«УТВЕРЖДАЮ»

Председатель Закупочной комиссии

Первый заместитель генерального

директора СП ООО «СамАвто»

_____ М.М. Ганиев

«_____» _____г.

ЗАКУПОЧНАЯ ДОКУМЕНТАЦИЯ
по отбору наилучших предложений на обновление антивируса до 450 лицензий сроком на 2 года согласно ТЗ
СП ООО «САМАВТО»

Заказчик:

СП ООО «Самаркандский автомобильный завод»

Самарканд-2022

В настоящей документации применяются следующие основные понятия:

Отбор – вид осуществления конкурентной закупочной процедуры, победителем которого признается участник, предложивший лучшие условия исполнения договора (далее по тексту «Отбор»);

Заказчик – основной инициатор закупки, покупатель - юридическое лицо, осуществляющее государственные закупки (далее по тексту «Заказчик»);

Закупочная комиссия (закупочная комиссия) – постоянный орган, осуществляющий проведение отбора, создаваемый с целью реализации принципов государственных закупок и обеспечения независимости принимаемых решений при проведении закупочных процедур (далее по тексту «Комиссия»);

Закупочная документация – документ, состоящий из нескольких частей, включающий инструктаж, условия и требования, предоставляемые для участников с целью подготовки предложения;

Претендент – хозяйствующий субъект, заявивший о своем намерении участвовать в отборе на предложенных условиях;

ИУО – инструкция участника отбора;

ИТО – информационная таблица отбора;

Квалификационные документы – перечень документов, необходимых для прохождения претендентом квалификационного отбора;

Предложение – форма выражения согласия претендента осуществить работу в соответствии с требованиями и условиями отбора;

Участник – претендент, прошедший квалификационный отбор и допущенный к участию в отборе с наличием товара в случае признания победителем;

Победитель – участник, предложивший наилучшее предложение по результатам изучения, оценки и сопоставления;

Обеспечение участия – согласно статье закона «предоставление участником заказчику гарантий по обеспечению выполнения им обязательств, возникающих в связи с подачей предложений»;

Критерии оценки - показатели, используемые для оценки предложений участников;

Специальный информационный портал (далее — портал) — веб-сайт и специальная электронная платформа оператора, обеспечивающие проведение государственных закупок, размещение и доступ к просмотру в электронной форме объявлений о государственных закупках, информации об итогах государственных закупок, предложениях участников отбора и иной информации, предусмотренной законодательством, а также проведение электронных государственных закупок.

I. ИНСТРУКЦИЯ ДЛЯ УЧАСТНИКА ОТБОРА

1 Общие положения.

1.1 Настоящая инструкция разработана в соответствии с Законом Республики Узбекистан «О государственных закупках» №684 от 22.04.20218 года. При проведении электронного отбора посредством использования информационно-коммуникационных технологий процедура электронного отбора регулируется соответствующими нормативными актами Республики Узбекистан.

1.2 Предмет отбора: **обновление антивируса до 450 лицензий сроком на 2 года согласно ТЗ**

1.3 Предельная стоимость закупа составляет:

255 384 640 сум (двести пятьдесят пять миллионов триста восемьдесят четыре тысячи шестьсот сорок сум ноль тийинов) с учетом НДС Цены, указанные в отборном предложении, не должны превышать предельную стоимость.

Условия оплаты: 15% предоплата, остальные 85% после предоставления лицензий и закрытия сопутствующих документов.

Условия поставки: согласно запросу Заказчика в течении 5 дней.

1.5 Технические требования к услугам представлено в технической части закупочной документации по отбору.

1.6 Форма заседании и закупочной комиссии могут проходить очной или заочной (путем опроса без совместного присутствия) форме.

2 Организатор отбора

2.1 Место проведения отбора: СП ООО «Самаркандский автомобильный завод» г. Самарканд, 140160, ул. С. Бухорий, 5.

2.2 Рабочим органом комиссии является Департамент материального снабжения (далее-«Рабочий орган»).

Адрес: г. Самарканд, 140160, ул. С. Бухорий, 5

Контактный телефоны: +998909747244;

Fax: +998 998662223839.

e – mail: saminfo@samauto.uz

Контактное лицо: Рзаев А.С., специалист по закупкам Департамента материального снабжения.

2.3 Отбор проводится закупочной комиссией, созданной Заказчиком, в составе не менее пяти членов.

2.4 Контрактодержатель: СП ООО «Самаркандский автомобильный завод»

3 Участники отбора

3.1 В отборе наилучших предложений (конкурс) могут принять участие резиденты и нерезиденты Республики Узбекистан, за исключением лиц приведенных в пункте 4.2 настоящей закупочной документации отбора наилучших предложений.

4 Порядок проведения отбора

4.1 Для участия в отборе, участник отбора должен:

а) получить (скачать) электронную версию закупочной документации по отбору, размещенной на специальном информационном портале для ознакомления с условиями отбора;

б) подать в электронном виде предложение (https://etender.uzex.uz/ в соответствии с требованиями закупочной документации.

Перед началом отбора, закупочной комиссией производится квалификационный отбор претендентов. К дальнейшему участию в конкурсе допускаются только те претенденты, которые прошли квалификационный отбор. В исключительных случаях по усмотрению закупочной комиссией могут быть допущены участники, не прошедшие квалификационный отбор.

Перечень документов, необходимых для проведения квалификационного отбора представлен в приложении №1 (формы №1,2,3,4) к настоящей инструкции.

Критерии квалификационной оценки представлены в Приложении №2

4.2 К участию в отборе не допускаются участники:

не предоставившие в установленный срок пакет необходимых документов для квалификационного отбора;

находящиеся на стадии реорганизации, ликвидации или банкротства;

находящиеся в состоянии судебного или арбитражного разбирательства с «Заказчиком»;

находящиеся в Едином реестре недобросовестных исполнителей;

имеющиеся просроченные задолженности по уплате налогов и сборов;

не имеющие необходимых технических, финансовых, материальных, кадровых и других ресурсов для исполнения договора.

зарегистрированные и имеющие банковские счета в государствах или на территориях, предоставляющих льготный налоговый режим и/или не предусматривающих раскрытие и предоставление информации при проведении финансовых операций (оффшорные зоны).

4.3 Заказчик отстраняет участника от участия в закупочных процедурах, если:

участник не соответствует квалификационным, техническим и коммерческим требованиям закупочной документации;

участник прямо или косвенно предлагает, дает или соглашается дать любому нынешнему либо бывшему должностному лицу или работнику заказчика, или другого государственного органа вознаграждение в любой форме, предложение о найме на работу, либо любую другую ценную вещь или услугу с целью повлиять на совершение какого-либо действия, принятие решения или применение какой-либо отборной процедуры заказчика в процессе государственных закупок;

у участника имеется несправедливое конкурентное преимущество или конфликт интересов в нарушение законодательства;

участник совершает антиконкурентные действия или в нарушение законодательства имеет конфликт интересов, а также при выявлении случаев аффилированности.

5 Язык отбора.

5.1 Предложение и вся связанная с ним корреспонденция, и документация должны быть на узбекском, русском языке или на английском.

В отборном предложении должна быть использована метрическая система измерений.

6 Предложение и порядок его оформления

6.1 Участники отбора, объявленного на портале, предоставляют предложения в электронном виде по установленному в объявлении порядку https://etender.uzex.uz/

6.2 Участник отбора:

несет ответственность за подлинность и достоверность предоставляемых информации и документов;

вправе подать только одно предложение на один лот;

вправе отозвать или внести изменения в поданное предложение до срока окончания подачи таких предложений.

6.3 Предложение должно состоят из:

техническая часть должна соответствовать техническим требованиям Заказчика и содержать в себе подробное техническое описание предлагаемой работы;

6.4 Требования к наличию обязательных документов в технической части предложения.

Пакет технической части предложения должен содержать следующие документы:

Подробное техническое описание работ, описание соответствия предложенной работы технической части настоящей инструкции.

Подтверждение от исполнителя работ в случае, если участник отбора является представителем исполнителя работ.

Перечень технической документации (брошюры, технические паспорта, инструкция по эксплуатации и т.п. или иные документы, содержащие полное и подробное описание предлагаемой работы).

6.5 Срок действия предложения участников должен составлять не менее 30 дней со дня окончания представления предложений.

7	**Продление срока предоставления отборных предложений**	7.1	В случае необходимости, заказчик может продлить срок представления предложений.
		7.2	Информация о продлении сроков представления предложений размещается на специальном информационном портале.
8	**Внесение изменений в закупочную документацию**	8.1	В случае необходимости заказчик вправе принять решение о внесении изменений в закупочную документацию. Решение о внесении изменений в закупочную документацию может приниматься не позднее чем за три дня до даты окончания срока подачи предложений. В процессе внесения изменений в закупочную документацию изменение продукции (работ, услуг) или ее характеристики не допускается. В случае внесения изменений в отборную документацию в срок окончания подачи предложений, отбор продлевается не менее чем на пять дней с даты внесения изменений в отборную документацию. Одновременно с этим вносятся изменения в объявление о проведении отбора, если была изменена информация, указанная в объявлении.
9	**Порядок и критерии оценки предложений**	9.1	Время, указанное в объявлении как время проведения отбора, закупочная комиссия для проведения оценки предложений рассматривает поданные предложения, поданными участниками отбора.
		9.2	Срок рассмотрения и оценки предложений участников отбора не может превышать десяти дней с момента окончания подачи предложений.
		9.3	При рассмотрении предложений проверяется наличие в них всех документов и правильность их оформления. В случае отсутствия соответствующих документов, закупочная комиссия вправе не допускать данное предложение к рассмотрению и оценке.
		9.4	Закупочная комиссия осуществляет оценку предложений, которые небыли отклонены, для выявления победителя отбора на основе критериев, указанных в закупочной документации по отбору.
		9.5	В случае установления недостоверности информации, содержащейся в документах, представленных участником отбора, закупочная комиссия вправе отстранить такого участника от участия в отборе на любом этапе отбора.
		9.6	Оценка предложений и определение победителя отбора производятся на основании критериев, изложенных в закупочной документации по отбору.
		9.7	Предложение признается надлежаще оформленным, если оно соответствует требованиям действующего законодательства Республики Узбекистан и закупочной документации по отбору.

9.8 Закупочная комиссия отклоняет предложение, если подавший его участник отбора не соответствует требованиям, установленным Законом и постановлением или предложение участника отбора не соответствует требованиям закупочной документации по отбору.

9.9 В процессе оценки предложений закупочная комиссия может запрашивать у участников отбора разъяснения по поводу их предложений. В процессе разъяснения не допускаются какие-либо изменения по сути предложения, а также по цене. Также участники отбора до завершения срока принятия предложений могут направлять запросы для разъяснения положений настоящей документации в форме официального запроса.

9.10 Если участники отбора представят предложения в разных валютах, суммы предложений при оценке будут пересчитаны в единую валюту по курсу Центрального банка Республики Узбекистан на дату проведения конкурса. Если участники отбора представят предложения на разных условия поставки суммы предложений при оценке будут пересчитаны с учетом налогов, обязательных сборов и пошлин.

9.11 Победителем признается участник отбора, предложивший лучшие условия исполнения договора на основе критериев, указанных в закупочной документации по отбору.

9.12 При наличии арифметических или иных ошибок закупочная комиссия вправе отклонить предложение либо определить иные условия их дальнейшего рассмотрения, известив об этом участника отбора.

9.13 В целях корректного сравнения цен иностранных и отечественных участников отбора, при оценке будут учтены соответствующие расходы (налоги, таможенные платежи и иные обязательные платежи), в случаях, предусмотренных действующим законодательством Республики Узбекистан.

9.14 Результаты рассмотрения предложений фиксируются в протоколе рассмотрения предложений.

9.15 Протокол рассмотрения предложений подписывается всеми членами закупочной комиссии и публикуется на специальном информационном портале в сроки согласно действующего законодательство Республики Узбекистан.

9.16 Любой участник в течение двух рабочих дней после публикации протокола рассмотрения предложений вправе направить заказчику запрос о предоставлении разъяснений результатов отбора. В течение трех рабочих дней с даты поступления такого запроса заказчик обязан представить участнику отбора соответствующие разъяснения.

10 Ответственность сторон и соблюдение конфиденциальности

10.1 Ответственность за соблюдение конфиденциальности, предусмотренной законодательством Республики Узбекистан, несут:
председатель и члены закупочной комиссии, а также члены рабочей группы, созданной для изучения предложений, за разглашение информации, допущение сговора с участниками, остальными членами комиссии и

привлеченными экспертами, а также за другие противоправные действия.

10.2 Победитель отбора наилучших предложений, не исполнивший обязательства по договору (по количественным, качественным и техническим параметрам), несет ответственность, предусмотренной законодательством Республики Узбекистан и/или заключенным договором.

11 Прочие условия

11.1 Участники подавшие предложения на участие в отборе согласны с условиями и критериями оценки предложений настоящей инструкции. В случае если участники, изъявившие желание участвовать в отборе, не согласны с условиями и критериями оценки предложений настоящей инструкции могут направлять официальное письмо в рабочий орган с предложениями о внесении изменений в закупочную документацию до завершения отбора и не должны подавать предложения на участия в отборе.

11.2 Участник отбора вправе направить Заказчику запрос о даче разъяснений положений закупочной документации в форме, определенной в объявлении на проведение отбора. В течение трех рабочих дней с даты поступления указанного запроса заказчик обязан направить в установленной форме разъяснения положений закупочной документации, если указанный запрос поступил к заказчику не позднее чем за три дня до даты окончания срока подачи предложений. Разъяснения положений закупочной документации не должны изменять ее сущность.

11.3 Отбор может быть объявлен закупочной комиссией не состоявшимися:

если в отборе принял участие один участник или никто не принял участие;

если по результатам рассмотрения предложений закупочная комиссия отклонила все предложения ввиду не соответствия требованиям закупочной документации по отбору;

11.4 Заказчик имеет право отменить отбор в любое время до акцепта выигравшего предложения. Заказчик в случае отмены отбора публикует обоснованные причины данного решения на специальном информационном портале.

12 Заключение договора

12.1 По результатам отбора договор заключается на условиях, указанных в закупочной документации по отбору и предложении, поданном участником отбора, с которым заключается договор.

12.2 Заказчик имеет право вступать в переговоры с победителем отбора о снижении цены.

12.3 В случае, если победитель отбора отказывается заключать договор на условиях отбора, право заключения договора переходит к резервному исполнителю. При этом, резервный Исполнитель может заключить договор по цене, предложенной победителем отбора, или отказаться от заключения договора.

Приложение №1

ПЕРЕЧЕНЬ

Квалификационных документов

1. Заявка для участия в отборе на имя председателя закупочной комиссии (Форма №1).
2. Общая информация об участнике отбора (Форма №2)
3. Гарантийное письмо, свидетельствующее, о том, что между заказчиком и участником не совершается антиконкурентные действий (Форма№ 3)
4. Гарантийное письмо, свидетельствующее, о том, что участник не находится в стадии реорганизации, ликвидации или банкротства, в состоянии судебного или арбитражного разбирательства с заказчиком, а также об отсутствии ненадлежащее исполненных обязательств по ранее заключенным договорам. (Форма 4)

Форма №1

НА ФИРМЕННОМ БЛАНКЕ УЧАСТНИКА

№:_____ Дата:
_____

Закупочной комиссии
СП ООО «Самаркандский автомобильный завод»
140160, г. Самарканд, ул. С.Бухорий, 5

ЗАЯВКА

Изучив закупочную документацию на закупку оказание работ *(указать наименование предлагаемой работы)*, по лоту № лота____, выставленного на https://etender.uzex.uz/ получение которых настоящим удостоверяем ответы на запросы №№ *(указать номера запросов в случае наличия письменных обращений и ответов к ним)*, получение которых настоящим удостоверяем, мы, нижеподписавшиеся *(наименование претендента отбора)*, намерены участвовать в отборе на поставку в соответствии с закупочной документацией.

В этой связи направляем следующие документы:

1. Пакет квалификационных документов на ____ листах (указать количество листов, в случае предоставления брошюр, буклетов, проспектов, компакт-дисков и т.д. указать количество);

2. Техническая часть отборного предложения;

3. Иные документы *(в случае представления других документов необходимо указать наименование и количество листов).*

Ф.И.О. ответственного лица за подготовку отборного предложения:

Контактный телефон/факс: _____

Адрес электронной почты: _____

Ф.И.О. и подпись руководителя или уполномоченного лица

Место печати

Форма №2

Общая информация об участнике отбора

1	Полное наименование юридического лица, с указанием организационно-правовой формы	
2	Сведение о регистрации (дата регистрации, регистрационный номер, наименование регистрирующего органа)	
3	Юридический адрес	
4	Контактный телефон, факс, e-mail	
5	Полные банковские реквизиты	
6	Основные направления деятельности	

Информация об опыте поставки требуемого товара/услуг/работ

№	Наименование товара	Наименование, адрес и контактная информация	Примечание

_____ *(подпись уполномоченного лица)*

_____ *(Ф.И.О. и должность уполномоченного лица)*

М.П.

Дата: «___» _____2022г.

Руководитель_____ Гл. бухгалтер_____

М.П.

Форма №3

НА ФИРМЕННОМ БЛАНКЕ УЧАСТНИКА

№:_____
Дата: _____

Закупочная комиссия

ГАРАНТИЙНОЕ ПИСЬМО

Настоящим письмом подтверждаем, что компания _____ :
(наименование компании)

- прямо или косвенно **не предлагает, не дает или не соглашается** дать любому нынешнему либо бывшему должностному лицу или работнику государственного заказчика или другого государственного органа вознаграждение в любой форме, безвозмездного оказания в их адрес услуг или выполнения работ, предложение о найме на работу с целью повлиять на совершение какого-либо действия, принятие решения или применение какой-либо закупочной процедуры государственного заказчика в процессе государственных закупок;

- участник **не совершает** антиконкурентные действия, не имеет конфликта интересов и аффилированности с членами закупочной комиссии заказчика и самим заказчиком.

Подписи:

Ф.И.О. руководителя _____

Место печати

Форма №4

НА ФИРМЕННОМ БЛАНКЕ УЧАСТНИКА

№:_____
Дата: _____

Закупочная комиссия

ГАРАНТИЙНОЕ ПИСЬМО

Настоящим письмом подтверждаем, что компания _____ :
(наименование компании)

- не имеет ненадлежащим образом исполненные обязательства по ранее заключенным договорам с Заказчиком;
- не находится в стадии реорганизации, ликвидации или банкротства;
- не находится в состоянии судебного или арбитражного разбирательства с *(наименование заказчика)*;
- а также банк компании не зарегистрирован в офшорных зонах;
- отсутствует в Едином реестре недобросовестных исполнителей.

Подписи:

Ф.И.О. руководителя _____

Место печати

Приложение №2

Порядок и критерии квалификационной оценки участников и предложений участников отбора.

Порядок и критерии квалификационного отбора участников.

Квалификационная оценка осуществляется закупочной комиссией. Если требуемая информация не представлена участником, закупочная комиссия вправе не допускать его к участию в отборе.

Критерии квалификационной оценки

№	Критерий	Оценка	Примечание
1	Исполнение обязательств по ранее заключенным договорам	Надлежащее / не надлежащее (проводится на основании гарантийного письма участника)	Если ненадлежащее, то участник дисквалифицируется
2	Состояние участника в стадии судебного или арбитражного разбирательства с Заказчиком	Да / нет (проводится на основании гарантийного письма участника и информации от заказчика)	Если да, то участник дисквалифицируется
3	Участник имеется в Едином реестре недобросовестных исполнителей	Имеется / Не имеется	Если имеется, то участник дисквалифицируется
4	Наличие задолженности по уплате налогов и других обязательных платежей (картотека №2)	Имеется / Не имеется (проводится на основании письма обслуживающего банка участника и информации от заказчика)	Если имеется, комиссия вправе дисквалифицировать участника
5	Наличие опыта и результаты выполнения подобных работ	Имеется / Не имеется	Если не имеется, комиссия вправе дисквалифицировать участника
6	Регистрация участника и банка участника в оффшорных зонах	Да / нет	Участник, а также участники, банки которых зарегистрированные в оффшорных зонах, к участию в отборе не допускаются
7	Состояние участника в стадии реорганизации, ликвидации или банкротства	Да / нет (проводится на основании гарантийного письма участника)	Если да, то участник дисквалифицируется

I. Этап: Техническая оценка предложений.

Осуществляется закупочной комиссией на основании документов технической части предложений. Предложения участников отбора, не прошедшие, по технической оценке, (набравшие 0 баллов по итогам выставления баллов) дисквалифицируются. При этом документы по ценовой части предложения возвращается участнику.

Критерии технической оценки

№	Критерий	Оценка	Примечание
1	Соответствие требованиям закупочной документации по отбору (ценовое и технические требования)	Соответствует – 1 балл Не соответствует – 0 баллов	Если не соответствует, то участник дисквалифицируется
2	Предложение имеет незначительное отклонение, при этом соответствует техническим требованиям заказчика на основании оценки экспертной группы	Допустить/Отклонить	Закупочная комиссия вправе отклонить или допустить участника отбора

II Этап: Ценовая оценка предложений.

Осуществляется закупочной комиссией после проведения технической оценки на основании документов по ценовой части.

Критерии ценовой оценки

№	Критерий	Оценка	Примечание
1	Наименьшая цена и соответствие по ценовой части закупочной документации по отбору	Наименьшая цена-наивысший балл Наивысшая цена-наименьший балл	Шкала баллов формируется в зависимости от количества предложений участников (шкала баллов соответствует количеству предложений, соответствующих требованиям технической части закупочной документации по отбору). Для корректного сравнения цен иностранных и отечественных Участников отбора, при анализе и оценке предложений могут быть учтены соответствующие расходы (налоги, таможенные платежи и иные обязательные платежи, и расходы), в случаях, предусмотренных законодательством Республики Узбекистан. В случае равных ценовых и технических параметрах отборных предложений по итогам оценки, закупочной комиссией во внимание принимаются дополнительные возможности участников отбора по предоставлению скидок (снижению стоимости предложения), путем проведения переговоров.

Техническая часть

№	Наименование, описание продукции/ услуги	Технические требования	Единица измерения	Кол-во (объем)
1	Наименование услуги	Покупка Антивирусного программного обеспечения на 450 пользователей на 2 года.	Шт.	1
2	Цель приобретения услуги	Служебная необходимость		
3	Требования к поставщику (исполнителю)	Наличие партнерского сертификата, подтверждающего факт того, что компания является официальном представителем продаваемой антивирусной программы.		
4	Требования к услуге	**Общие требования** Антивирусная защита (АЗ) должна представлять собой масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети рабочих станций и серверов. В рамках всей организации должны использоваться единые антивирусные средства. Отдельно стоящие персональные компьютеры, то есть не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от всех типов вредоносных программ (антивирус). Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке. Для организаций имеющих офисы за границей должна иметься возможность выбора языка интерфейса консоли управления для подключения к серверу администрирования, без переустановки консоли и сервера для ИТ персонала родной язык которого отличается от русского. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке. Технические параметры программных средств антивирусной защиты должны соответствовать или превосходить следующие указанные параметры: Антивирусные средства и средства централизованного управления должны включать: • лицензионные файлы ключей для пакетов антивирусного программного обеспечения (АПО); при использовании схемы с несколькими серверами удаленного администрирования кластерная технология для		

		организации связи между серверами не требуется дополнительных лицензий на связь между серверами. • программные средства антивирусной защиты рабочих станций, серверов и мобильных устройств (смартфонов, планшетов) • агент администрирования для выполнения связи между сервером администрирования и защищаемыми узлами • программные средства централизованного управления, мониторинга и обновления на ОС Windows, Linux/BSD, Mac OS, мобильные ОС Android; • программные средства централизованного управления должны иметь WEB консоль для управления и формирования отчетов; • централизованное управление может осуществляться с любого устройства через Web - браузер; • программные средства централизованного управления могут устанавливаться на Windows и Linux платформы • обновляемые антивирусные базы данных и компоненты ядра антивирусной системы; • Прокси- сервер - компонент для обеспечения высокой масштабируемости решения и уменьшения нагрузки на центральный сервер администрирования • наличие инструмента для обнаружения неизвестных компьютеров, осуществляющего автоматический поиск ПК в локальной сети, без необходимости осуществлять их ручной поиск и добавление; • наличие различных вариантов установки агентов администрирования клиентской части антивирусного программного обеспечения такие как: удаленно или локально : - Push установка, - Установка через e-mail, - Установка с применением съемного носителя , например USB, - Локальная установка; • эксплуатационную документацию на русском языке. • Наличие выделенного программного инструмента для управления лицензиями. С его помощью можно отслеживать лицензии, активированные модули и связанные с лицензиями события, такие как окончание срока действия, использование и авторизация. • Наличие выделенной утилиты для создания локального хранилища вирусных сигнатур, без использования сервера централизованного управления. • Наличие возможности организации двухфакторной аутентификации пользователей консоли сервера централизованного управления. • сервис дополнительного уровня безопасности продуктов включающий встроенную песочницу **Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows**		

		Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС: • Microsoft Windows Vista; • Microsoft Windows Vista x64; • Microsoft Windows 7 • Microsoft Windows 7 x64. • Microsoft Windows 8 • Microsoft Windows 8.1 • Microsoft Windows 10 Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей: • интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением; • резидентный антивирусный мониторинг; • возможность полностью скрыть интерфейс антивирусного ПО • антивирусное сканирование по команде пользователя или администратора; • антивирусное сканирование по расписанию; • антивирусное сканирование при определенных условиях: - после обновлений антивирусных баз данных; - каждый раз при запуске компьютера; - каждые сутки при первом запуске компьютера; - при успешном Интернет или VPN соединении; - вход пользователя; - при обнаружении подозрительной активности, в том числе и активным модулем «защита в режиме реального времени». - состояние простоя, автоматически сканирует локальные диски, если компьютер находится в состоянии простоя, в одном из следующих трех режимов: заставка, блокировка компьютера, выход пользователя • наличие задачи на выключение ПК по завершению сканирования • антивирусное сканирование трафика по следующим протоколам: FTP, HTTP и HTTPs, POP3 и POP3s, а так же IMAP и IMAPs трафика. • наличие дополнительного модуля по защите документов Microsoft Office и сканировании проходящих через Internet Explorer файлов • защита от еще неизвестных вредоносных программ на основе эвристического анализа; • возможность добавлять в исключения только определенные угрозы, в независимости от их местонахождения на ПК: • обнаружение скрытых процессов;		

		• возможность устанавливать только необходимые компоненты антивирусной защиты (модульная установка); • возможность отключения антивирусной защиты при необходимости; • антивирусная проверка и лечение файлов, упакованных программами типа *PKLITE, LZEXE, DIET, EXEPACK* и пр.; • антивирусная проверка и лечение файлов в архивах форматов *ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE*; • содержать настраиваемую систему предотвращения вторжений Host Intrusion Prevention System (HIPS) для предотвращения попыток внешнего воздействия, изменения, а так же для мониторинга процессов, файлов и ключей реестра; • возможность работы HIPS по ряду заранее подготовленных режимов фильтрации; • обеспечивать защиту от хакерских атак, путем использования межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/HIPS) при работе в вычислительных сетях любого типа, включая беспроводные; • персональный файервол; • возможность настройки нескольких профилей файервола, с автоматическим переключением данных профилей, при выполнении определенных условий; • управление всем сетевым трафиком компьютера в обоих направлениях; • низкоуровневое сканирование трафика; • поддержка протокола IPv6; • поддержка встроенной песочницы для защиты от угроз нулевого дня; • модуль сканирования UEFI; • выделенный модуль защиты от вирусов шифраторов; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность управления доступом к веб-ресурсам, путем создания списка заблокированных либо разрешенных веб-сайтов, а также путем запрета всех веб-сайтов, кроме тех, которые внесены в список разрешенных; • активный режим фильтрации для приложений, а так же возможность отключения фильтрации или перевод в пассивный режим для исключенных приложений; • настраиваемый веб-контроль по категориям сайтов, позволяющий задавать правила применения политики использования сети Интернет на уровне пользователей или групп пользователей; • Наличие в модуле веб-контроля возможности кастомизации страницы предупреждения или блокирования • фильтрации для доверенных приложений; • сканирование из контекстного меню; • отключение фильтрации для доверенных веб-адресов;		

		• отключение фильтрации для доверенных IP адресов; • возможность исключить из проверки доверенные процессы, хэш суммы, файлы и папки. • настройка нескольких профилей обновлений (например, для мобильных пользователей) с возможностью обновления из сети Интернет; • Наличие агента администрирования антивирусного программного обеспечения (АПО) для рабочих станций • наличие планировщика в клиенте антивирусного ПО; • возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы; • ядро и все основные модули продукта не требуют перезагрузки и активны сразу после установки; • наличие специализированной утилиты для сбора файлов журналов о конфигурации системы, установке и функционировании антивирусного пакета для ускорения решения проблем при возможных проблемах с антивирусным пакетом • наличие модуля сканирования в состоянии простоя, автоматически сканирует локальные диски, если компьютер находится в состоянии простоя, в одном из следующих трех режимов: заставка, блокировка компьютера, выход пользователя • возможность подключения уже установленных лицензий антивирусной защиты рабочих станций к серверу централизованного управления без необходимости удаления существующего пакета антивирусной защиты, путем установки агента администрирования ; • запуск обновления антивирусных баз данных после установки модемного соединения или VPN; • возможность создания задачи запуска приложения стороннего производителя в планировщике антивируса при определенных условиях или по временному интервалу; • защита на лету от вредоносных сценариев, загружаемых с Web-страниц • блокирование нежелательных и рекламных сообщений • самообучаемый антиспам; • защита почтовых клиентов: Microsoft Outlook, Outlook Express,Windows Mail, Windows Live Mail; • черные и белые списки антиспама, списки исключений • ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • наличие функциональности использования общего локального кэша для повышения скорости сканирования в виртуализированных средах;		

		• защита от фишинга: защищает от попыток получить пароли и другую конфиденциальную информацию, запрещая доступ к вредоносным веб-сайтам, которые принимают вид нормальных веб-сайтов; • Защита от эксплойтов: блокировщик эксплойтов контролирует поведение процессов и выявляет подозрительную активность, которая является типичной для целевых атак и ранее неизвестных эксплойтов – угроз нулевого дня • наличие модуля сканирования памяти, который отслеживает поведение процессов и сканирует зловредные процессы, когда они снимают маскировку в памяти; • защита от ботнетов: помогает обнаруживать вредоносные программы, анализируя их схемы обмена данными и протоколы • регулировка распределения ресурсов рабочей станции между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме; • настройка лимитов сканирования по параметрам – глубина вложенности (архивов), размера объекта и времени сканирования объекта; • наличие модуля, позволяющего проводить автоматическое сканирование содержания подключаемых внешних устройств хранения данных, а так же применять расширенный анализ для запуска файлов с таких устройств; • наличие модуля, позволяющего настроить ограничения доступа (нет доступа, только чтение, полный доступ, предупреждение) для каждого пользователя или для группы пользователей как по типу устройства (CD/DVD/Blu-Ray, USB хранилища данных, USB принтеры, устройства обработки изображений, Устройства FireWire, кард ридеров, модемов, LPT\COM порты, Bluetooth устройства) так и по заданным атрибутам (производитель, модель, серийный номер) задавать одно правило на несколько устройств ; • интеграция с MS NAP и CISCO NAC; • возможность формирования аварийных дампов памяти, на случай сбоя приложения • возможность отката обновлений вирусных баз на предыдущие версии и приостановка их обновления с последующим автоматическим включением обновления через указанный промежуток времени; • наличие функциональности возобновлять прерванные загрузки баз данных сигнатур вирусов и модули продуктов при обновлении; • интеграция с центром безопасности Windows; • интеграция с центром обновления Windows , для установки патчей закрывающих обнаруженные уязвимости, с выбором необходимых обновлений от «необязательных» обновлений до «критических»; • настройка проверки исполняемых файлов и загрузочных областей компьютера в качестве отдельной задачи; • технологии самозащиты приложения, защиты от удаленного несанкционированного управления		

		сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; • проверка наличия актуальных обновлений системы; • наличие настраиваемой функции автоматического скрытия уведомлений при работе антивируса для приложений, работающих в полноэкранном режиме, т.е. при работе приложения в полноэкранном режиме на экран не выводятся информационные уведомления о работе антивирусного программного обеспечения; • наличие множества путей уведомления администраторов о важных событиях, происходящих на рабочих станциях (почтовое сообщение, всплывающее окно, запись в журнал событий); • обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на отчуждаемых носителях информации; • экспорт логов и отчетов в форматы XML,TXT, DAT, DMP; • наличие облачной технологии детектирования неизвестных угроз, контроль приложений на основе репутационного сервиса; • наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную; • возможность создания дисков аварийного восстановления; • экономия электроэнергии в режиме автономного питания; • системные требования не должны превышать: 300мб RAM, HDD 1гб, Processor Intel или AMD, одноядерный, x86 или x64 1ГГц. • размер дистрибутива антивирусного пакета не должен превышать – 165 Мб. **Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows** Программные средства антивирусной защиты систем серверов под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС: • Microsoft Windows Server 2008 (x86 и x64) • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows Server 2008 x64 R2 SP1 / x64 R2 CORE • Microsoft Windows Server 2008 x86 SP2 / x64 SP2 CORE • Microsoft Windows Server 2012 x64 / x64 CORE • Microsoft Windows Server 2012 x64 R2 / x64 R2 CORE • Microsoft Windows Hyper-V Server 2008 R2 • Microsoft Windows Hyper-V Server 2012 • Microsoft Windows Hyper-V Server 2012 R2 Серверы Storage, Small Business и MultiPoint: • Microsoft Windows Storage Server 2008 R2 Essentials с пакетом обновления 1		

		• Microsoft Windows Storage Server 2012 • Microsoft Windows Storage Server 2012 R2 • Microsoft Windows Small Business Server 2008 (x64) • Microsoft Windows Small Business Server 2011 (x64) • Microsoft Windows Server 2012 Essentials • Microsoft Windows Server 2012 R2 Essentials • Microsoft Windows MultiPoint Server 2010 • Microsoft Windows MultiPoint Server 2011 • Microsoft Windows MultiPoint Server 2012 Программные средства антивирусной защиты файловых серверов под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей: • интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением; • резидентный антивирусный мониторинг; • антивирусное сканирование по команде пользователя или администратора; • антивирусное сканирование по расписанию; • антивирусное сканирование при определенных условиях: - после обновлений антивирусных баз данных; - каждый раз при запуске компьютера; - каждые сутки при первом запуске компьютера; - при успешном Интернет или VPN соединении; - вход пользователя; - при обнаружении подозрительной активности, в том числе и активным модулем «защита в режиме реального времени». • антивирусное сканирование трафика по следующим протоколам: FTP, HTTP и HTTPs, а так же POP3 и POP3s трафика • антивирусное сканирование Hyper-V на наличие вирусов на безагентной основе • защита от еще неизвестных вредоносных программ на основе эвристического анализа; • содержать настраиваемую систему предотвращения вторжений Host Intrusion Prevention System (HIPS) для предотвращения попыток внешнего воздействия, изменения, а так же для мониторинга процессов, файлов и ключей реестра; • возможность работы HIPS по ряду заранее подготовленных режимов фильтрации • возможность добавлять в исключения только определенные угрозы, в независимости от их местонахождения на ПК: • возможность исключить определенные процессы приложений, хэш суммы из сканирования на наличие вирусов; • обнаружение руткитов (скрытых файлов/системных аномалий); • антивирусная проверка и лечение файлов, упакованных программами типа *PKLITE, LZEXE, DIET, EXEPACK* и пр.;		

		• антивирусная проверка и лечение файлов в архивах форматов *ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE*; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность создания задачи запуска приложения стороннего производителя в планировщике антивируса; • защита на лету от вредоносных сценариев, загружаемых с Web-страниц; • возможность настройки параметров антивирусного пакета из интерфейса командной строки • функция автоматического обнаружение и исключения файлов на сервере, имеющих критическое значение для бесперебойной работы; • возможность задать количество модулей сканирования для увеличения скорости сканирования; • возможность управления доступом к веб-ресурсам, путем создания списка заблокированных либо разрешенных веб-сайтов, а также путем запрета всех веб-сайтов, кроме тех, которые внесены в список разрешенных; • активный режим фильтрации для приложений, а так же возможность отключения фильтрации или перевод в пассивный режим для исключенных приложений; • сканирование из контекстного меню; • отключение фильтрации для доверенных веб-адресов; • многопоточное сканирование; • настройка нескольких профилей обновлений (например для мобильных пользователей) с возможностью обновления из интернета. • наличие планировщика в антивирусном пакете . • наличие агента администрирования антивирусного программного обеспечения (АПО) для файловых серверов • возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы; • ядро и все основные модули продукта не требуют перезагрузки и активны сразу после установки; • возможность подключения уже установленных лицензий антивирусной защиты рабочих станций к серверу централизованного управления без необходимости удаления существующего пакета антивирусной защиты, путем установки агента администрирования ; • наличие облачной технологии детектирования неизвестных угроз, контроль приложений на основе репутационного сервиса;		

		• запуск обновления антивирусных баз после установки модемного соединения или VPN; • ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • наличие специализированной утилиты для сбора файлов журналов о конфигурации системы, установке и функционировании антивирусного пакета для ускорения решения проблем при возможных проблемах с антивирусным пакетом • наличие функциональности использования общего локального кэша для повышения скорости сканирования в виртуализированных средах; • защита от фишинга: защищает от попыток получить пароли и другую конфиденциальную информацию, запрещая доступ к вредоносным веб-сайтам, которые принимают вид нормальных веб-сайтов; • Защита от эксплойтов: блокировщик эксплойтов контролирует поведение процессов и выявляет подозрительную активность, которая является типичной для целевых атак и ранее неизвестных эксплойтов – угроз нулевого дня • поддержка встроенной песочницы для защиты от угроз нулевого дня; • модуль сканирования UEFI; • выделенный модуль защиты от вирусов шифраторов; • модуль защиты от сетевых атак; • модуль защиты от ботнетов; • наличие модуля сканирования памяти, который отслеживает поведение процессов и сканирует зловредные процессы, когда они снимают маскировку в памяти; • регулировка распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме; • настройка лимитов сканирования по параметрам – глубина вложенности (архивов), размера объекта и времени сканирования объекта; • блокировка сменных носителей информации и устройств (USB); • наличие модуля, позволяющего настроить ограничения доступа (нет доступа/только чтение/полный доступ/предупреждение) для каждого пользователя или для группы пользователей как по типу устройства (CD/DVD/Blu-Ray, USB хранилища данных, USB принтеры, устройства обработки изображений, Устройства FireWire, кард ридеров, модемов, LPT\COM порты, Bluetooth устройства) так и по заданным атрибутам (производитель/модель/серийный номер) задавать одно правило на несколько устройств ; • интеграция с центром безопасности Windows; • интеграция с центром обновления Windows, для установки патчей закрывающих обнаруженные уязвимости, с выбором необходимых обновлений от «необязательных» обновлений до «критических»; • поддержка Windows Management Instrumentation		

		• настройка проверки исполняемых файлов и загрузочных областей компьютера в качестве отдельной задачи; • поддержка кластерных систем с возможностью автоматического объединения антивирусного ПО (автоматическая синхронизация конфигурации ПО на кластерах) • технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; • проверка наличия актуальных обновлений операционной системы; • полноценная работа без графического интерфейса, администрирование и конфигурирование АПО через командную строку; • возможность автоматизации работы за счет выполнения сценариев, позволяющих конфигурировать АПО и выполнять какие-либо действия; • автоматическое скрытие уведомлений при работе антивируса в полноэкранном режиме; • наличие настраиваемой функции автоматического скрытия уведомлений при работе антивируса для приложений, работающих в полноэкранном режиме; • наличие множества путей уведомления администраторов о важных событиях, происходящих на серверах (почтовое сообщение, всплывающее окно, запись в журнал событий); • обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на отчуждаемых носителях информации; • наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную; • возможность создания дисков аварийного восстановления; • размер дистрибутива антивирусного пакета не должен превышать – 127 Мб. **Требования к средствам антивирусной защиты мобильных устройств** Программные средства для антивирусной защиты смартфонов и планшетов должны функционировать под управлением мобильных ОС: Android 5 (Lollipop) и выше Программные средства антивирусной защиты смартфонов должны обеспечивать следующую функциональность: • возможность проведения аудита безопасности устройства с генерацией отчета; • постоянная защиту файловой системы смартфона, планшета;		

		• проверка всех приложений, файлов, папок и карты памяти в режиме реального времени; • проверка объектов файловой системы, находящихся на смартфоне или на подключенных картах расширения памяти, по требованию пользователя и по расписанию; • надежное изолирование зараженных объектов в карантинном хранилище; • обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов; • блокирование нежелательных SMS и MMS сообщений; • контроль приложений для отслеживания установленных приложений, блокировать доступ к определенным приложениям и снижать степень риска, предлагая пользователям удалять некоторые программы • задание минимальных уровней безопасности и сложность кодов разблокировки экрана; • указание максимального количества неудачных попыток разблокировки; • указание максимального срока действия для кода разблокировки экрана; • настройка таймера блокировки экрана; • ограничить использование камеры. • защита от фишинга: защита пользователей от попыток получить пароли, банковские данные и прочую конфиденциальную информацию незаконными веб-сайтами, выдающими себя за законные • центр уведомлений: предоставляет сведения о разных событиях, о причинах их несоответствия корпоративным политикам и о том как эту несовместимость устранить • защита от кражи и утери смартфона. Обеспечить возможность удаленной блокировки мобильного устройства; • возможность дистанционно удалить информацию со смартфона; • возможность определить доверенную SIM-карту; • автоматическая скрытая отправка уведомления посредством SMS-сообщения, с предупреждением об использовании не доверенной SIM-карте. Так же сообщение должно включать информацию, необходимую для идентификации злоумышленника: телефонный номер текущей SIM-карты, номер IMSI и номер IMEI телефона. • расширенный сброс до заводских установок: все доступные на устройстве данные будут удалены (заголовки файлов будут уничтожены). Кроме того, на телефоне будут восстановлены заводские настройки по умолчанию • возможность включить сирену:Потерянное устройство блокируется и начинает издавать очень громкий звук, даже если звук на устройстве отключен • Наличие встроенного агента администрирования антивирусного программного обеспечения (АПО) • Системные требования: Операционная система: Android 5 (Lollipop) и более поздние версии. Разрешение сенсорного экрана: 480 x 800 пкс. Процессор: ARM с набором инструкций ARMv7 или x86 Intel Atom. Свободное место для хранения данных:20МБ.		

		Требования к системе управления антивирусной защитой Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей: • масштабируемое решение: масштабирование производится за счет использования прокси серверов • интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением; • Прокси- сервер - компонент для обеспечения высокой масштабируемости решения и уменьшения нагрузки на центральный сервер администрирования • наличие инструмента для обнаружения неизвестных компьютеров, осуществляющий автоматический поиск ПК в локальной сети, без необходимости осуществлять их ручной поиск и добавление; • централизованная установка/обновление/удаление программных средств антивирусной защиты, настройки, администрирования; • централизованный сбор информации и создание отчетов о состоянии антивирусной защиты; • защищенное соединение между сервером и клиентом; • программные средства централизованного управления должны иметь WEB консоль для управления и формирования отчетов; • централизованное управление может осуществляться с любого устройства через Web - браузер; • создание отчетов в наглядном графическом виде; • экспорт логов и отчетов в форматы HTML,TXT, CSV, PDF; • наличие модуля поддержки SIEM; • предварительная настройка политик для групп или клиентов (профили обновлений, запрещенные сайты, расписание планировщика и т.д.); • возможность отправки сообщений, как на мобильные устройства, так и на персональные компьютеры; • возможность удаленного создания журнала аудита безопасности с мобильного устройства • возможность установки пользовательских приложений; • наличие различных вариантов установки агентов администрирования клиентской части антивирусного программного обеспечения такие как: удаленно или локально : - Push установка, - Установка через e-mail, - Установка с применением съемного носителя , например USB, - Локальная установка; • наличие возможности автоматически выбирать соответствующий установочный пакет агента для операционных систем или в ручном режиме. • настройка политик безопасности для клиентов; • возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и		

		драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы; • возможность удаленного запуска определенного сценария на конечных клиентах, предназначенного для удаления/изменения критических объектов системы. • отсутствие необходимости перезагрузки ПК после установки системы управления антивирусной защиты; • автоматизированное обновление программных средств антивирусной защиты и антивирусных баз; • возможность произвести быстрый откат обновлений сигнатурных баз для отдельных компьютеров или групп; • доставка обновлений на рабочие места пользователей сразу после их получения; • централизованный карантин; • возможность создания групп управляемых компьютеров как вручную, так и автоматически на основе структуры Active Directory; • возможность синхронизации с Active Directory как по расписанию, так и вручную; • автоматический поиск незащищенных рабочих станций с учетом топологии сети; • аудит изменений в настройках сервера по учетным записям; • построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; • обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на носителях информации; • механизм оповещения о событиях в работе установленных приложений антивирусной защиты и возможность настройки рассылки почтовых уведомлений о них; • наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную; • возможность создания динамических групп, в которые динамически будут включаться клиентские станции при соответствии условиям данных групп; • работа со статическими и динамическими группами • различные варианта уведомлений администратора сети (по e-mail,использование SNMP-ловушки); • возможность создания резервных копий содержимого базы данных и настроек сервера; • возможность подключения к консоли сервера удаленного администрирования с использованием доменных имени пользователя и пароля; • администрирование серверов и рабочих станций Windows, Linux\BSD, а так же решений для защиты мобильных ОС (Android); • наличие функции пробуждения по локальной сети Wake on LAN • возможность автоматического определения «клонированных машин» с помощью сложной логики обнаружения отпечатков оборудования. • наличие протокола для репликации, с использованием «PNS» (Push Notification Service) и поддержкой многоадресных вызовов для WOL. • функционал для инвентаризации оборудования. • наличие функции быстрого отключения или включения уведомлений на выбранных компьютерах для		

		прерывания или возобновления обмена данными с сервером администрирования • поддержка баз данных MS SQL, MySQL; • программные средства централизованного управления могут устанавливаться на Windows и Linux платформы • программные средства должны поддерживать установку на отказоустойчивые кластеры Windows и Linux платформ • сервер удаленного администрирования может быть установлен и должен поддерживать операционные системы Windows Server: ○ Windows Server 2003 x86 SP2 /x64 SP2 ○ Windows Server 2003 x86 R2 SP2 /x64 R2 SP2 ○ Windows Server 2008 x64 R2 SP1 / x64 R2 CORE ○ Windows Server 2008 x86 SP2 / x64 SP2 ○ Windows Server 2012 x64 / x64 CORE ○ Windows Server 2012 x64 R2 / x64 R2 CORE ○ Windows Server 2016 x64 ○ Windows Server 2019 x64 ○ Microsoft SBS 2003 x86 SP2 / x86 R2 ○ Microsoft SBS 2008 x64 SP2 ○ Microsoft SBS 2011 x64 Standard / x64 Essential Linux: ○ Ubuntu 12.04 LTS x86 Desktop / Server ○ Ubuntu 12.04 LTS x64 Desktop / Server ○ Ubuntu14.04. LTS x86 Desktop / Server ○ Ubuntu 14.04 LTS x64 Desktop / Server ○ RHEL Server 6 x86 / x64 ○ RHEL Server 7 x86 / x64 ○ CentOS 6 x86 / x64 ○ CentOS 7 x86 / x64 ○ SLED 11 x86 / x64 ○ SLES 11 x86 /x64 ○ OpenSUSE 13 x86 / x64 ○ Debian 7 x86 / x64 ○ Fedora 19 x86 / x64 • Программные средства централизованного управления, мониторинга и обновления должны функционировать на виртуальных платформах следующих версий: ○ VMware vSphere/ESXi (версии 5.0 и новее) ○ VMware Workstation (версии 9 и новее) ○ VMware Player (версии 7 и новее) ○ Microsoft Hyper-V (Server 2012 и 2012 R2) ○ Oracle VirtualBox (версии 4.3.24 и новее) Наличие выделенного программного инструмента для управления лицензиями. С его помощью можно отслеживать лицензии, активированные модули и связанные с лицензиями события, такие как окончание срока действия, использование и авторизация. Работа с инструментом под разными ролями как владелец лицензии или как администратор безопасности. Возможность выполнять следующие действия: • просматривать состояние лицензий в реальном времени; • отслеживать отдельные устройства (и при этом их отключать); • настраивать уведомления, связанные с событиями лицензии;		

		• хранить лицензии одновременно в старой и новой формах в смешанных средах; • обменивать ключи лицензий на сообщения электронной почты и пароли, с помощью которых также можно активировать программы; • назначать несколько лицензий на одну учетную запись; • разрешать другим лицам использовать лицензии (активировать их); • настраивать уведомления для более удобного отслеживания состояния лицензии; • наличие функции синхронизации с сервером централизованного управления. • наличие выделенной утилиты для мигрирования с более ранних версий антивирусного программного обеспечения с сохранением настроек политик и информационной базы журналов событий. • наличие выделенной утилиты для создания локального хранилища вирусных сигнатур, без использования сервера централизованного управления. • наличие возможности организации двухфакторной аутентификации пользователей консоли сервера централизованного управления. Поддержка двухфакторной аутентификации для 10 пользователей консоли сервера централизованного управления. При использовании данной функциональности должно быть использовано решение двухфакторной аутентификации того же производителя, что и сам пакет антивирусного программного обеспечения. • наличие возможности деактивации лицензий на узлах через создание заданий на сервере управления. **Сервис дополнительного уровня безопасности продуктов** для защиты рабочих станций, файловых и почтовых серверов с помощью встроенной песочницы на основе технологий машинного обучения для обнаружения новых, ранее неизвестных угроз. В сервисе должна быть реализована следующая функциональность: • Детектирование на основе анализа поведения • Машинное обучение • Обнаружение угроз нулевого дня • Встроенная песочница Сервис на основе технологий машинного обучения для обнаружения новых, ранее неизвестных угроз поставляется в составе решения по антивирусной защите рабочих станций, файловых серверов локальной сети заказчика. • Наличие поддержки антивирусными продуктами дополнительной функциональности, активируемой отдельной лицензией. Сервис предназначен для продуктов того же производителя антивирусного обеспечения, что и сам сервис. Сервис должен активироваться и управляться из центра обеспечения безопасности системы.		

		• Сервис должен поддерживать работу с антивирусными решениями по защите рабочих станций, файловых серверов и почтовых серверов. • Для работы с сервисом необходим только доступ в сеть интернет, никаких аппаратных средств в сети заказчика не требуется. Сервис должен обеспечивать: • Многоуровневую защиту - иметь не менее 3 моделей машинного обучения. Система выполняет работу с образцами в виртуальной среде или в песочнице. Система моделирует поведение пользователей, чтобы обмануть образцы вредоносных программ и использует модели нейронных сетей Deep Learning для сравнения поведения образцов с поведением всех известных образцов вредоносных программ. • Детальный обзор - Каждый изучаемый образец отображается в консоли центра безопасности, где наглядно и удобно представлена детальная информация о его характеристиках и происхождении. • Высокую скорость анализа – предоставлять анализ 90% неизвестных образцов в течение 5 минут • Мобильность – наличие возможности анализа файлов вне зависимости от местонахождения пользователей в корпоративной сети или за ее пределами. • Наличие возможности отправки подозрительных файлов вручную или автоматически на основе конфигурации политики. • Возможность отправки файлов вручную из веб-консоли Центра обеспечения безопасности или с клиентских компьютеров с активированным сервисом. • Возможность управлять действиями сервиса через API Центра обеспечения безопасности • Наличие возможности отправки больших файлов объемом до 64 Мб • Поддерживаемые типы файлов для отправки на проверку: • Документы (.docx, .xslx, .rtf и др.) • Исполняемые файлы (файлы .exe, .dll, .sys и др.) • JAR, LNK, REG, MSI, SWF и др • Сценарии (.bat, .cmd, .js, .vbs, .ps и др.) • Ole2 - при использовании с продуктами по защите почтовых серверов • .hta • Наличие функциональности предоставления отчета о поведении проверенного образца, в котором будет приведено краткое описание поведения наблюдаемого образца. В Отчете о файле должна содержаться следующая информация: • Имя компьютера, отправившего файл • указание Пользователя на исходном компьютере, отправившего файл. В некоторых случаях это может быть системный пользователь • Причина отправки (автоматически, вручную). • указана Часть облака, получившая файл • Хеш SHA1 отправленного файла. • Имя файла и его полный путь в файловой системе отправителей. • Размер файла. • Категория файла (тип файла). • Наличие в отчете параметров: **Состояние** и **Статус**: • **Состояние** означает текущее состояние файла в процессе выполнения анализа		

		• **Статус** означает результат анализа поведения или отсутствие результата • Наличие категории статуса, присвоенного проверенным образцам, которое отображается в консоли центра управления или в отчете по образцу: • **Не заражено** - Модули обнаружения не идентифицируют образец как вредоносный. • **Подозрительный** - Модуль обнаружения определил поведение файла как подозрительное, но не вредоносное. • **Вредоносный** - Поведение файла считается вредоносным. • Наличие функциональности распространения результатов о проверенных файлах во все продукты для обеспечения безопасности в компании пользователя в течение не более 2 минут • Наличие функциональности предоставления списка о всех переданных файлах в консоль Центра обеспечения безопасности. Можно просмотреть список отправленных файлов в выделенном разделе консоли. • Возможность настройки отправки образцов в консоли Центра обеспечения безопасности • Возможность настройки исключений для образцов и настройки политик для продуктов обеспечения безопасности в консоли Центра обеспечения безопасности. **Требования к обновлению антивирусных баз** Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей: • реализована возможность создания зеркала обновлений для экономии трафика; • зеркало обновлений можно создать на любом ПК сети не зависимо от используемой операционной системы Windows/Linux , в том числе и на конечной рабочей станции при помощи AV-клиента с обязательным наличием как минимум двух путей раздачи обновлений (HTTP и SMB), для активации зеркала не должна требоваться установка дополнительных модулей, как на сервер, так и на рабочую станцию; • типы обновлений: обновление БД сигнатур вирусов, программных компонентов, обновление ядра; • пакеты обновления зеркала можно загружать двумя способами: по протоколу HTTP (рекомендуется) и с помощью общего сетевого диска (SMB); • обновления можно распространять на электронных носителях информации (FDD\CD\DVD\ USB-drive); • осуществляется проверка целостности и подлинности обновлений средствами электронной цифровой подписи. **Требования к эксплуатационной документации** Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы на русском языке, в том числе: • руководство пользователя (администратора);		

		• руководство администратора средств удаленного администрирования. Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты. **Требования к технической поддержке** Техническая поддержка антивирусного программного обеспечения должна: • предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории следующих стран: Российская Федерация, Республика Казахстан, Республика Беларусь, Киргизская Республика, Республика Молдова, Республика Таджикистан, Республика Узбекистан, круглосуточно без праздников и выходных (24x7) по электронной почте и через Интернет, а также по телефону; • Web-сайт производителя АЗ должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке, пополняемую базу знаний и русскоязычный форум.		
5	Срок оказания услуги	**В течение 730 дней**		