касперского» https://reestr.digital.gov.ru/reestr/301482/	условная единица*	799	1 119,44	894 432,56	НДС не облагается в соответствии пп.26 п.2 ст.149 НК РФ
				1	1 123,16	1 123,16	
	ИТОГО: 895 555,72 (Восемьсот девяносто пять тысяч пятьсот пятьдесят пять) рублей 72 копейки. НДС не облагается в соответствии с пп. 26 п. 2. ст. 149 Налогового кодекса Российской Федерации.					**895 555,72**	

От Сублицензиата :
ФГБУ «НМИЦ ПН им. В.П. Сербского»
Минздрава России
Заместитель генерального директора
по финансово-экономическим вопросам

_____ / М.А. Юрасова/

М.П.

От Лицензиата:
ООО "СОФТЕКС"
Генеральный директор

_____ /Д.О. Дорофеев/

М.П. (при наличии)

Заключен контракт по процедуре 0373100113723000140
Заказчик: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ "НАЦИОНАЛЬНЫЙ МЕДИЦИНСКИЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР ПСИХИАТРИИ И НАРКОЛОГИИ ИМЕНИ В.П. СЕРБСКОГО" МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Участник: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "СОФТЕКС"
Начальная цена контракта: 900 056
Итоговая цена контракта: 895 555,72
Файл контракта: Договор 140-10-2023ЦПН.docx 98d63c5d10929454f8f127e778848aab

Контракт подписан заказчиком:
Владелец сертификата: Шаклеин Константин Николаевич
Организация: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ "НАЦИОНАЛЬНЫЙ МЕДИЦИНСКИЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР ПСИХИАТРИИ И НАРКОЛОГИИ ИМЕНИ В.П. СЕРБСКОГО" МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Должность: Заместитель генерального директора по организационным вопросам
Город: г. Москва
Страна: RU
Контрольная сумма подписанного документа:
e5c24082f75c851c97d8d74db74882db09a0483af1eb89a6d0cdf7aa92652680
Алгоритм шифрования: ГОСТ Р 34.11/34.10-2001
Дата подписания: 02.10.2023 10:32 [GMT +3]

Контракт подписан участником:
Владелец сертификата: ООО "СОФТЕКС"
Фамилия, имя, отчество: ДОРОФЕЕВ ДМИТРИЙ ОЛЕГОВИЧ
Организация: ООО "СОФТЕКС"
Должность: ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
Город: БАРНАУЛ ГОРОД
Страна: RU
Контрольная сумма подписанного документа:
a6daf642310138bfb612fbb6b376dc93ff659beeb4b63e7956768d1ee6d70d33
Алгоритм шифрования: ГОСТ Р 34.11/34.10-2001
Дата подписания: 27.09.2023 16:03 [GMT +3]