**ИЗВЕЩЕНИЕ О ЗАПРОСЕ КОТИРОВОК в электронной форме НА ПРИОБРЕТЕНИЕ (ПРОДЛЕНИЕ) ЛИЦЕНЗИЙ, ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ КОМПЛЕКСА ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

**1. Наименование закупки:** приобретение (продление) лицензий, технической поддержки комплекса программных средств защиты информации согласно проекту договора (приложение № 2 к извещению).

**2. Способ закупки:** запрос котировок в электронной форме.

**3. Наименование заказчика:** Муниципальное унитарное предприятие Единый расчетно-кассовый центр городского округа город Уфа Республики Башкортостан (сокращенное наименование: МУП ЕРКЦ г. Уфы)

**Местонахождение заказчика:** Российская Федерация, Республика Башкортостан, г. Уфа.

**Почтовый адрес:** 450098, Республика Башкортостан, г. Уфа, ул. Комсомольская, д. 165/1.

**Адрес электронной почты: erkcweb@gmail.com**

**Контактные телефоны и фамилия должностного лица заказчика:**

тел. (347) 246 5000; генеральный директор: Винникова А.Н.

**Контактные телефоны** **и фамилия специалиста по закупкам заказчика:**

(347) 246 5000 (доб. 1142) Саламасова Олеся Геннадиевна.

**4. Предмет договора:** обновление, сопровождение и приобретение программного обеспечения

**5. Дата начала подачи заявок:** «10» декабря 2021 г. с 09.00 (время уфимское).

**6. Дата окончания подачи заявок:** «17» декабря 2021 г., 09:00 (время уфимское).

**7. Место подачи заявок:** электронная торговая площадка - https://bashzakaz.ru/ ООО «Башзаказ» (далее по тексту – ЭТП).

**8.** **Порядок предоставления документации о закупке:** в электронной форме, в соответствии с регламентом ЭТП.

**9. Место поставки товара:** г. Уфа, ул. Комсомольская, д. 165/4

**10. Сведения о начальной (максимальной) цене договора:** 1 759 096 (один миллион семьсот пятьдесят девять тысяч девяносто шесть) рублей 67 копеек.

В цену договора должны включаться все расходы, связанные с выполнением договора, в том числе все налоги, сборы и иные платежи, предусмотренные законодательством РФ.

**11. Сроки поставки товара:** в течение срока действия договора, согласно проекту договора (приложение № 2 к извещению). **Срок действия договора 12 месяцев с даты подписания договора, либо до полного исполнения обязательств.**

**12. Обеспечение заявки:** без обеспечения.

**13. Обеспечение исполнения договора:** без обеспечения.

**14. Дата вскрытия (открытия доступа к заявкам, поданным в электронной форме) и рассмотрения заявок:** «17» декабря 2021 г. 09:05 (местное время).

**15. Место и дата подведения итогов запроса котировок:** Республика Башкортостан, г. Уфа, ул. Комсомольская, д. 165/1, «17» декабря 2021 года 17:30 (местное время.)

**16. Дата заключения договора по результатам рассмотрения заявок:** не ранее чем через 10 дней и не позднее чем через 20 дней с даты размещения в ЕИС итогового протокола, составленного по результатам закупки.

**17. Преференции для контрагентов:** не установлены.

**18. Условия оплаты товара, работ, услуг:** в соответствии с Проектом договора**.**

**19. Качество поставляемого товара:** в соответствии с Проектом договора.

**20. Объем, срок предоставления гарантий качества поставляемого товара:** в соответствии с Проектом договора.

**21.** **Форма заявки:** заявка оформляется по форме, являющейся приложением к настоящему извещению (приложение № 1). Участник закупки вправе составить заявку в произвольной форме (по собственной форме) с тем условием, что собственная форма будет по содержанию соответствовать форме, предлагаемой Заказчиком.

**22.** Извещение о проведении закупки размещается в ЕИС и доступно для ознакомления без взимания платы.

**23. Прочие условия:** в случае изменения налогового законодательства цена договора, предложенная победителем закупки, может измениться на разницу, возникшую вследствие изменений, внесенных в налоговое законодательство РФ.

**24.** **Порядок подачи заявок на участие в запросе котировок**

24.1. Заявка на участие в запросе котировок должна включать:

1) документ, содержащий сведения об участнике закупок, подавшем заявку: ИНН/КПП/ОГРН, фирменное наименование (полное наименование), организационно-правовую форму, место нахождения, почтовый адрес (для юридического лица), фамилию, имя, отчество, ИНН/ОГРНИП (при наличии), паспортные данные, место жительства (для физического лица), номер контактного телефона;

2) копии учредительных документов участника закупок (для юридических лиц);

3) копии документов, удостоверяющих личность (для физических лиц);

4) выписку из Единого государственного реестра юридических лиц (для юридических лиц) либо Единого государственного реестра индивидуальных предпринимателей (для индивидуальных предпринимателей), полученную не ранее чем за месяц до дня размещения в ЕИС извещения о проведении закупки, или нотариально заверенную копию такой выписки;

5) надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица или индивидуального предпринимателя согласно законодательству соответствующего государства (для иностранных лиц). Эти документы должны быть получены не ранее чем за шесть месяцев до дня размещения в ЕИС извещения о проведении закупки;

6) документ, подтверждающий полномочия лица осуществлять действия от имени участника закупок - юридического лица (копия решения о назначении или об избрании физического лица на должность, в соответствии с которым это физическое лицо обладает правом действовать от имени участника без доверенности). Если от имени участника закупки действует иное лицо, заявка должна включать и доверенность на осуществление действий от имени участника закупок, заверенную печатью участника закупок (при наличии) и подписанную от его имени лицом (лицами), которому в соответствии с законодательством РФ, учредительными документами предоставлено право подписи доверенностей (для юридических лиц), либо нотариально заверенную копию такой доверенности;

7) решение об одобрении или о совершении крупной сделки (его копию), если требование о необходимости такого решения для совершения крупной сделки установлено законодательством РФ, учредительными документами юридического лица и если для участника закупок поставка товаров, выполнение работ, оказание услуг, выступающих предметом договора, предоставление обеспечения исполнения договора являются крупной сделкой. Если указанные действия не считаются для участника закупки крупной сделкой, представляется соответствующее письмо;

8) документ, декларирующий следующее:

- участник закупки не находится в процессе ликвидации (для участника - юридического лица), не признан по решению арбитражного суда несостоятельным (банкротом) (для участника - как юридического, так и физического лица);

- на день подачи конверта с заявкой деятельность участника закупки не приостановлена в порядке, предусмотренном Кодексом РФ об административных правонарушениях;

- у участника закупки отсутствуют недоимка по налогам, сборам, задолженность по иным обязательным платежам в бюджеты бюджетной системы РФ за прошедший календарный год, размер которых превышает 25 процентов от балансовой стоимости активов участника закупки по данным бухгалтерской отчетности за последний отчетный период;

- сведения об участнике закупки отсутствуют в реестрах недобросовестных поставщиков, ведение которых предусмотрено [Законом](consultantplus://offline/ref=972737D48DCE0AD9623B2ED97560D65D8CC8DA94A5782B4507979E533Fp3S5F) N 223-ФЗ и [Законом](consultantplus://offline/ref=972737D48DCE0AD9623B2ED97560D65D8CC8DA94A27A2B4507979E533Fp3S5F) N 44-ФЗ;

- участник закупки обладает исключительными правами на интеллектуальную собственность либо правами на использование интеллектуальной собственности в объеме, достаточном для исполнения договора (если в связи с исполнением договора Заказчик приобретает права на интеллектуальную собственность либо исполнение договора предполагает ее использование);

9) предложение о цене договора;

10) документы (их копии), подтверждающие соответствие участника запроса котировок требованиям законодательства РФ и извещения о проведении запроса котировок к лицам, которые осуществляют поставки товаров, выполнение работ, оказание услуг;

11) документы (их копии), подтверждающие соответствие товаров, работ, услуг требованиям законодательства РФ к таким товарам, работам, услугам, если законодательством РФ установлены требования к ним и если представление указанных документов предусмотрено извещением о проведении запроса котировок. Исключение составляют документы, которые согласно гражданскому законодательству могут быть представлены только вместе с товаром;

12) обязательство участника запроса котировок представить до момента заключения договора сведения о цепочке собственников, включая бенефициаров (в том числе конечных), и документы, подтверждающие эти сведения, если требование о предоставлении таких сведений было установлено в извещении о проведении запроса котировок;

13) согласие на поставку товаров, выполнение работ, оказание услуг в соответствии с условиями, установленными извещением о проведении запроса котировок;

14) иные документы в соответствии с требованиями настоящего извещения о проведении запроса котировок.

24.2. Заявка на участие в запросе котировок должна включать опись входящих в ее состав документов. Все листы заявки на участие должны быть прошиты и пронумерованы. Она должна быть скреплена печатью участника запроса котировок (при наличии) и подписана участником или лицом, им уполномоченным. Соблюдением указанных требований участник запроса котировок подтверждает, что все документы и сведения, входящие в состав заявки, поданы от его имени и являются достоверными. Не допускается устанавливать иные требования к оформлению заявки на участие в запросе котировок, помимо предусмотренных настоящим пунктом извещения.

Ненадлежащее исполнение участником запроса котировок требования, согласно которому все листы заявки должны быть пронумерованы, не является основанием для отказа в допуске к участию.

**Подача заявки в электронной форме осуществляется участником закупки в соответствии с правилами, установленными ЭТП.**

24.3. Участник запроса котировок имеет право подать только одну заявку на участие в запросе котировок. Он вправе изменить или отозвать поданную заявку в любой момент до истечения срока подачи заявок.

24.4. Участник запроса котировок может подать конверт с заявкой на участие лично либо направить его посредством почтовой связи. Секретарь комиссии по закупкам обязан обеспечить целостность конвертов с заявками и конфиденциальность содержащихся в них сведений до вскрытия конвертов с заявками.

24.5. Каждый конверт с заявкой на участие в запросе котировок, поступивший в течение срока подачи заявок на участие и после его окончания, регистрируется секретарем комиссии по закупкам в журнале регистрации заявок.

По требованию Участника секретарь комиссии выдает расписку в получении конверта с заявкой с указанием даты и времени ее получения, регистрационного номера заявки.

24.6. Прием заявок на участие в запросе котировок прекращается непосредственно перед вскрытием конвертов с такими заявками.

24.7. Заявки на участие в запросе котировок, полученные после окончания срока их подачи, вскрываются, но не возвращаются участникам закупки.

24.8. Заказчик обеспечивает конфиденциальность относительно всех полученных от Участников сведений, в том числе содержащихся в заявках. Предоставление этой информации другим Участникам или третьим лицам возможно только в случаях, прямо предусмотренных действующим законодательством Российской Федерации или Положением о закупках Заказчика.

24.9. Заказчик вправе отклонить заявки Участников, в случае выявления факта заключения между Участниками какого-либо соглашения с целью повлиять на определение Победителя закупочной процедуры.

24.10. Заказчик отклоняет все заявки Участника по одному лоту, если им подано более одной заявки и предыдущая(ие) заявка(и) не была(и) отозвана(ы).

24.11. Заказчик вправе отклонить заявки участника, если Участником не были предоставлены все документы, предусмотренные настоящим извещением, либо были поданы документы, оформленные с нарушением требований, установленных настоящим извещением.

24.12. Заказчик вправе запросить у соответствующих органов и организаций сведения о проведении ликвидации Участника закупки - юридического лица, подавшего заявку на участие в запросе котировок, о наличии решения арбитражного суда о признании такого Участника - юридического лица, индивидуального предпринимателя банкротом и об открытии конкурсного производства, о приостановлении деятельности такого участника в порядке, предусмотренном КоАП РФ, о наличии задолженностей такого участника по начисленным налогам, сборам и иным обязательным платежам в бюджеты любого уровня и в государственные внебюджетные фонды за прошедший календарный год, об обжаловании наличия таких задолженностей и о результатах рассмотрения жалоб.

24.13. Любой участник закупки вправе направить Заказчику запрос о даче разъяснений положений извещения об осуществлении закупки и (или) документации о закупке при осуществлении Заказчиком закупки в электронной форме в порядке, предусмотренном [ст. 3.3](consultantplus://offline/ref=972737D48DCE0AD9623B2ED97560D65D8CC8DA94A5782B4507979E533F35B9A34813129E86pAS3F) Закона N 223-ФЗ, в остальных случаях в письменной форме, в том числе в виде электронного документа. В течение трех дней со дня поступления такого запроса Заказчик размещает в ЕИС разъяснения с указанием предмета запроса, но без указания участника закупки, от которого поступил запрос. В рамках разъяснений положений извещения и (или) документации о закупке Заказчик не может изменять предмет закупки и существенные условия проекта договора.

24.14. Заказчик вправе не давать разъяснений положений извещения и (или) документации о закупке, если запрос поступил позднее чем за три рабочих дня до даты окончания срока подачи заявок на участие в закупке.

24.15. Заказчик по собственной инициативе или в соответствии с запросом участника закупки вправе принять решение о внесении изменений в извещение и (или) документацию о закупке. Изменять предмет закупки не допускается.

24.16. Изменения, внесенные в извещение об осуществлении конкурентной закупки, документацию о закупке, размещаются в ЕИС не позднее трех дней со дня принятия решения об их внесении.

В результате внесения указанных изменений срок подачи заявок на участие в закупке должен быть продлен следующим образом. С даты размещения в ЕИС изменений в извещение об осуществлении закупки, документацию о закупке до даты окончания срока подачи заявок на участие в закупке должно оставаться не менее половины срока подачи заявок на участие в закупке, установленного настоящим извещением.

24.17. Заказчик не несет ответственности, если участник закупки не ознакомился с включенными в извещение о запросе котировок изменениями, которые размещены надлежащим образом.

24.18. Заказчик вправе отменить проведение закупки по одному и более предмету закупки (лоту) до наступления даты и времени окончания срока подачи заявок на участие в закупке. Решение об отказе от проведения закупки размещается в ЕИС в день его принятия.

После окончания срока подачи заявок на участие в закупке Заказчик вправе отменить проведение закупки только в случае возникновения обстоятельств непреодолимой силы в соответствии с гражданским законодательством Российской Федерации.

**25. Требования к Участникам закупки.**

25.1. В настоящем извещении о проведении запроса котировок устанавливаются следующие обязательные требования к участникам закупки:

1) участник закупки должен соответствовать требованиям законодательства Российской Федерации к лицам, осуществляющим поставки товаров, выполнение работ, оказание услуг, которые являются предметом закупки;

2) участник закупки должен отвечать требованиям, установленным настоящим извещением о закупке и Положению о закупках Заказчика;

3) участник закупки не находится в процессе ликвидации (для участника - юридического лица), не признан по решению арбитражного суда несостоятельным (банкротом) (для участника - как юридического, так и физического лица);

4) на день подачи заявки или конверта с заявкой деятельность участника закупки не приостановлена в порядке, предусмотренном [Кодексом](consultantplus://offline/ref=972737D48DCE0AD9623B2ED97560D65D8CC9D99EA1722B4507979E533Fp3S5F) РФ об административных правонарушениях;

5) у участника закупки отсутствует недоимка по налогам, сборам, задолженность по иным обязательным платежам в бюджеты бюджетной системы РФ за прошедший календарный год, размер которых превышает 25 процентов от балансовой стоимости активов участника закупки по данным бухгалтерской отчетности за последний отчетный период;

6) сведения об участнике закупки отсутствуют в реестрах недобросовестных поставщиков, ведение которых предусмотрено [Законом](consultantplus://offline/ref=972737D48DCE0AD9623B2ED97560D65D8CC8DA94A5782B4507979E533Fp3S5F) N 223-ФЗ и [Законом](consultantplus://offline/ref=972737D48DCE0AD9623B2ED97560D65D8CC8DA94A27A2B4507979E533Fp3S5F) N 44-ФЗ;

7) участник закупки обладает исключительными правами на интеллектуальную собственность либо правами на использование интеллектуальной собственности в объеме, достаточном для исполнения договора. Данное требование предъявляется, если в связи с исполнением договора Заказчик приобретает права на интеллектуальную собственность либо исполнение договора предполагает ее использование.

25.2. К участникам закупки не допускается устанавливать требования дискриминационного характера.

25.3. Не допускается предъявлять к участникам закупки, товарам, работам, услугам, условиям исполнения договора требования, не предусмотренные извещением и (или) документацией о закупке, а также оценивать и сопоставлять заявки на участие в закупке по критериям и в порядке, которые не указаны в извещении и (или) документации о закупке.

25.4. Требования, предъявляемые к участникам закупки, закупаемым товарам, работам, услугам, условиям исполнения договора, а также критерии и порядок оценки и сопоставления заявок на участие в закупке применяются в равной степени в отношении всех участников закупки.

**26. Условия допуска к участию и отстранения от участия в закупках.**

26.1. Комиссия по закупкам отказывает участнику закупки в допуске к участию в процедуре закупки в следующих случаях:

1) выявлено несоответствие участника хотя бы одному из требований, перечисленных в [п.](#P427) 25 настоящего извещения;

2) участник закупки и (или) его заявка не соответствуют иным требованиям, установленным извещением о проведении запроса котировок;

3) участник закупки не представил документы, необходимые для участия в процедуре закупки;

4) в представленных документах или в заявке указаны недостоверные сведения об участнике закупки и (или) о товарах, работах, услугах;

5) участник закупки не предоставил обеспечение заявки на участие в закупке, если такое обеспечение предусмотрено извещением и (или) документацией о закупке.

**27. Порядок заключения и исполнения договора.**

27.1. Договор заключается Заказчиком в порядке, установленном настоящим извещением, с учетом норм законодательства РФ.

27.2. Договор по результатам проведения закупки Заказчик заключает не ранее чем через 10 дней и не позднее чем через 20 дней с даты размещения в ЕИС итогового протокола, составленного по результатам закупки, в следующем порядке.

В проект договора, который прилагается к извещению о проведении закупки и (или) документации, включаются реквизиты победителя (единственного участника) и условия исполнения договора, предложенные победителем (единственным участником) в заявке на участие в закупке.

В течение пяти дней со дня размещения в ЕИС итогового протокола закупки Заказчик передает победителю (единственному участнику) два экземпляра заполненного проекта договора.

Победитель закупки (единственный участник) в течение пяти дней со дня получения двух экземпляров проекта договора подписывает их, скрепляет печатью (при наличии) и передает Заказчику.

Заказчик не ранее чем через 10 дней со дня размещения в ЕИС протокола закупки, на основании которого заключается договор, подписывает и скрепляет печатью (при наличии) оба экземпляра договора и возвращает один из них победителю закупки (единственному участнику).

Договор по результатам осуществления закупки в электронной форме заключается в указанном ранее порядке и сроки с учетом особенностей документооборота в электронной форме с использованием программно-аппаратных средств электронной площадки и подписывается электронной подписью лиц, имеющих право действовать от имени соответственно участника такой закупки, заказчика.

Если в соответствии с законодательством РФ заключение договора требует получение одобрения от органа управления Заказчика, то договор должен быть заключен не позднее чем через пять дней с даты указанного одобрения. Аналогичный срок действует с даты вынесения решения антимонопольного органа по результатам рассмотрения жалобы на действия (бездействие) Заказчика, комиссии по закупкам, оператора электронной площадки.

27.3. Если участник закупки, с которым заключается договор согласно настоящему извещению, получив проект договора в срок, предусмотренный для заключения договора, обнаружит в его тексте неточности, технические ошибки, опечатки, несоответствие условиям, которые были предложены в заявке этого участника закупки, оформляется протокол разногласий. Протокол разногласий составляется в письменной форме. Он должен содержать следующие сведения:

1) место, дату и время составления протокола;

2) наименование предмета закупки и номер закупки;

3) положения договора, в которых, по мнению участника закупки, содержатся неточности, технические ошибки, опечатки, несоответствие условиям, предложенным в заявке данного участника.

Подписанный участником закупки протокол в тот же день направляется Заказчику.

Заказчик рассматривает протокол разногласий в течение двух рабочих дней со дня его получения от участника закупки. Если замечания участника закупки учтены полностью или частично, Заказчик вносит изменения в проект договора и повторно направляет его участнику. Вместе с тем Заказчик вправе направить участнику закупки договор в первоначальном варианте и отдельный документ с указанием причин, по которым в принятии замечаний участника закупки, содержащихся в протоколе разногласий, отказано. В случае когда по результатам учета замечаний изменяются количество, объем, цена закупаемых товаров, работ, услуг или сроки исполнения договора по сравнению с указанными в протоколе, составленном по результатам закупки, информация об этом размещается в ЕИС не позднее 10 дней со дня внесения изменений.

Участник закупки, с которым заключается договор, в течение пяти дней со дня его получения подписывает договор в окончательной редакции Заказчика, скрепляет его печатью (при наличии) и возвращает Заказчику.

В случае проведения закупки в электронной форме направление протокола разногласий Заказчику и дальнейший обмен документами между поставщиком и Заказчиком в части подписания договора осуществляются с использованием программно-аппаратных средств электронной площадки.

27.4. Участник закупки признается уклонившимся от заключения договора в случае, когда:

1) не представил подписанный договор (отказался от заключения договора) в редакции Заказчика в срок, определенный настоящим извещением;

2) не предоставил обеспечение исполнения договора в срок, установленный документацией (извещением) о закупке, или предоставил с нарушением условий, указанных в документации (извещении) о закупке, - если требование о предоставлении такого обеспечения было предусмотрено документацией о закупке и проектом договора;

3) не представил сведения о цепочке собственников, включая бенефициаров (в том числе конечных), и документы, подтверждающие данные сведения, - если требование о представлении таких сведений и документов установлено документацией о закупке и проектом договора.

27.5. Не позднее одного рабочего дня, следующего за днем, когда установлены факты, предусмотренные в [п.](#P482) 27.4. настоящего извещения, Заказчик составляет протокол о признании участника уклонившимся от заключения договора.

27.6. В случае когда участник закупки признан уклонившимся или отказался от заключения договора, договор заключается с участником запроса котировок, предложение о цене которого является следующим после предложения победителя.

26.7. Договоры, заключенные по результатам закупок, изменяются в порядке и по основаниям, которые предусмотрены положениями этих договоров, а также законодательством РФ, с учетом особенностей, установленных настоящим извещением и Положением о закупках Заказчика.

27.8. Максимальная цена договора является твердой и может изменяться только в следующих случаях:

1) цена снижается по соглашению сторон без изменения предусмотренного договором количества товаров, объема работ, услуг и иных условий исполнения договора;

2) возможность изменить цену договора предусмотрена таким договором.

27.9. При заключении и исполнении договора Заказчик по согласованию с участником, с которым заключается договор, вправе увеличить количество поставляемого товара, если это предусмотрено документацией о закупке. Цена единицы товара в таком случае не должна превышать цену, определяемую как частное от деления цены договора, указанной в заявке участника конкурса, запроса предложений, запроса котировок (предложенной участником аукциона), с которым заключается договор, на количество товара, установленное в документации о закупках.

27.10. Если количество, объем, цена закупаемых товаров, работ, услуг или сроки исполнения договора изменяются по сравнению с указанными в итоговом протоколе, Заказчик не позднее 10 дней со дня внесения изменений в договор размещает в ЕИС информацию об измененных условиях.

27.11. При исполнении договора не допускается перемена поставщика, за исключением случаев, когда новый поставщик является правопреемником поставщика, с которым заключен договор, вследствие реорганизации юридического лица в форме преобразования, слияния или присоединения либо когда такая возможность прямо предусмотрена договором. При перемене поставщика его права и обязанности переходят к новому поставщику в том же объеме и на тех же условиях.

Если при исполнении договора происходит перемена Заказчика, то права и обязанности Заказчика, установленные договором и не исполненные к моменту такой перемены, переходят к новому лицу в объеме и на условиях, предусмотренных заключенным договором.

27.12. При исполнении договора по согласованию сторон допускается поставка товара, качество, технические и функциональные характеристики (потребительские свойства) которого улучшены по сравнению с указанными в договоре.

27.13. В договор включается условие о порядке, сроках и способах предоставления обеспечения исполнения договора, если соответствующее требование установлено Заказчиком в документации о закупке.

**Приложение № 1 к извещению**

**ПРИМЕРНАЯ ФОРМА КОТИРОВОЧНОЙ ЗАЯВКИ**

На бланке организации

Дата, исх. номер

Руководителю заказчика

**Котировочная заявка**

**Участник закупки:**

|  |  |
| --- | --- |
| Юридический адрес |  |
| Фактический адрес |  |
| Контактный телефон |  |
| Факс |  |
| Банковские реквизиты: | |
| ИНН |  |
| КПП |  |
| ОГРН |  |
| БИК |  |
| р/с |  |
| к/с |  |
| Наименование банка |  |
|  | |

Изучив извещение о запросе котировок мы, нижеподписавшиеся, сообщаем, что в отношении  *наименование участника*  не проводится ликвидация, отсутствует решение арбитражного суда о признании банкротом, деятельность  *наименование участника*  не приостановлена в порядке, предусмотренном Кодексом РФ об административных правонарушениях, сведения о  *наименование участника*  отсутствуют в Реестрах недобросовестных поставщиков, предусмотренных Федеральными законами 44-ФЗ от 22.03.2013г. и 223-ФЗ от 18.07.2011 г., у  *наименование участника*  отсутствует недоимка по налогам, сборам, задолженность по иным обязательным платежам в бюджеты бюджетной системы РФ за прошедший календарный год, размер которых превышает 25 процентов от балансовой стоимости активов участника закупки по данным бухгалтерской отчетности за последний отчетный период.

Мы,  *наименование участника*  предлагаем осуществить поставку товара в соответствии с условиями, указанными в Проекте договора.

Мы,  *наименование участника\_\_\_\_* выражаем согласие на исполнение договора в соответствии с условиями, изложенными в проекте договора и в извещении о запросе котировок.

**Спецификация поставляемого товара в соответствии с Заданием на поставку:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  п/п | Наименование товара,  (тип, марка, комплектность) | Единица измерения | Кол-во | Цена за единицу | Сумма (с НДС) |
|  |  |  |  |  |  |
|  | **ИТОГО** |  |  |  |  |

|  |  |
| --- | --- |
| **Сведения о включенных в цену договора расходах\*** |  |
| **Цена договора** |  |
| **Срок поставки** |  |
| **Гарантийные обязательства** |  |
| **Условия оплаты** |  |

\* В цену договора, предлагаемую Исполнителем должны входить все расходы, связанные с поставляемым товаром, в том числе расходы на перевозку, уплату таможенных пошлин, налогов, сборов и другие обязательные платежи, и иные расходы, предусмотренные Извещением или Проектом договора

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность подпись/печать

**Проект договора**

**Приложение № 2 к извещению**

**Договор №\_\_\_\_\_\_\_\_\_\_\_\_**

**на оказание услуг по развитию и поддержке системы защиты информации**

г. Уфа «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

МУП ЕРКЦ г.Уфы, именуемый в дальнейшем «Заказчик», в лице генерального директора Винниковой Айгуль Наилевны, действующего на основании Устава, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_», именуемый в дальнейшем «Исполнитель», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_., действующего на основании \_\_\_\_\_\_\_\_\_\_\_, с другой стороны, в дальнейшем вместе именуемые «Стороны», с соблюдением требований Федерального закона от 18.07.2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» (далее – Федеральный закон №223-ФЗ) и иного законодательства Российской Федерации, на основании результатов размещения государственного заказа путем проведения электронного аукциона (на основании протокола подведения итогов электронного аукциона \_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_ г.) заключили настоящий Договор (далее - Договор) о нижеследующем:

**1. Предмет Договора**

1.1. Исполнитель обязуется оказать услуги по обновлению, сопровождению и приобретению программного обеспечения (далее ПО):

1.1.1 Программный комплекс ViPNet:

* услуги по технической поддержке продуктов ViPNet для сети № 1960, уровень Расширенный

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Количество** |
| 1 | ПО ViPNet Administrator 4.х ( КС2) | 1 |
| 2 | ViPNet Coordinator HW1000 | 1 |
| 3 | ПО ViPNet Client 4.х (КС2) | 350 |

1.1.2 Антивирус Касперского

* Kaspersky Endpoint Security для бизнеса – Расширенный, продление лицензии на 340 РС, подписка на 1 год
* Kaspersky Security для почтовых серверов, продление лицензии на 200 РС, подписка на 1 год

1.1.3 Система резервного копирования Acronis Защита Данных Расширенная:

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Количество** |
| 1 | Неисключительное право на программное обеспечение Acronis Защита Данных Расширенная для физического сервера | 28 |
|  | Сертификат на техническую поддержку Acronis Защита Данных Расширенная для физического сервера | 28 |
| 2 | Неисключительное право на программное обеспечение Acronis Защита Данных Расширенная для рабочей станции | 8 |
| 3 | Сертификат на техническую поддержку Acronis Защита Данных Расширенная для рабочей станции | 8 |

1.1.4 Неисключительные права на использование программы для ЭВМ «Автоматизация формирования и актуализации внутренней документации учреждений и организаций (Альфа-док)». Клиентская лицензия «КИИ.ПДн.Эксперт» на срок 1 (один) год

1.2. В состав Услуг входит передача Сертификатов активации сервисов технической поддержки программных продуктов (далее – Сертификат) и передача лицензий/лицензионных соглашений, кодов/ключей активации ПО в соответствии со Спецификацией (Приложение №1 к Договору).

1.3. Требования, предъявляемые к услугам, оказываемым в рамках настоящего Договора, а также функциональные, технические, качественные характеристики и эксплуатационные характеристики (при необходимости) материалов, объем, содержание, и другие условия оказания услуг определяются Техническим заданием (Приложение № 2 к Договору), являющимся неотъемлемой частью Договора.

1.4. При исполнении Договора по согласованию Заказчика с Исполнителем допускается оказание услуг, качество, технические и функциональные характеристики (потребительские свойства) которых являются улучшенными по сравнению с качеством и такими техническими и функциональными характеристиками услуг, указанными в Договоре.

**2. Обязанности сторон**

2.1. Исполнитель обязуется:

2.1.1. Оказать Заказчику услуги, в комплекте, предусмотренном Спецификацией (Приложение №1 к Договору).

2.1.2. Предоставить Заказчику бумажные экземпляры Сертификатов, заверенных подписями уполномоченных должностных лиц производителей и печатью производителей программного обеспечения, указанного в Спецификации к Договору (далее - Производитель).

2.1.3. Оказывать как своими силами, так и силами Производителя техническую поддержку программного обеспечения, указанного в Спецификации в соответствии с Перечнем и характеристиками оказываемых услуг (Приложение №2 к Договору).

2.1.4. Оказывать техническую поддержку в течение 1 (одного) года с момента предоставления Сертификата, в будние дни по телефону с 9:00 до 18:00 по московскому времени, в будние дни по электронной почте с 9:00 до 18:00 по московскому времени.

2.1.5. Назначить специалиста отдела информационных технологий и защиты информации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ответственным за исполнение п. 2.1.4. Договора. Телефон для связи \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, адрес электронной почты \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

2.1.6. Рассматривать обращение Заказчика и предпринимать по нему все необходимые действия в течение 24 часов. В случае, если решить вопрос, изложенный в обращении Заказчика, не представляется возможным в силу объективных причин - в течение трех-пяти рабочих дней с момента направления обращения на адрес электронной почты Исполнителя.

2.1.7. Предоставить информацию о способе связи с Производителем с указанием номера телефона и адреса электронной почты, в рамках оказания технической поддержки Программного обеспечения.

2.2. Заказчик обязуется:

2.2.1. Принять услуги и оплатить в порядке, установленном Договором.

2.2.2. Назначить главного специалиста по организации начисления и сбору платежей Уватьева В.Г. ответственным за обращения в рамках исполнения пункта 2.1.3 и 2.1.4 настоящего Договора. Телефон для связи +7 (347) 2465000, адрес электронной почты uvatjev@erkcufa.ru

**3. Порядок и место оказания услуг**

3.1. Выполнение услуг осуществляется Исполнителем в течение 365 календарных дней с момента заключения Договора по адресу: Уфа, ул. Комсомольская 165/4 силами и за счет Исполнителя, по предварительному согласованию с Заказчиком.

3.2. Услуги должны быть оказаны в соответствии с Техническим заданием (Приложение № 2 к Договору).

3.3. Факт оказания услуг Исполнителем и принятия их Заказчиком должен быть подтвержден актом об оказании услуг, подписанным обеими сторонами.

3.4. Акт об оказании услуг должен быть подписан Заказчиком в течение пяти рабочих дней с момента его получения от Исполнителя, если услуги оказаны Исполнителем надлежащим образом и в полном объеме, либо в те же сроки Заказчиком направляется в письменной форме мотивированный отказ от подписания такого документа.

3.5. Передача Сертификатов технической поддержки считается состоявшейся, если выполнены все условия приема и передачи Сертификатов, а именно:

* передан бумажный экземпляр Сертификата на оказание услуг по технической поддержке Программного обеспечения, содержащий в себе номер Сертификата, информацию об уровне сопровождения и перечень продуктов, заверенный подписью уполномоченного должностного лица Производителя и печатью Производителя (оригиналы).
* зарегистрирован электронный экземпляр Сертификата на оказание услуг по технической поддержке Программного обеспечения, содержащий в себе номер Сертификата, информацию об уровне сопровождения и перечень продуктов, в личном кабинете на сайте производителя программного обеспечения.
* зарегистрирован электронный экземпляр Лицензии на программное обеспечение, содержащий в себе номер Лицензии и перечень продуктов, в личном кабинете на сайте производителя программного обеспечения.

**4. Цена, порядок расчетов**

4.1 Стоимость Услуг по настоящему Договору согласно Спецификации (далее - сумма Договора) составляет **\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) рублей**. Цена Договора является твердой в течение всего срока действия Договора, не подлежит изменению в связи с изменениями МРОТ, налогового законодательства, иных обстоятельств, за исключением случаев, предусмотренных законодательством Российской Федерации.

4.2. Оплата Услуг производится в течение 10 (Десяти) рабочих дней после подписания Заказчиком документа о приемке.

4.3. Указанная в Договоре стоимость Услуг включает в себя все необходимые платежи Исполнителя автору и иным правообладателям Программного обеспечения.

4.4. В случае изменения расчетного счета, Исполнитель обязан в однодневный срок в письменной форме сообщить об этом Заказчику, указав новые реквизиты расчетного счета, в противном случае все риски, связанные с перечислением Заказчиком денежных средств на указанный в Договоре счет Исполнителя, несет Исполнитель.

4.5. Оплата, по решению Заказчика может быть уменьшена на сумму неустойки (пеней, штрафов) при условии перечисления в установленном порядке неустойки (пени, штрафа) в доход соответствующего бюджета бюджетной системы Российской Федерации на основании платежного документа, оформленного получателем бюджетных средств, с указанием Исполнителя, за которого осуществляется перечисление неустойки (пеней, штрафов) в соответствии с условиями Договора. При этом оплата Исполнителю будет осуществлена за вычетом неустойки перечисленной в доход соответствующего бюджета бюджетной системы Российской Федерации.

4.6. В случае, если Договор заключается с физическим лицом, за исключением индивидуального предпринимателя или иного занимающегося частной практикой лица, Заказчик уменьшает сумму, подлежащую уплате физическому лицу, на размер налоговых платежей, связанных с оплатой Договора.

**5. Ответственность сторон**

5.1. В случае неисполнения, несвоевременного или ненадлежащего исполнения обязательств по Договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации и Договором. Возмещению подлежит прямой действительный ущерб, упущенная выгода не возмещается. Бремя доказывания убытков лежит на потерпевшей стороне.

В случае просрочки исполнения Заказчиком обязательств, предусмотренных Договором, а также в иных случаях неисполнения или ненадлежащего исполнения заказчиком обязательств, предусмотренных Договором, подрядчик вправе потребовать уплаты неустоек (штрафов, пеней). Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного Договором, начиная со дня, следующего после дня истечения установленного Договором срока исполнения обязательства. Такая пеня устанавливается в размере одной трехсотой действующей на дату уплаты пеней ставки рефинансирования Центрального банка Российской Федерации от не уплаченной в срок суммы.

5.2. Штрафы начисляются за ненадлежащее исполнение заказчиком обязательств, предусмотренных Договором, за исключением просрочки исполнения обязательств, предусмотренных Договором. Размер штрафа устанавливается в виде фиксированной суммы, определенной в порядке, установленном постановлением Правительства РФ от 25.11.2013 № 1063 "Об утверждении Правил определения размера штрафа, начисляемого в случае ненадлежащего исполнения заказчиком, исполнителем (подрядчиком, исполнителем) обязательств, предусмотренных Договором (за исключением просрочки исполнения обязательств заказчиком, исполнителем (подрядчиком, исполнителем), и размера пени, начисляемой за каждый день просрочки исполнения исполнителем (подрядчиком, исполнителем) обязательства, предусмотренного Договором" (далее - Постановление № 1063) и составляет 2,5 % цены Договора - \_\_\_\_\_\_\_\_\_\_ руб. \_\_\_\_\_\_ коп.

5.3. В случае просрочки исполнения обязательств, предусмотренных Договором, а также в иных случаях неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Договором, заказчик направляет требование об уплате неустоек (штрафов, пеней).

5.4. Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного Договором, начиная со дня, следующего после дня истечения установленного Договором срока исполнения обязательства, и устанавливается Договором в размере, определенном в порядке, установленном Постановлением № 1063, но не менее чем одна трехсотая действующей на дату уплаты пени ставки рефинансирования Центрального банка Российской Федерации от цены Договора, уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных Договором и фактически исполненных Исполнителем, и определяется по формуле:

П=(Ц-В) х С

(где Ц – цена Договора; В – стоимость фактически исполненного в установленный срок Исполнителем обязательства по Договору, определяемая на основании документа о оказании услуг, в том числе отдельных этапов исполнения Договора; С – размер ставки).

Размер ставки определяется по формуле:

С=СЦБ х ДП

(где СЦБ – размер ставки рефинансирования, установленной Центральным банком Российской Федерации на дату уплаты пени, определяемый с учетом коэффициента К; ДП – количество дней просрочки).

Коэффициент К определяется по формуле:

К=ДП/ДК х 100%

(где ДП – количество дней просрочки; ДК – срок исполнения обязательства по Договору (количество дней).

При К, равном 0-50 процентам, размер ставки определяется за каждый день просрочки и принимается равным 0,01 ставки рефинансирования, установленной Центральным банком Российской Федерации на дату уплаты пени.

При К, равном 50-100 процентам, размер ставки определяется за каждый день просрочки и принимается равным 0,02 ставки рефинансирования, установленной Центральным банком Российской Федерации на дату уплаты пени.

При К, равном 100 процентам и более, размер ставки определяется за каждый день просрочки и принимается равным 0,03 ставки рефинансирования, установленной Центральным банком Российской Федерации на дату уплаты пени.

5.5. Штрафы начисляются за неисполнение или ненадлежащее исполнение Исполнителем обязательств, предусмотренных Договором, за исключением просрочки исполнения Исполнителем обязательств (в том числе гарантийного обязательства), предусмотренных Договором. Размер штрафа устанавливается в виде фиксированной суммы, определенной в порядке, установленном Постановлением № 1063 и составляет 10 % цены Договора – \_\_\_\_\_\_\_\_\_\_\_\_ руб. 00 коп.

5.6. Сторона 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.

5.7. Уплата неустоек (штрафов, пеней) не освобождает стороны от выполнения принятых обязательств.

**6. Обстоятельства непреодолимой силы**

6.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Договору, в случае если оно явилось следствием обстоятельств непреодолимой силы, а именно: наводнения, пожара, землетрясения, диверсии, военных действий, блокады, изменения законодательства, препятствующих надлежащему исполнению обязательств по настоящему Договору, а также других чрезвычайных обстоятельств, ко­торые возникли после заключения настоящего Договора и непосредственно повлияли на исполнение Сторонами своих обязательств, а также которые Стороны были не в состоянии предвидеть и предотвратить.

6.2. Сторона, подвергшаяся действию обстоятельств непреодолимой силы, обязана немедленно письменно уведомить другую Сторону о возникновении, виде и возможной продолжительности действия указанных обстоятельств. Данное уведомление должно быть подтверждено компетентным органом территории, где данное обстоятельство имело место (в случае если Исполнителем является нерезидент Российской Федерации - Торгово-промышленной палатой страны, где данное обстоятельство имело место).

6.3. Если такого уведомления не будет сделано в насколько возможно короткий срок, Сторона, подвергшаяся действию обстоятельств непреодолимой силы, лишается права ссылаться на них в свое оправдание, разве что само то обстоятельство не давало возможности послать уведомление.

6.4. Возникновение обстоятельств непреодолимой силы продлевает срок исполнения обязательств по настоящему Договору на период, который в целом соответствует сроку действия наступившего обстоятельства.

6.5. Если обстоятельства непреодолимой силы будут продолжаться свыше 10 дней, то каждая из Сторон вправе требовать расторжения настоящего Договора полностью или частично и в таком случае ни одна из Сторон не будет иметь права требовать от другой Стороны возмещения возможных убытков.

**7. Обеспечение исполнения Договора**

7.1 Размер обеспечения исполнения Договора составляет 5% начальной (максимальной) цены Договора – \_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) рублей \_\_\_\_\_ коп.

7.2. В случае, если предложенная в заявке участника закупки (Исполнителя) цена снижена на двадцать пять и более процентов ниже начальной (максимальной) цены Договора, Договор заключается только после предоставления таким участником обеспечения исполнения Договора в размере, превышающем в 1,5 (полтора) раза размер обеспечения исполнения Договора, указанный в документации об аукционе, что составляет – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) рублей \_\_\_ коп., или информации, подтверждающей добросовестность такого участника на дату подачи.

Реквизиты счета для предоставления обеспечения исполнения Договора:

Получатель: МУП ЕРКЦ г.Уфы

Номер лицевого счета:

Номер расчетного счета: 40702810206020100020 ОТДЕЛЕНИЕ №8598 СБЕРБАНКА РОССИИ

к/сч 30101810300000000601

БИК: 048073601

ИНН 0276069810

КПП 027601001

В назначении платежа указать: внесение денежных средств в качестве обеспечения исполнения Договора по аукциону в электронной форме № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Исполнение обязательств по Договору может обеспечиваться предоставлением банковской гарантии, выданной банком и соответствующей требованиям действующего законодательства Российской Федерации, или внесением денежных средств на указанный Заказчиком счет, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими Заказчику. Способ обеспечения исполнения Договора определяется участником закупки, с которым заключается Договор, самостоятельно.

Оригинал безотзывной банковской гарантии передается Заказчику не позднее 10 рабочих дней с момента заключения Договора. Срок действия банковской гарантии должен превышать срок действия Договора не менее чем на один месяц.

* 1. В случае если по каким-либо причинам обеспечение исполнения Договора перестало быть действительным, закончило свое действие или иным образом перестало обеспечивать исполнение Исполнителем его обязательств по Договору, Исполнитель обязуется в течение 10 рабочих дней предоставить Заказчику иное (новое) надлежащее обеспечение исполнения Договора на тех же условиях и в том же размере, предусмотренные условиями настоящего Договора.
  2. В случае предоставления Заказчику обеспечения исполнения Договора, денежные средства, внесенные в качестве обеспечения исполнения настоящего Договора должны быть возвращены Исполнителю после исполнения всех обязательств по настоящему Договору в течение 10 банковских дней.
  3. В ходе исполнения Договора Исполнитель вправе предоставить Заказчику обеспечение исполнения Договора, уменьшенное на размер выполненных обязательств, предусмотренных Договором, взамен ранее предоставленного обеспечения исполнения Договора. При этом может быть изменен способ обеспечения исполнения Договора.

**8. Порядок урегулирования споров и расторжение Договора**

8.1. Стороны принимают все меры для того, чтобы любые спорные вопросы, разногласия либо претензии, касающиеся исполнения настоящего Договора, были урегулированы путем переговоров с оформлением совместного протокола урегулирования споров.

8.2. В случае не достижения взаимного согласия все споры, разногласия подлежат разрешению в Арбитражном суде РБ в соответствии с действующим законодательством.

8.3. Расторжение Договора допускается по соглашению сторон, по решению суда, а в случае одностороннего отказа стороны Договора от исполнения Договора в соответствии с гражданским законодательством. В случае расторжения Договора по вине или инициативе Исполнителя сумма обеспечения Договора Исполнителю не возвращается, переходит в полном объеме Заказчику.

8.4. Заказчик вправе принять решение об одностороннем отказе от исполнения Договора по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения отдельных видов обязательств. Принятие решения об одностороннем отказе от исполнения Договора Заказчика осуществляется в соответствии с Федеральным законом № 223-ФЗ.

8.5. Решение Заказчика об одностороннем отказе от исполнения Договора направляется Исполнителю по почте заказным письмом с уведомлением о вручении по адресу Исполнителя, указанному в Договоре, либо посредством факсимильной связи, либо по адресу электронной почты, либо с использованием иных средств связи и доставки, обеспечивающих фиксирование такого уведомления и получение Заказчиком подтверждения о его вручении Исполнителю. Датой такого надлежащего уведомления признается дата получения Заказчиком подтверждения о вручении Исполнителю указанного уведомления либо дата получения Заказчиком информации об отсутствии Исполнителя по его адресу, указанному в Договоре.

8.6. Решение Заказчика об одностороннем отказе от исполнения Договора вступает в силу и Договор считается расторгнутым через десять дней с даты надлежащего уведомления Заказчиком Исполнителя об одностороннем отказе от исполнения Договора.

8.7. Заказчик обязан отменить не вступившее в силу решение об одностороннем отказе от исполнения Договора, если в течение десятидневного срока с даты надлежащего уведомления Исполнителя о принятом решении об одностороннем отказе от исполнения Договора устранено нарушение условий Договора, послужившее основанием для принятия указанного решения, а также Заказчику компенсированы затраты на проведение экспертизы. Данное правило не применяется в случае повторного нарушения Исполнителем условий Договора, которые в соответствии с [гражданским законодательством](garantF1://10064072.4502) являются основанием для одностороннего отказа Заказчика от исполнения Договора.

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

8.9. Информация о Исполнителе, с которым Договор расторгнут в связи с односторонним отказом Заказчика от исполнения Договора, включаются в установленном в соответствии с Федеральным законом № 223-ФЗ порядке в реестр недобросовестных поставщиков.

8.10. При расторжении Договора в связи с односторонним отказом стороны Договора от исполнения Договора другая сторона Договора вправе потребовать возмещения только фактически понесенного ущерба, непосредственно обусловленного обстоятельствами, являющимися основанием для принятия решения об одностороннем отказе от исполнения Договора.

**9. Срок действия Договора**

Настоящий Договор вступает в силу с момента его подписания и действует до выполнения Сторонами всех взаимных обязательств.

**10. Общие положения**

10.1. Любые изменения, дополнения и приложения к настоящему Договору действительны, если они выполнены в письменной форме и подписаны уполномочен­ными представителями каждой из Сторон.

10.2. Официальным языком Договора является русский язык.

В случае разночтений в текстах, написанных на разных языках, официальный язык Договора признается основным для решения всех вопросов, касающихся значения или интерпретации Договора.

10.3. Настоящий Договор будет считаться исполненным и прекратившим свое действие после выполнения Сторонами взаимных обязательств и осуществления окончательных расчетов между Сторонами по настоящему Договору.

10.4. Любое уведомление, запрос или согласие, выдача которых необходима или разрешена в связи с настоящим Договором, оформляется в письменном виде и направляется одной Стороной другой Стороне заказной почтой, электронной почте или факсу по следующим адресам:

Заказчику:   
Адрес: г. Уфа, ул. Комсомольская 165/1

Телефон, факс: +7 (347) 2465000

Контактное лицо: Уватьев В.Г.

e-mail: uvatjev@erkcufa.ru

Исполнителю:  
Адрес: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Телефон, факс: \_\_\_\_\_\_\_\_\_\_\_\_

e-mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Контактное лицо: \_\_\_\_\_\_\_\_\_\_\_\_

Любое действие, осуществление которого необходимо или разрешено, и любой документ, оформление которого необходимо или разрешено Заказчиком или Исполнителем в рамках настоящего Договора, могут быть предприняты или оформлены сотрудниками, указанными ниже и являющимися уполномочен­ными представителями Сторон.

**11. Адреса и реквизиты сторон**

|  |  |
| --- | --- |
| **Заказчик** | **Исполнитель** |
| МУП ЕРКЦ г.Уфы  450098 г.Уфа, ул.Комсомольская, 165/1  ИНН 0276069810  КПП 027601001  р/сч 40702810206020100020  ОТДЕЛЕНИЕ №8598 СБЕРБАНКА РОССИИ  БИК 048073601  к/сч 30101810300000000601 |  |
| Подпись:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Винникова А.Н./  М.П. |  |

Приложение №1

к Договору

№ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

**СПЕЦИФИКАЦИЯ**

­­­­­­­­­­­­­­­­­­­­­­­­­­

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/п | Наименование | Страна происхождения, товарный знак (при наличии) | Количество, шт. | Цена, р. | Сумма с НДС, р |
| 1 |  | Россия |  |  |  |
|  | **ИТОГО** | | | |  |

Приложение №2

к Договору

**Техническое задание**

**на продление лицензий и приобретение технической поддержки программных средств защиты информации**

1. **Требования к поставщику**

Поставщик должен иметь действующую лицензию ФСБ России на осуществление деятельности, связанной с криптографическими (шифровальными) средствами; действие лицензии должно распространяться на работы (услуги), согласно пунктам 12, 20, 21 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося Приложением к постановлению Правительства РФ № 313 от 16.04.2012 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», либо наличие лицензии ФСБ России на осуществление распространения шифровальных (криптографических) средств и на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств.

**Поставщик должен иметь официальное представительство или офис на территории города Уфы Республики Башкортостан. Поставщик должен являться авторизованным/сертифицированным партнером производителей с наличием сертифицированных специалистов технической поддержки (подтверждается копией трудового договора либо копией трудовой книжки, либо иным аналогичным документом, а также соответствующими действующими сертификатами.**

1. **Требования к качеству и безопасности услуг**

Качество услуг должно соответствовать санитарно-эпидемиологическим нормам, а также иным требованиям качества, безопасности жизни и здоровья, требованиям сертификации, безопасности (государственным стандартам и т.п.), лицензирования, если такие требования предъявляются действующим законодательством Российской Федерации или производителем.

1. **Требования к гарантийному сроку**

Гарантийный срок оказанной услуги должен быть не менее 12 (двенадцати) месяцев с даты подписания акта оказанных услуг.

Гарантийный срок распространяется на произведенные работы.

В случае некачественного оказания услуг Исполнитель в течение гарантийного срока обязуется устранить возникшие неполадки за свой счет и обеспечить качественное оказание услуг.

В цену Договора, включаются расходы по оплате всех необходимых налогов, пошлин и сборов.

1. **Технические требования на оказание услуг по развитию и поддержке системы защиты информации** 
   1. **Сертификат активации сервиса совместной технической поддержки ПО ViPNet для сети № 1960 на срок 1 год, уровень – Расширенный**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Количество** |
| 1 | ПО ViPNet Administrator 4.х ( КС2) | 1 |
| 2 | ПАК ViPNet Coordinator HW 1000 | 1 |
| 3 | ПО ViPNet Client 4.х (КС2) | 350 |

Общие требования:

Наличие у Исполнителя сертифицированного специалиста по администрированию программного обеспечения ViPNet Custom в г. Уфа (подтверждается трудовым договором и соответствующими сертификатами).

Наличие у Исполнителя действующей лицензии ФСБ России на осуществление деятельности, связанной с криптографическими (шифровальными) средствами; действие лицензии должно распространяться на работы (услуги), согласно пунктам 12, 20, 21 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося Приложением к постановлению Правительства РФ № 313 от 16.04.2012 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», либо наличие лицензии ФСБ России на осуществление распространения шифровальных (криптографических) средств и на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств.

Перечень предоставляемых услуг:

* Консультации по работе ПО ViPNet по электронной почте, по телефону «Горячей линии», с выездом к Заказчику
  + Прием сообщений должен вестись с учетом режима рабочего времени.
  + Приём обращений и консультирование по электронной почте с 9:00 до 18:00;
  + Приём обращений и консультирование по телефону горячей линии с 9:00 до 18:00
* Консультирование при установке программного обеспечения ViPNet, включающее:
  + Рекомендации по процессу установки продукта в объеме эксплуатационной документации;
  + Ответы на вопросы, возникающие при установке
* Консультирование при эксплуатации должно включать в себя:
  + Рекомендации по настройке продукта в объеме эксплуатационной документации;
  + Ответы на вопросы, возникающие в процессе эксплуатации;
  + Расшифровка кодов ошибок;
  + Рекомендации по «тонкой» настройке продукта с учетом особенностей системы Заказчика;
* Обновление программного обеспечения ViPNet при выходе новых версий:
  + Должны быть предоставлены обновления (hotfix), а также все изменения, производимые в рамках минорной (MINOR) версии программного обеспечения ViPNet (service pack) без взимания дополнительной платы
  + Должны быть предоставлены новые версии (изменение мажорной (MAJOR) версии, поколения) программного обеспечения ViPNet без взимания дополнительной платы
  + Новые версии должны передаваться посредством пересылки экземпляров программного обеспечения ViPNet на CD-дисках
* Исправление ошибок и предоставление релизов с исправлениями в рамках версии:
* Должны быть предоставлены обновления (hotfix), устраняющее дефекты, выявленные в продукте.
* Восстановление работоспособности (ремонт) вышедшего из строя оборудования (аппаратной платформы ПАК) из состава Продуктов Заказчика в соответствии с гарантийными обязательствами ОАО «ИнфоТеКС»
* Проведение не реже одного раза в месяц мониторинга состояния эксплуатации сети ViPNet с оформлением технического отчета. В отчете указываются выводы по соответствию технических конфигураций АРМ, использующих ПО ViPNet, положениям эксплуатационной документации и формуляра на ПО ViPNet.
* Проведение работ по плановой смене ключевой информации и в случае их компрометации.
* Выявление и устранение проблем, возникающих у пользователей при эксплуатации продуктов и выявленных в ходе ежемесячного мониторинга (используя электронную почту, «горячую» телефонную линию, выезды к заказчику).
* Разработка рекомендаций:
* для обеспечения деятельности информационных служб Заказчика, связанных с эксплуатацией ПО ViPNet,
* для реализации функций удостоверяющего центра корпоративного уровня класса КС2,
* по организации межсетевого взаимодействия сетей ViPNet,
* по организации сегментирования и туннелирования в защищенной сети ViPNet,
* по совместной эксплуатации ПО ViPNet с другими СЗИ (Dallas Lock, КриптоПРО, Континент АП).
  1. **Технические требования Антивирусного средства Kaspersky Endpoint Security для бизнеса – Расширенный и защиты почтовых серверов**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Количество** |
| 1 | Программное обеспечение Kaspersky Endpoint security для бизнеса - Расширенный для защиты рабочих станций и файловых серверов, лицензия на 1 год, продление | 340 |
| 2 | Программное обеспечение Kaspersky Security для почтовых серверов, лицензия на 1 год, продление | 200 |

Общие требования

Антивирусные средства должны включать:

• Программные средства антивирусной защиты для рабочих станций Windows.

• Программные средства антивирусной защиты для рабочих станций Linux.

• Программные средства антивирусной защиты для файловых серверов Windows.

• Программные средства антивирусной защиты для файловых серверов Linux.

• Программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов).

• Программные средства централизованного управления, мониторинга и обновления.

• Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange.

• Обновляемые базы данных сигнатур вредоносных программ и атак.

• Эксплуатационную документацию на русском языке.

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

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

Требования к программным средствам антивирусной защиты для рабочих станций Windows

* Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий:
* Windows 7 Home / Professional / Enterprise (32 / 64-разрядная);
* Windows 8 Professional / Enterprise (32 / 64-разрядная);
* Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
* Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядная).
* В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:
* антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
* фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
* проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
* блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
* распознавания и блокировку фишинговых и небезопасных сайтов;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
* возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
* контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
* возможность управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
* записи в журнал событий о записи и/или удалении файлов на съемных дисках;
* контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
* защиты от атак типа BadUSB;
* запуск специальной задачи для обнаружения закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
* защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
* установки только выбранных компонентов программного средства антивирусной защиты;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* запуск задач по расписанию и/или сразу после запуска приложения;
* гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* возможность проверки целостности антивирусной программы;
* возможность добавления исключений из антивирусной проверки по контрольной сумме файла, маске имени/директории или по наличию у файла доверенной цифровой подписи;
* наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
* наличие защищенного хранилища для отчетов о работе антивируса;
* возможность включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
* возможность интеграции с Windows Defender Security Center;
* наличие поддержки Antimalware Scan Interface (AMSI);
* наличие поддержки Windows Subsystem for Linux (WSL);
* возможность защитить паролем восстановление объектов из резервного хранилища.
* полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем;
* восстановления зашифрованного содержимого в случае сбоев загрузочного агента или 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);

Требования к программным средствам антивирусной защиты для рабочих станций Linux:

* Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 32-битных операционных систем следующих версий:
* Ubuntu 16.04 LTS и выше;
* Red Hat® Enterprise Linux® 6.7 и выше;
* CentOS 6.7 и выше;
* Debian GNU / Linux 9.4 и выше;
* Debian GNU / Linux 10;
* Linux Mint 18.2 и выше;
* Linux Mint 19 и выше;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.3 Рабочая станция;
* Альт Линукс 8.3 Рабочая станция К;
* Альт Линукс 8.3 Сервер;
* Альт Линукс 8.3 Образование;
* Альт Линукс 9 Рабочая станция;
* Альт Линукс 9 Образование;
* Гослинукс 6.6;
* Mageia 4.
* Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 64-битных операционных систем следующих версий:
* Ubuntu 16.04 LTS и выше;
* Ubuntu 18.04 LTS и выше;
* Red Hat Enterprise Linux 6.7 и выше;
* Red Hat Enterprise Linux 7.2 и выше;
* Red Hat Enterprise Linux 8.0 и выше;
* CentOS 6.7 и выше;
* CentOS 7.2 и выше;
* CentOS 8.0 и выше;
* Debian GNU / Linux 9.4 и выше;
* Debian GNU / Linux 10.1 и выше;
* OracleLinux 7.3 и выше;
* OracleLinux 8 и выше;
* SUSE® Linux Enterprise Server 15 и выше;
* openSUSE® Leap 15 и выше;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.3 Рабочая станция;
* Альт Линукс 8.3 Рабочая станция К;
* Альт Линукс 8.3 Сервер;
* Альт Линукс 8.3 Образование;
* Альт Линукс 9 Рабочая станция;
* Альт Линукс 9 Сервер;
* Альт Линукс 9 Образование;
* Amazon Linux AMI;
* Linux Mint 18.2 и выше;
* Linux Mint 19 и выше;
* Astra Linux Special Edition 1.5 (обычный режим и режим замкнутой программной среды);
* Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды);
* Astra Linux Common Edition «Орел» 2.12;
* ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем;
* ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем;
* Гослинукс 6.6;
* Гослинукс 7.2;
* AlterOS 7.5 и выше;
* Pardus OS 19.1.
* В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:
* резидентного антивирусного мониторинга;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* проверку ресурсов доступных по SMB / NFS;
* возможность проверки памяти ядра;
* эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
* проверку сообщений электронной почты в текстовом формате (Plain text);
* наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
* защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
* возможность включения опции блокирования файлов во время проверки;
* помещение подозрительных и поврежденных объектов на карантин;
* проверку почтовых баз приложений Microsoft Outlook на наличие вредоносных объектов;
* возможность перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
* возможность управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли.
* возможность управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения
* возможность проверки съемных дисков
* возможность отслеживания во входящем сетевом трафике активности, характерной для сетевых атак
* возможность проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым

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

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

32-разрядных операционных систем Microsoft Windows

* Windows Server® 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Windows Server 2008 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше.

64-разрядных операционных систем Microsoft Windows

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

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

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

Требования к программным средствам антивирусной защиты мобильных устройств

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

* Android 4.2-10.0.
* iOS 10.0-13.0.
* iPadOS.

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

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

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

* возможность удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;
* возможность отправки команды блокирования и удаления данных;
* возможность создавать групповые политики безопасности мобильных устройств;
* удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM;
* получать отчеты и статистику о работе мобильных устройств пользователей;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervised mode;
* возможность централизованного управления с помощью единой консоли управления.

Требования к программным средствам централизованного управления, мониторинга и обновления:

* Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
* Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Pro для рабочих станций 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 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 2019 Standard 64-разрядная;
* Windows Server 2019 Standard 64-разрядная;
* Microsoft Windows Server 2019 Datacenter 64-разрядная;
* Microsoft Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-разрядная;
* Microsoft Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-разрядная;
* Microsoft Windows Server 2016 (вариант установки Server Core RS3 (v1709) (LTSB/CBB) 64-разрядная;
* Microsoft Windows Server 2016 Standard (LTSB) 64-разрядная;
* Microsoft Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
* Microsoft Windows Server 2016 Datacenter (LTSB) 64-разрядная;
* Microsoft Windows Server 2012 R2 Standard 64-разрядная;
* Microsoft Windows Server 2012 R2 Server Core 64-разрядная;
* Microsoft Windows Server 2012 R2 Foundation 64-разрядная;
* Microsoft Windows Server 2012 R2 Essentials 64-разрядная;
* Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;
* Microsoft Windows Server 2012 Standard 64-разрядная;
* Microsoft Windows Server 2012 Server Core 64-разрядная;
* Microsoft Windows Server 2012 Foundation 64-разрядная;
* Microsoft Windows Server 2012 Essentials 64-разрядная;
* Microsoft Windows Server 2012 Datacenter 64-разрядная;
* Microsoft Windows Storage Server 2016 64-разрядная;
* Microsoft Windows Storage Server 2012 R2 64-разрядная;
* Microsoft Windows Storage Server 2012 64-разрядная;
* Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:
* VMware vSphere 6.5;
* VMware vSphere 6.7;
* VMware Workstation 15 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;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x;
* Parallels Desktop 14;
* Oracle VM VirtualBox 6.x.
* Программные средства централизованного управления, мониторинга и обновления должны 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;
* Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная;
* MySQL Standard Edition 5.7 32-разрядная / 64-разрядная;
* MySQL Enterprise Edition 5.7 32-разрядная / 64-разрядная;
* Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;
* MariaDB Server 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB.
* В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:
* выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
* возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
* возможность настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в 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;
* возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
* возможность иерархии триггеров, по которым происходит перераспределение;
* тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* инвентаризация установленного ПО и оборудования на компьютерах пользователей;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* функция управления мобильными устройствами через сервер Exchange ActiveSync;
* функция управления мобильными устройствами через сервер iOS MDM;
* возможность отправки SMS-оповещений о заданных событиях;
* централизованная установка сертификатов на управляемые мобильные устройства;
* возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
* возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
* построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* поддержка Windows Failover Clustering;
* поддержка интеграции с Windows сервисом Certificate Authority;
* наличие веб-консоли управления приложением;
* наличие портала самообслуживания пользователей;
* портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
* наличие системы контроля возникновения вирусных эпидемий;
* возможность установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
* возможность интеграции по OpenAPI;
* возможность управления антивирусной защитой с использованием WEB консоли.
* автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
* наличие преднастроенных ролей пользователей средств централизованного управления;
* должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей;
* возможность подключения по RDP или штатными средствами из консоли управления;
* пользователю должен выводиться запрос на разрешение дистанционного подключения;
* наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal);
* должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;
* возможность запускать скрипты или 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 или 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 или CEF\ LEEF.

Требования к программным средствам антивирусной защиты и фильтрации спама для серверов Microsoft Exchange

* Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
* Microsoft Windows Server 2019 Standard или Datacenter.
* Microsoft Windows Server 2016 Standard или Datacenter.
* Microsoft Windows Server 2012 R2 Standard или Datacenter.
* Microsoft Windows Server 2012 Standard или Datacenter.
* Microsoft Windows Small Business Server 2011 SP1 Standard.
* Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise или Datacenter.
* Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать с программным обеспечением Microsoft Exchange Server следующих версий:
* Microsoft Exchange Server 2019, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт.
* Microsoft Exchange Server 2016, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт.
* Microsoft Exchange Server 2013 SP1, развернутый как минимум в одной из следующих ролей: Почтовый ящик, Пограничный транспорт или Сервер клиентского доступа (CAS).
* Microsoft Exchange Server 2010 SP3, развернутый как минимум в одной из следующих ролей: Транспортный концентратор, Почтовый ящик или Пограничный транспорт.
* Консоль управления программными средствами антивирусной защиты для серверов Microsoft Exchange должна быть реализована с использованием Microsoft Management Console и должна функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
* Microsoft Windows 10;
* Microsoft Windows 8.1;
* Microsoft Windows 8;
* Microsoft Windows 7 SP1 Professional, Enterprise или Ultimate;
* Microsoft Windows Server 2016;
* Microsoft Windows Server 2012 R2 Standard или Datacenter;
* Microsoft Windows Server 2012 Standard или Datacenter;
* Microsoft Windows Small Business Server 2011 SP1 Standard;
* Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise или Datacenter;
* Microsoft Windows Server 2019 Standard или Datacenter.
* Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны обеспечивать реализацию следующих функциональных возможностей:
* совместимость с DAG в Microsoft Exchange;
* поиск и удаление по требованию всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
* поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в хранящихся на сервере Microsoft Exchange (в том числе в общих папках) сообщениях, включая вложения;
* наличие эвристических методов детектирования;
* проверка почтовых хранилищ и общих папок на сервере, в фоновом режиме для гарантированной обработки всех объектов с использованием самой актуальной версии антивирусных баз без заметного увеличения нагрузки на сервер;
* возможность лечить зараженные архивы;
* возможность выявления и удаления не только однозначно вредоносных, но и потенциально опасных приложений, таких как: рекламные программы, программы-сборщики информации, программы автоматического дозвона на платные сайты и другие утилиты, которые могут использоваться злоумышленниками в своих целях;
* возможность детектирования вредоносных и фишинговых ссылок в теле письма;
* сохранение копий изменяемых сообщений в резервном хранилище, что позволяет восстановить важную информацию в случае некорректного лечения объекта;
* набор параметров поиска для удобства нахождения объекта в резервном хранилище;
* дополнительный уровень проверки с помощью репутационных облачных сервисов;
* возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;
* наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз;
* проверка различных параметров письма, таких как адреса отправителей и получателей, размер письма, а также поля заголовка сообщения;
* фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
* проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);
* проверка IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF);
* проверка с помощью сервиса SPAM URI Realtime Block lists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
* использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и файлов вложений);
* возможность использовать роли пользователей/администраторов для разграничения доступа к настройкам безопасности;
* аудит изменения параметров программы по событиям в журнале событий Windows;
* мониторинг состояния программы, получение статистики работы программы и управление белыми и черными списками адресов Анти-Спама с помощью команд в среде Windows PowerShell;
* использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и имён файлов);
* возможность фильтрации файлов Microsoft Office, содержащих макросы;
* возможность проверки и удаления сообщений, являющихся спамом или содержащих фишинговые и вредоносные ссылки;
* проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
* создание отчетов по работе системы защиты;
* возможность автоматической рассылки отчетов администраторам по расписанию;
* возможность обновления антивирусных баз как с сайтов производителя, так и с внутренних сетевых ресурсов организации;
* возможность фоновой проверки почтовых ящиков и общих папок с использованием Exchange Web Services;
* детальные отчеты в формате HTML;
* наличие возможности отправки отчётов и уведомлений на указанные адреса электронной почты;
* мониторинг работы программы с помощью System Center - Operations Manager;
* интеграция с Active Directory;
* централизованный просмотра состояния защиты;
* возможность распределять роли администраторов системы.

Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

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

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

проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к эксплуатационной документации

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

«Руководство пользователя (администратора)»

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

Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

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

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

* 1. **Технические требования на Acronis Защита Данных Расширенная**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Количество** |
| 1 | Сертификат на техническую поддержку Acronis Защита Данных Расширенная для физического сервера | 28 |
| 2 | Сертификат на техническую поддержку Acronis Защита Данных Расширенная для рабочей станции | 8 |

* + 1. **Требования к технической поддержке**

Подписка на техническую поддержку должна предоставлять следующие возможности:

4.1. Контакт со службой технической поддержки посредством телефона, электронной почты.

4.2. Техническая поддержка должна быть доступна на русском языке в рабочие часы, в будни.

4.3. Обозначение критичности проблемы при создании заявке в службе технической поддержке.

4.4. В критичных случаях при обращении в службу технической поддержки первая реакция инженера должна последовать в течение нескольких часов.

4.5. Подписка на техническую поддержку в период своего действия должна гарантировать бесплатные обновления продукта, в том числе переход на новую версию продукта.

5. ПО должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных.

* 1. **Технические требования к предоставлению неисключительных (пользовательских) прав на Программу для ЭВМ «Автоматизация формирования и актуализации внутренней документации учреждений и организаций (АльфаДок)» на срок 1 (один) год. Тариф КИИ.ПДн.Эксперт. Клиентская лицензия "КИИ.ПДн.Эксперт" на срок 1 (один) год**

Исполнитель должен обеспечить передачу неисключительного права на использование программы для ЭВМ «Автоматизация формирования и актуализации внутренней документации учреждений и организаций (Альфа-док)». Клиентская лицензия «КИИ.ПДн.Эксперт» на срок 1 (один) год (далее – Программа Автоматизации) в составе:

* Разработка организационно-распорядительной документации по категорированию объектов КИИ;
* Разработка организационно-распорядительной документации по обработке и защите ПДн, отправка уведомления и информационных писем в Роскомнадзор, генерация согласий на обработку ПДн;
* Разработка моделей угроз и действий нарушителя;
* Разработка документации по эксплуатации криптосредств;
* Ведение электронных журналов;
* Учет проверок регуляторов, информирование о плановых проверках Роскомнадзора;
* Планирование внутренних проверок режима защиты информации;
* Самооценка готовности к проверкам регуляторов Роскомнадзора, ФСБ России;
* Разработка технической документации по защите информации: технических паспортов на информационные системы, технических заданий на создание системы защиты информации, матрицы доступа;
* Анализ технической защищенности информационных систем;
* Формирование аналитических отчетов;
* Самооценка готовности к проверкам ФСТЭК России.

Информационная поддержка:

* консультации по вопросам обеспечения безопасности информации, а также по вопросам пользования Программой Автоматизации (online-консультант, e-mail, телефон);
* предоставление возможности участия в периодических бесплатных вебинарах по обеспечению безопасности информации, использованию и новым возможностям Программы Автоматизации (в течение срока действия лицензии)
  + 1. **Требования к Программе Автоматизации в целом.**

Программа Автоматизации должна быть включена в Единый реестр российских программ для электронных вычислительных машин и баз данных (<https://reestr.minsvyaz.ru/reestr/>).

Программа Автоматизации должна включать в себя следующие функциональные подсистемы:

* Подсистема внесения/изменения исходных данных;
* Подсистема пользовательских стилей документации;
* Подсистема генерации и выгрузки документации;
* Подсистема управления профилем пользователя;
* Подсистема информационной поддержки пользователя (консультирования);
* Подсистема планирования событий и постановки/контроля выполнения задач, получения уведомлений;
* Подсистема регистрации заявок на участие в вебинарах;
* Подсистема ведения журналов по информационной безопасности в электронном виде;
* Подсистема оценки готовности к проверкам Роскомнадзора;
* Подсистема оценки готовности к проверкам ФСБ России;
* Подсистема оценки готовности к проверкам ФСТЭК России;
* Подсистема получения информации о плановых проверках надзорных органов;
* Подсистема ведения перечня внутренних проверок;
* Подсистема автоматической подачи уведомления/информационного письма в Роскомнадзор;
* Подсистема быстрого доступа к формам документов в области информационной безопасности;
* Подсистема базы знаний;
* Подсистема оперативного мониторинга состояния защиты информации в организации по данным в Программе Автоматизации;
* Подсистема быстрой обработки «рабочих ситуаций»
* Подсистема автоматического формирования согласий на обработку ПДн, адаптированных под категории субъектов ПДн;
* Подсистема ведения реестра информационных систем;
* Подсистема формирования отчетности по данным организации;
* Подсистема категорирования объектов критической информационной инфраструктуры.

Доступ к подсистемам должен быть реализован в виде тематических рабочих столов с соответствующими ярлыками для перехода к какой-либо подсистеме. Перечень доступных пользователю рабочих столов:

* Избранное;
* Панель управления;
* Документы;
* Операционная деятельность;
* Рабочие ситуации;
* Органайзер;
* Обучение;
* Аналитика.

Программа Автоматизации должна обеспечивать централизованное хранение и обработку информации в СУБД.

В Программе Автоматизации должна быть реализована защита канала связи посредством протокола https (по умолчанию) и предусмотрена возможность защиты канала связи сертифицированными криптографическими средствами защиты информации с встроенными функциями межсетевого экранирования.

Программа Автоматизации должна поддерживать следующие режимы функционирования:

* Основной режим, в котором все функциональные подсистемы выполняют все свои основные функции;
* Профилактический режим, в котором одна или все подсистемы не выполняют своих функций.

В основном режиме функционирования Программа Автоматизации должна обеспечивать возможность работы пользователей с учетом их возможного нахождения в командировках (в других часовых поясах) в режиме 24 часа в сутки 7 дней в неделю (24х7).

В профилактическом режиме Программа Автоматизации должна обеспечивать возможность проведения следующих мероприятий:

* регламентное техническое обслуживание;
* модернизацию информационно-телекоммуникационной инфраструктуры;
* устранение аварийных ситуаций.

Общее время проведения профилактических работ не должно превышать 2% от общего времени работы Программы Автоматизации в основном режиме.

* + - 1. **Требования к обеспечению информационной безопасности**

В Программе Автоматизации должны быть выполнены требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, что должно быть подтверждено аттестатом соответствия Программы Автоматизации требованиям безопасности.

Исполнитель не должен разглашать и использовать конфиденциальную информацию, принадлежащую Заказчику, которая может стать ему известной в ходе Поставки. Исполнитель несет ответственность за соблюдение этого требования в соответствии с законодательством Российской Федерации.

* + - 1. **Требования к функциям, выполняемым Программой Автоматизации**
         1. **Подсистема внесения/изменения исходных данных**

Подсистема внесения/изменения исходных данных должна быть реализована в виде пошагового Мастера опроса с возможностью сохранения введенной информации на текущем шаге, перехода на следующий и предыдущий шаги.

Мастер опроса должен предполагать переход на следующий шаг только в том случае, если заполнены все обязательные поля предыдущего. При попытке перехода на недоступный шаг должен быть предусмотрен вывод сообщения о недостающей для перехода информации. Для перехода на произвольный доступный шаг должна быть предусмотрена навигация в виде списка шагов в Мастере опроса.

На каждом шаге должны быть предусмотрены краткие справочные комментарии, которые позволяют облегчить процесс ввода данных в Программу Автоматизации.

В Программе Автоматизации должны быть предусмотрены информационные справки, которые помогут пользователю внести правильную информацию в поля Мастера опроса.

Для вводимых параметров при необходимости должны быть предусмотрены:

* предварительное заполнение падежных форм;
* возможность выбора значений из справочников.

Должна быть предусмотрена возможность импорта перечня сотрудников и структурных подразделений из файлов \*.xls, \*.xlsx и \*.csv.

Подсистема должна обеспечивать сбор аналитических данных для формирования комплекта организационно-распорядительной документации по вопросам обеспечения безопасности информации, а также модели угроз безопасности информации (включая модель нарушителя).

Моделирование угроз безопасности должно реализовываться на основании опроса о реализованных мерах, об особенностях и условиях обработки информации.

* + - * 1. **Подсистема пользовательских стилей документации**

Должна быть предусмотрена возможность настройки стилей следующих типов документации:

* Приказ/распоряжение;
* Положение/политики/акты.

При настройке стилей всех типов документации должны быть доступны для редактирования следующие параметры:

* Шрифт (Times New Roman, Arial, Calibri, Courier New);
* Размер шрифта (11пт, 12пт, 13пт, 14пт);
* Междустрочный интервал (1, 1.15, 1.5);
* Верхнее поле;
* Нижнее поле;
* Левое поле;
* Правое поле.

Для документации типа Приказ/распоряжение должны быть доступны для редактирования следующие параметры:

* Шапка документа;
* Написание названия документа (Распоряжение, приказ или постановление, выравнивание, стиль шрифта);
* Написание номера, даты документа и населённого пункта (с возможностью выбора расположения и выравнивания);
* Написание слова «приказываю»
* Параметры списков в документе;
* Параметры блока подписи и согласования документа;
* Параметры названия приложений;
* Параметры списков в приложении;
* Параметры нумерации разделов приложений;
* Параметры маркированных списков;
* Параметры названий таблиц в приложениях;
* Параметры нумерации строк в таблицах.

Для документации типа Положение/политики/акты должны быть доступны для редактирования следующие параметры:

* Написание названия документа (стиль шрифта);
* Параметры блока утверждения документа;
* Параметры заголовков документов;
* Параметры нумерации разделов;
* Параметры маркированных списков;
* Параметры названий таблиц в приложениях;
* Параметры нумерации строк в таблицах.

В данной подсистеме должно быть предусмотрено отображение типового документа для просмотра и изменения настроек документа.

* + - * 1. **Подсистема генерации и выгрузки документации**

На момент предоставления неисключительных (пользовательских) прав на Программу Автоматизации портфель документов, генерируемых Программой Автоматизации, должен иметь следующий состав:

* Приказ/распоряжение о комиссии по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных;
* Приказ/распоряжение об ответственном за организацию обработки персональных данных;
* Приказ/распоряжение об ответственном за обеспечение безопасности персональных данных в информационных системах персональных данных;
* Приказ/распоряжение об утверждении перечня информационных систем персональных данных и перечня персональных данных, содержащихся в программных комплексах, входящих в состав информационных систем персональных данных;
* Приказ/распоряжение об утверждении перечня персональных данных;
* Приказ/распоряжение об утверждении перечней сотрудников, осуществляющих обработку персональных данных и имеющих доступ к обрабатываемым персональным данным;
* Приказ/распоряжение о сотрудниках, которым разрешены действия по внесению изменений в базовую конфигурацию информационных систем и системы защиты персональных данных (в случае, если установленный уровень защищенности ПДн при их обработке в ИС имеет значение 1, 2 или 3);
* Приказ/распоряжение о сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них (в случае, если установленный уровень защищенности ПДн при их обработке в ИС имеет значение 1 или 2);
* Приказ/распоряжение о сотрудниках, имеющих доступ к содержанию электронного журнала сообщений (в случае, если установленный уровень защищенности ПДн при их обработке в ИС имеет значение 1 или 2);
* Приказ/распоряжение об обеспечении безопасности материальных носителей персональных данных;
* Приказ/распоряжение об обеспечении безопасности помещений, в которых размещены информационные системы персональных данных и сохранности носителей персональных данных;
* Приказ/распоряжение об утверждении форм документов, необходимых в целях выполнения требований законодательства в области персональных данных;
* Приказ/распоряжение об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты;
* Приказ/распоряжение об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации при ведении журнала, содержащего персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию организации (в случае наличия пропускного режима);
* Приказ/распоряжение о системе разграничения доступа в информационных системах персональных данных;
* Приказ/распоряжение о комиссии по уничтожению ПД;
* Политика в отношении обработки персональных данных;
* Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
* Порядок хранения, использования и передачи персональных данных сотрудников;
* Акт определения уровня защищенности персональных данных в информационных системах;
* Модель угроз безопасности персональных данных в информационных системах персональных данных (на каждую информационную систему);
* Рекомендации по внесению изменений в Должностные инструкции персонала в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
* Рекомендации по выполнению требований по обеспечению безопасности персональных данных в информационных системах персональных данных;
* Технический паспорт (на каждую информационную систему);
* Техническое задание;
* Памятка по работе с пакетом документов (в Библиотеке уникальных документов);
* План мероприятий по реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и принятых в соответствии с ним нормативных правовых актов;
* Распоряжение об утверждении Положения о комиссии по категорированию объектов критической информационной инфраструктуры;
* Распоряжение об утверждении комиссии по категорированию объектов критической информационной инфраструктуры;
* Распоряжение об утверждении перечня объектов критической информационной инфраструктуры, подлежащих категорированию (в том числе форма отправки сведений во ФСТЭК России);
* Акт категорирования объекта критической информационной инфраструктуры (на каждый объект);
* Модель угроз безопасности информации в автоматизированной системе управления (на каждую АСУ);
* Сопроводительное письмо в ФСТЭК с перечнем объектов критической информационной инфраструктуры, подлежащих категорированию;
* Форма утверждения перечня объектов критической информационной инфраструктуры с ФСТЭК;
* Сопроводительное письмо в ФСТЭК с результатами категорирования объектов критической информационной инфраструктуры;
* Форма о результатах присвоения объекту критической информационной инфраструктуры категории значимости (на каждый объект).

Наименования отдельных документов могут быть изменены по согласованию с Заказчиком.

Должна быть предусмотрена возможность сохранения утвержденных версий документа.

Должна быть предусмотрена возможность подписания утвержденной версии документа (в формате \*.docx) с помощью электронной подписи, встраиваемой в тело документа, с применением алгоритма ГОСТ Р 34.10-2012 (Национальный стандарт Российской Федерации ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 215-ст)).

Должно быть предусмотрено отображение общей информации о портфеле документов, включая наименования документов и их статусов.

Должны быть предусмотрены следующие статусы документов:

* Сформирован;
* Выгружен;
* Утвержден;
* Изменения в данных;
* Изменения в оформлении;
* Изменения в шаблоне;
* Не заполнены данные.

Должна быть предусмотрена возможность предварительного просмотра сформированных документов.

Должна быть предусмотрена выгрузка актуальных версий документов, как конкретного документа (в формате \*.docx, \*.pdf ), так и всех документов одним архивом (в формате \*.zip).

Должно быть предусмотрено автоматическое изменение состава пакета документов в ходе эксплуатации Программы Автоматизации в целях приведения в соответствие с новыми требованиями законодательства Российской Федерации с сохранением утвержденных версий документов. Состав портфеля документов должен учитывать условия обработки защищаемой информации.

Должна быть предусмотрена возможность пользования библиотекой уникальных документов (не генерируемых автоматически), с возможностью самостоятельной загрузки документов пользователем. Должна быть обеспечена возможность скачать и просмотреть документы, а для документов, загруженных пользователем – и удаления документов. Должна отображаться следующая информация о документах:

* Наименование;
* Описание;
* Состояние;
* Источник.

Подсистема должна обеспечивать генерацию комплекта организационно-распорядительной документации и моделей угроз безопасности информации (включая модели нарушителя) на основании собранных ранее аналитических данных. Моделирование угроз безопасности должно реализовываться на основании опроса экспертов о реализованных мерах, об особенностях и условиях обработки информации. Генерация моделей угроз (включая модели нарушителя) должна быть выполнена в строгом соответствии с методическими документами ФСТЭК России и ФСБ России в области определения актуальных угроз безопасности информации.

* + - * 1. **Подсистема управления профилем пользователя**

Должна быть предусмотрена возможность управления следующими параметрами профиля пользователя:

* Фамилия, Имя, Отчество пользователя;
* Фотография (графическое изображение);
* Должность;
* Номер телефона;
* Часовой пояс;
* Местоположение;
* Подписка на информационные рассылки.

Должна отображаться следующая информация:

* Логин;
* Адрес электронной почты;
* Наименование организации;
* Тариф;
* Срок действия тарифа.

Должна быть предусмотрены следующие возможности управления профилем:

* Смена адреса электронной почты;
* Смена пароля;
* Смена ФИО.

Подсистема информационной поддержки пользователя (консультирования)

Должны быть предусмотрены следующие возможности информационной поддержки пользователя:

* онлайн-консультант (Онлайн-консультант должен обеспечивать ведения нескольких диалогов пользователя со службой поддержки. Каждый диалог должен определяться темой и типом вопроса);
* заказ звонка (Заявка на звонок должна содержать Фамилию, Имя, Отчество, город, номер телефона, удобное время для звонка, тему звонка);
* задать вопрос (должен содержать Фамилию, Имя, Отчество, город, адрес электронной почты для ответа и текст сообщения).

Для зарегистрированных пользователей должно быть доступно описание работы с Программой Автоматизации, а также ответы на часто задаваемые вопросы.

* + - * 1. **Подсистема планирования событий и постановки/контроля выполнения задач, получения уведомлений**

В Программе Автоматизации должна быть предусмотрена возможность внесения информации о предстоящих событиях, как произвольных, запланированных самим пользователем, так и событий, генерируемых Программой Автоматизации.

Запланированные события должны отображаться на всех «рабочих столах» пользователя в календаре, а также списком, который состоит из ближайших событий. Дополнительно, должна быть предусмотрена возможность перехода в расширенный календарь с режимами отображения год, месяц, неделя, день. Должна быть обеспечена возможность фильтрации событий по их категории, а также получения уведомлений/напоминаний о событии в Программе Автоматизации.

При создании события заполняется следующая информация:

* Название;
* Место;
* Начало;
* Окончание;
* Повтор;
* Напоминание;
* Календарь;
* Отметка о важности события;
* Заметки.

В Программе Автоматизации должна быть предусмотрена возможность создания задач, изменения статусов задач и закрытия/удаления задач, как произвольных, запланированных самим пользователем, так и задач, генерируемых Программой Автоматизации. Пользователь должен иметь возможность получать уведомления в системе о новых задачах и напоминания о сроке задач.

При создании задачи заполняется следующая информация:

* Тема;
* Текст задачи;
* Дата исполнения;
* Напоминание;
* Комментарий;
* Исполнитель.

Возможные статусы задач:

* Новый;
* В работе;
* Решено;
* Закрыт.
  + - * 1. **Подсистема регистрации заявок на участие в вебинарах**

В Программе Автоматизации должна быть предусмотрена возможность просмотра перечня периодических бесплатных вебинаров по обеспечению безопасности информации, использованию и новым возможностям Программы Автоматизации (в течение срока действия лицензии), с указанием наименования вебинара, даты и времени его проведения, а также целевой аудитории.

Для каждого вебинара должна быть доступна кнопка отправки заявки на участие в вебинаре, по нажатию на которую пользователю должна предоставляться для заполнения форма заявки.

* + - * 1. **Подсистема ведения журналов по информационной безопасности в электронном виде**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому для пользователя доступен перечень журналов для ведения в электронном виде. Должна быть предусмотрена возможность добавления записей в журнал и выгрузки печатной формы журнала по нажатию на кнопку «Выгрузка».

Для каждой записи в журнале должны фиксироваться дата последнего изменения записи и логин пользователя, который произвел эти изменения.

Перечень журналов, доступных для тарифа:

* Журнал поэкземплярного учета средств защиты информации;
* Журнал поэкзмеплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов;
* Журнал учета обращений субъектов персональных данных;
* Лицевой счет пользователя криптосредств;
* Журнал учета хранилищ (сейфов);
* Журнал учета нештатных ситуаций информационных систем персональных данных, выполнения профилактических работ, установки и модификации программных средств на ПЭВМ;
* Журнал учета отчуждаемых машинных носителей персональных данных;
* Журнал проверок электронных журналов;
* Журнал учета передачи персональных данных;
* Журнал периодического тестирования средств защиты информации.
* Журнал обучения пользователей правилам работы с криптосредствами.
  + - * 1. **Подсистема оценки готовности к проверкам Роскомнадзора**

В Программе Автоматизации на рабочем столе «Аналитика» должен быть предусмотрен ярлык, при переходе по которому пользователю доступна возможность оценки готовности к проверке Роскомнадзора. Оценка готовности состоит из списка необходимых пунктов, которые необходимо выполнить для того, чтобы подготовиться к проверке. При этом часть пунктов проставляется пользователем вручную, часть пунктов проставляется автоматически Программой Автоматизации.

Для пользователя должна быть доступна возможность отметить выполненными пункты, которые доступны для отметки вручную. По результатам отметки пунктов подсчитывается общий процент готовности к проверке, а также пользователю доступен список рекомендаций для прохождения проверки.

* + - * 1. **Подсистема оценки готовности к проверкам ФСБ России**

В Программе Автоматизации на рабочем столе «Аналитика» должен быть предусмотрен ярлык, при переходе по которому пользователю доступна возможность оценки готовности к проверке ФСБ России. Оценка готовности состоит из списка необходимых пунктов, которые необходимо выполнить для того, чтобы подготовиться к проверке. При этом часть пунктов проставляется пользователем вручную, часть пунктов проставляется автоматически Программой Автоматизации.

Для пользователя должна быть доступна возможность отметить выполненными пункты, которые доступны для отметки вручную. По результатам отметки пунктов подсчитывается общий процент готовности к проверке, а также пользователю доступен список рекомендаций для прохождения проверки.

* + - * 1. **Подсистема оценки готовности к проверкам ФСТЭК России**

В Программе Автоматизации на рабочем столе «Аналитика» должен быть предусмотрен ярлык, при переходе по которому пользователю доступна возможность оценки готовности к проверке ФСТЭК России. Оценка готовности состоит из списка необходимых пунктов, которые необходимо выполнить для того, чтобы подготовиться к проверке. При этом часть пунктов проставляется пользователем вручную, часть пунктов проставляется автоматически Программой Автоматизации.

Для пользователя должна быть доступна возможность отметить выполненными пункты, которые доступны для отметки вручную. По результатам отметки пунктов подсчитывается общий процент готовности к проверке, а также пользователю доступен список рекомендаций для прохождения проверки.

* + - * 1. **Подсистема получения информации о плановых проверках надзорных органов**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому пользователю доступна информация о плановых проверках надзорных органов. Пользователь должен иметь возможность добавить внеплановую проверку вручную, а также отмечать пройденной проверку из списка проверок с возможностью прикрепить результат прохождения проверки в виде файла.

При создании проверки пользователь может заполнить следующие поля:

* Дата проверки;
* Срок проведения проверки;
* Орган контроля;
* Цель;
* Наименование проверяемого подразделения, филиала;
* Причина проверки;
* Замечания по результатам проверки;
* Срок устранения замечания;
* Штрафы;
* Отметка о прохождении проверки;
* Комментарий;
* Наименование документа по результатам проверки.
  + - * 1. **Подсистема ведения перечня внутренних проверок**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому пользователю доступно управление внутренними проверками в организации. Также здесь должна быть возможность отметить проверку выполненной и ввести дополнительную информацию о проверке.

Добавление или изменение перечня внутренних проверок в организации должно быть доступно в Мастере опросов на отдельном шаге. По умолчанию Программой Автоматизации должен быть введен список рекомендуемых проверок с возможностью изменения. При добавлении проверки должна быть обеспечена возможность выбора наименования проверки из справочника или ввода наименования проверки вручную. Перечень проверок, введенный на шаге, должен отображаться в соответствующем документе в Портфеле документов.

* + - * 1. **Подсистема автоматической подачи уведомления/информационного письма в Роскомнадзор**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому пользователь имеет возможность автоматической отправки уведомления/информационного письма в Роскомнадзор. Должна быть возможность проверки статуса поданного уведомления/информационного письма в Программе Автоматизации, а также возможность просмотра поданного уведомления/информационного письма по переходу на сайт Роскомнадзора.

* + - * 1. **Подсистема быстрого доступа к формам документов в области информационной безопасности**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому пользователю доступен перечень форм, которые необходимо подписать сотрудникам организации, а также перечень дополнительных форм, которые необходимо подписать сотрудникам в случае появления соответствующих прецедентов. Должна быть возможность скачивания указанных форм (в формате \*.docx, \*.pdf) и их просмотра.

Список форм, доступных пользователю:

* Разъяснение субъекту персональных данных (работнику) юридических последствий отказа предоставить свои персональные данные;
* Типовая форма согласия субъекта персональных данных на обработку персональных данных;
* Форма согласия субъекта персональных данных на поручение обработки персональных данных третьему лицу;
* Обязательство о соблюдении конфиденциальности персональных данных;
* Уведомление о факте обработки персональных данных без использования средств автоматизации;
* Форма ознакомления с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных.

Список дополнительных форм, доступных пользователю:

* Акт на списание и уничтожение машинных (бумажных) носителей информации;
* Уведомление о получении персональных данных от третьих лиц;
* Уведомление об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке персональных данных.
  + - * 1. **Подсистема базы знаний**

В Программе Автоматизации для пользователя должен быть доступен раздел База знаний, в котором содержится расширенная информация о Программе Автоматизации. Должна быть предусмотрена возможность просмотра содержащейся информации, а также навигации по разделам Базы знаний.

* + - * 1. **Подсистема оперативного мониторинга состояния защиты информации в организации по данным в Программе Автоматизации**

В Программе Автоматизации должен быть предусмотрен отдельный рабочий стол «Панель управления», который отображает текущий статус процесса организации информационной безопасности в организации, исходя из введенных данных, в виде отдельных тематических виджетов. Из каждого виджета должна быть предусмотрена возможность перехода к соответствующей подсистеме в Программе Автоматизации.

На рабочем столе «Панель управления» на момент поставки доступны следующие виджеты:

* Заполнение данных;
* Документы;
* Проверки регуляторов;
* Внутренние проверки;
* Список задач;
* Защищенность информационных систем.

Виджеты «Документы» и «Проверки регуляторов» должны иметь возможность индивидуальной настройки виджетов.

Запланированные и прошедшие события должны быть отображены в виде таймлайна с возможность масштабирования. Из таймлайна должна быть предусмотрена возможность перехода к календарю событий организации в Программе Автоматизации.

Количественное отображение введенных данных должно быть показано в виде статистики по имеющимся ресурсам организации в отдельном блоке «Ресурсы».

Для отслеживания вносимых изменений пользователями в систему и происходящих событий в системе должен быть доступен «Журнал событий». Просмотр событий в Журнале должен быть возможен отдельно по событиям пользователей и по событиям системы.

* + - * 1. **Подсистема быстрой обработки «рабочих ситуаций».**

В Программе Автоматизации должен быть предусмотрен тематический рабочий стол «Рабочие ситуации», который содержит перечень доступных для пользователя ярлыков, разделенных по тематическим блокам: «Сотрудники», «Оборудование и ПО» и «СЗИ».

На рабочем столе «Рабочие ситуации» на момент поставки доступны следующие «рабочие ситуации»:

* Приём нового сотрудника;
* Назначение ответственных;
* Доступ сотрудников;
* Добавление программного комплекса;
* Добавление АРМ/сервера;
* Добавление сетевого оборудования;
* Установка СЗИ.

Каждая «рабочая ситуация» должна представлять из себя опросник, по результатам которого пользователь должен получить список рекомендаций и сформированных документов с возможностью скачивания.

Должна быть предусмотрена возможность перехода к незавершенной «рабочей ситуации», а также просмотра результатов завершенной «рабочей ситуации».

* + - * 1. **Подсистема автоматического формирования согласий на обработку ПДн, адаптированных под категории субъектов ПДн**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому пользователь имеет возможность сформировать согласия на обработку ПДн, поручение обработки ПДн, передачу ПДн, согласие на включение ПДн в общедоступные источники для каждой категории субъектов ПДн, по которым Организация обрабатывает ПДн, а также для их законных представителей. Согласия должны формироваться на основе данных, введенных пользователем в Мастере опроса, а также в Программе Автоматизации.

Должны быть предусмотрены следующие статусы согласий:

* Сформировано;
* Выгружено;
* Изменения в данных;
* Изменения в оформлении;
* Не создано;
* Не заполнены данные;
* Не требуется.

Должна быть предусмотрена возможность предварительного просмотра сформированных согласий.

Должна быть предусмотрена выгрузка сформированных согласий в формате \*.docx, \*.pdf.

* + - * 1. **Подсистема ведения реестра информационных систем**

В Программе Автоматизации на рабочем столе «Аналитика» должен быть предусмотрен ярлык, при переходе по которому пользователю доступен перечень ИСПДн организации, содержащий общую информацию об ИСПДн, сведения об аттестации, количество актуальных угроз и процент технической защищенности, а также состояние защищенности каждой ИСПДн требуемыми средствами защиты информации.

Для каждой информационной системы из реестра ИСПДн должен быть возможен переход в Карточку ИСПДн, в которой пользователю доступны следующие блоки:

* характеристики ИСПДн;
* состав ИСПДн;
* состояние защищенности АРМ/серверов требуемыми средствами защиты информации;
* угрозы безопасности информации.

Пользователю должны быть доступны возможности просмотра рекомендаций по устранению актуальных угроз и проставления отметок о выполнении необходимых мер по закрытию угрозы. Проставление мер в Программе автоматизации должно выполняться синхронно с Мастером опроса.

Для каждой ИСПДн на основе состояния защищенности ИСПДн требуемыми средствами защиты информации и количества актуальных угроз в ИСПДн должен быть определен процент технической защищенности ИСПДн.

Должна быть возможность скачивания карточки ИСПДн (в формате \*.docx).

* + - * 1. **Подсистема формирования отчетности по данным организации**
* В Программе Автоматизации на рабочем столе «Аналитика» должен быть предусмотрен ярлык, при переходе по которому пользователь имеет возможность ознакомится со сводной информацией по ресурсам организации и сформировать аналитические отчеты. Отчеты должны формироваться на основе данных, введенных пользователем в Мастере опроса, а также в Программе Автоматизации.

На рабочем столе «Отчёты» на момент поставки доступны следующие отчёты:

* Эксплуатируемые информационные системы;
* Используемые СЗИ;
* Сотрудники.

Каждый отчет должен иметь возможность настройки по выбранным параметрам.

Должна быть предусмотрена выгрузка сформированных отчетов в формате \*.docx, \*.pdf.

* + - * 1. **Подсистема категорирования объектов критической информационной инфраструктуры**

В Программе Автоматизации имеется возможность обозначения уже имеющихся информационных систем как объектов критической информационной инфраструктуры и ввода информации о новых объектах (в том числе – автоматизированных систем управления). Для категорирования предусмотрена возможность назначения комиссии. Категория значимости объекта критической информационной инфраструктуры высчитывается автоматически по введенным данным.

По введенным и вычисленным автоматически данным формируется пакет документов по категорированию объектов критической информационной инфраструктуры.

1. **Требования по обеспечению режима конфиденциальности при оказании услуг**

В период оказания услуг и после их окончания Исполнитель не должен разглашать и использовать конфиденциальную информацию, принадлежащую Заказчику, перечень которой определен внутренним распорядительным документом Заказчика, которая может стать ему известной в ходе оказания услуг. Исполнитель несет ответственность за соблюдение этого требования в соответствии с Законодательством Российской Федерации.

**СПЕЦИФИКАЦИЯ**

­­­­­­­­­­­­­­­­­­­­­­­­­­

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| п/п | Наименование | Страна происхождения, товарный знак (при наличии) | Количество, шт. | Цена, р. | Сумма с НДС, р |
| 1 |  |  |  |  |  |
|  | **ИТОГО** | | | |  |

Приложение № 2 к Договору

№ \_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_2020 г.

**Техническое задание**

**на продление лицензий и приобретение технической поддержки программных средств защиты информации**

1. **Требования к Исполнителю**

Исполнитель должен иметь действующую лицензию ФСБ России на осуществление деятельности, связанной с криптографическими (шифровальными) средствами; действие лицензии должно распространяться на работы (услуги), согласно пунктам 12, 20, 21 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося Приложением к постановлению Правительства РФ № 313 от 16.04.2012 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», либо наличие лицензии ФСБ России на осуществление распространения шифровальных (криптографических) средств и на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств.

**Исполнитель должен иметь официальное представительство или офис на территории города Уфы Республики Башкортостан. Исполнитель должен являться авторизованным/сертифицированным партнером производителей с наличием сертифицированных специалистов технической поддержки (подтверждается копией трудового договора либо копией трудовой книжки, либо иным аналогичным документом, а также соответствующими действующими сертификатами.**

1. **Требования к качеству и безопасности услуг**

Качество услуг должно соответствовать санитарно-эпидемиологическим нормам, а также иным требованиям качества, безопасности жизни и здоровья, требованиям сертификации, безопасности (государственным стандартам и т.п.), лицензирования, если такие требования предъявляются действующим законодательством Российской Федерации или производителем.

1. **Требования к гарантийному сроку**

Гарантийный срок оказанной услуги должен быть не менее 12 (двенадцати) месяцев с даты подписания акта оказанных услуг.

Гарантийный срок распространяется на произведенные работы.

В случае некачественного оказания услуг Исполнитель в течение гарантийного срока обязуется устранить возникшие неполадки за свой счет и обеспечить качественное оказание услуг.

В цену Договора, включаются расходы по оплате всех необходимых налогов, пошлин и сборов.

1. **Технические требования на оказание услуг по развитию и поддержке системы защиты информации** 
   1. **Сертификат активации сервиса совместной технической поддержки ПО ViPNet для сети № 1960 на срок 1 год, уровень – Расширенный**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Количество** |
| 1 | ПО ViPNet Administrator 4.х ( КС2) | 1 |
| 2 | ПАК ViPNet Coordinator HW 1000 | 1 |
| 3 | ПО ViPNet Client 4.х (КС2) | 350 |

Общие требования:

Наличие у Исполнителя сертифицированного специалиста по администрированию программного обеспечения ViPNet Custom в г. Уфа (подтверждается трудовым договором и соответствующими сертификатами).

Наличие у Исполнителя действующей лицензии ФСБ России на осуществление деятельности, связанной с криптографическими (шифровальными) средствами; действие лицензии должно распространяться на работы (услуги), согласно пунктам 12, 20, 21 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося Приложением к постановлению Правительства РФ № 313 от 16.04.2012 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», либо наличие лицензии ФСБ России на осуществление распространения шифровальных (криптографических) средств и на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств.

Перечень предоставляемых услуг:

* Консультации по работе ПО ViPNet по электронной почте, по телефону «Горячей линии», с выездом к Заказчику
  + Прием сообщений должен вестись с учетом режима рабочего времени.
  + Приём обращений и консультирование по электронной почте с 9:00 до 18:00;
  + Приём обращений и консультирование по телефону горячей линии с 9:00 до 18:00
* Консультирование при установке программного обеспечения ViPNet, включающее:
  + Рекомендации по процессу установки продукта в объеме эксплуатационной документации;
  + Ответы на вопросы, возникающие при установке
* Консультирование при эксплуатации должно включать в себя:
  + Рекомендации по настройке продукта в объеме эксплуатационной документации;
  + Ответы на вопросы, возникающие в процессе эксплуатации;
  + Расшифровка кодов ошибок;
  + Рекомендации по «тонкой» настройке продукта с учетом особенностей системы Заказчика;
* Обновление программного обеспечения ViPNet при выходе новых версий:
  + Должны быть предоставлены обновления (hotfix), а также все изменения, производимые в рамках минорной (MINOR) версии программного обеспечения ViPNet (service pack) без взимания дополнительной платы
  + Должны быть предоставлены новые версии (изменение мажорной (MAJOR) версии, поколения) программного обеспечения ViPNet без взимания дополнительной платы
  + Новые версии должны передаваться посредством пересылки экземпляров программного обеспечения ViPNet на CD-дисках
* Исправление ошибок и предоставление релизов с исправлениями в рамках версии:
* Должны быть предоставлены обновления (hotfix), устраняющее дефекты, выявленные в продукте.
* Восстановление работоспособности (ремонт) вышедшего из строя оборудования (аппаратной платформы ПАК) из состава Продуктов Заказчика в соответствии с гарантийными обязательствами ОАО «ИнфоТеКС»
* Проведение не реже одного раза в месяц мониторинга состояния эксплуатации сети ViPNet с оформлением технического отчета. В отчете указываются выводы по соответствию технических конфигураций АРМ, использующих ПО ViPNet, положениям эксплуатационной документации и формуляра на ПО ViPNet.
* Проведение работ по плановой смене ключевой информации и в случае их компрометации.
* Выявление и устранение проблем, возникающих у пользователей при эксплуатации продуктов и выявленных в ходе ежемесячного мониторинга (используя электронную почту, «горячую» телефонную линию, выезды к заказчику).
* Разработка рекомендаций:
* для обеспечения деятельности информационных служб Заказчика, связанных с эксплуатацией ПО ViPNet,
* для реализации функций удостоверяющего центра корпоративного уровня класса КС2,
* по организации межсетевого взаимодействия сетей ViPNet,
* по организации сегментирования и туннелирования в защищенной сети ViPNet,
* по совместной эксплуатации ПО ViPNet с другими СЗИ (Dallas Lock, КриптоПРО, Континент АП).
  1. **Технические требования Антивирусного средства Kaspersky Endpoint Security для бизнеса – Расширенный и защиты почтовых серверов**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Количество** |
| 1 | Программное обеспечение Kaspersky Endpoint security для бизнеса - Расширенный для защиты рабочих станций и файловых серверов, лицензия на 1 год, продление | 330 |
| 2 | Программное обеспечение Kaspersky Security для почтовых серверов, лицензия на 1 год, продление | 230 |

Общие требования

Антивирусные средства должны включать:

• Программные средства антивирусной защиты для рабочих станций Windows.

• Программные средства антивирусной защиты для рабочих станций Linux.

• Программные средства антивирусной защиты для файловых серверов Windows.

• Программные средства антивирусной защиты для файловых серверов Linux.

• Программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов).

• Программные средства централизованного управления, мониторинга и обновления.

• Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange.

• Обновляемые базы данных сигнатур вредоносных программ и атак.

• Эксплуатационную документацию на русском языке.

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

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

Требования к программным средствам антивирусной защиты для рабочих станций Windows

* Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий:
* Windows 7 Home / Professional / Enterprise (32 / 64-разрядная);
* Windows 8 Professional / Enterprise (32 / 64-разрядная);
* Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
* Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядная).
* В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:
* антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
* фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
* проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
* блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
* распознавания и блокировку фишинговых и небезопасных сайтов;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
* возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
* контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
* возможность управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
* записи в журнал событий о записи и/или удалении файлов на съемных дисках;
* контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
* защиты от атак типа BadUSB;
* запуск специальной задачи для обнаружения закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
* защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
* установки только выбранных компонентов программного средства антивирусной защиты;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* запуск задач по расписанию и/или сразу после запуска приложения;
* гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* возможность проверки целостности антивирусной программы;
* возможность добавления исключений из антивирусной проверки по контрольной сумме файла, маске имени/директории или по наличию у файла доверенной цифровой подписи;
* наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
* наличие защищенного хранилища для отчетов о работе антивируса;
* возможность включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
* возможность интеграции с Windows Defender Security Center;
* наличие поддержки Antimalware Scan Interface (AMSI);
* наличие поддержки Windows Subsystem for Linux (WSL);
* возможность защитить паролем восстановление объектов из резервного хранилища.
* полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем;
* восстановления зашифрованного содержимого в случае сбоев загрузочного агента или 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);

Требования к программным средствам антивирусной защиты для рабочих станций Linux:

* Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 32-битных операционных систем следующих версий:
* Ubuntu 16.04 LTS и выше;
* Red Hat® Enterprise Linux® 6.7 и выше;
* CentOS 6.7 и выше;
* Debian GNU / Linux 9.4 и выше;
* Debian GNU / Linux 10;
* Linux Mint 18.2 и выше;
* Linux Mint 19 и выше;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.3 Рабочая станция;
* Альт Линукс 8.3 Рабочая станция К;
* Альт Линукс 8.3 Сервер;
* Альт Линукс 8.3 Образование;
* Альт Линукс 9 Рабочая станция;
* Альт Линукс 9 Образование;
* Гослинукс 6.6;
* Mageia 4.
* Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 64-битных операционных систем следующих версий:
* Ubuntu 16.04 LTS и выше;
* Ubuntu 18.04 LTS и выше;
* Red Hat Enterprise Linux 6.7 и выше;
* Red Hat Enterprise Linux 7.2 и выше;
* Red Hat Enterprise Linux 8.0 и выше;
* CentOS 6.7 и выше;
* CentOS 7.2 и выше;
* CentOS 8.0 и выше;
* Debian GNU / Linux 9.4 и выше;
* Debian GNU / Linux 10.1 и выше;
* OracleLinux 7.3 и выше;
* OracleLinux 8 и выше;
* SUSE® Linux Enterprise Server 15 и выше;
* openSUSE® Leap 15 и выше;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.3 Рабочая станция;
* Альт Линукс 8.3 Рабочая станция К;
* Альт Линукс 8.3 Сервер;
* Альт Линукс 8.3 Образование;
* Альт Линукс 9 Рабочая станция;
* Альт Линукс 9 Сервер;
* Альт Линукс 9 Образование;
* Amazon Linux AMI;
* Linux Mint 18.2 и выше;
* Linux Mint 19 и выше;
* Astra Linux Special Edition 1.5 (обычный режим и режим замкнутой программной среды);
* Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды);
* Astra Linux Common Edition «Орел» 2.12;
* ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем;
* ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем;
* Гослинукс 6.6;
* Гослинукс 7.2;
* AlterOS 7.5 и выше;
* Pardus OS 19.1.
* В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:
* резидентного антивирусного мониторинга;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* проверку ресурсов доступных по SMB / NFS;
* возможность проверки памяти ядра;
* эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
* проверку сообщений электронной почты в текстовом формате (Plain text);
* наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
* защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
* возможность включения опции блокирования файлов во время проверки;
* помещение подозрительных и поврежденных объектов на карантин;
* проверку почтовых баз приложений Microsoft Outlook на наличие вредоносных объектов;
* возможность перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
* возможность управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли.
* возможность управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения
* возможность проверки съемных дисков
* возможность отслеживания во входящем сетевом трафике активности, характерной для сетевых атак
* возможность проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым

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

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

32-разрядных операционных систем Microsoft Windows

* Windows Server® 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Windows Server 2008 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше.

64-разрядных операционных систем Microsoft Windows

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

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

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

**Требования к программным средствам антивирусной защиты мобильных устройств:**

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

* Android 4.2-10.0.
* iOS 10.0-13.0.
* iPadOS.

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

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

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

* возможность удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;
* возможность отправки команды блокирования и удаления данных;
* возможность создавать групповые политики безопасности мобильных устройств;
* удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM;
* получать отчеты и статистику о работе мобильных устройств пользователей;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervised mode;
* возможность централизованного управления с помощью единой консоли управления.

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

* Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
* Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Pro для рабочих станций 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 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 2019 Standard 64-разрядная;
* Windows Server 2019 Standard 64-разрядная;
* Microsoft Windows Server 2019 Datacenter 64-разрядная;
* Microsoft Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-разрядная;
* Microsoft Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-разрядная;
* Microsoft Windows Server 2016 (вариант установки Server Core RS3 (v1709) (LTSB/CBB) 64-разрядная;
* Microsoft Windows Server 2016 Standard (LTSB) 64-разрядная;
* Microsoft Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
* Microsoft Windows Server 2016 Datacenter (LTSB) 64-разрядная;
* Microsoft Windows Server 2012 R2 Standard 64-разрядная;
* Microsoft Windows Server 2012 R2 Server Core 64-разрядная;
* Microsoft Windows Server 2012 R2 Foundation 64-разрядная;
* Microsoft Windows Server 2012 R2 Essentials 64-разрядная;
* Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;
* Microsoft Windows Server 2012 Standard 64-разрядная;
* Microsoft Windows Server 2012 Server Core 64-разрядная;
* Microsoft Windows Server 2012 Foundation 64-разрядная;
* Microsoft Windows Server 2012 Essentials 64-разрядная;
* Microsoft Windows Server 2012 Datacenter 64-разрядная;
* Microsoft Windows Storage Server 2016 64-разрядная;
* Microsoft Windows Storage Server 2012 R2 64-разрядная;
* Microsoft Windows Storage Server 2012 64-разрядная;
* Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:
* VMware vSphere 6.5;
* Vmware vSphere 6.7;
* Vmware Workstation 15 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;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x;
* Parallels Desktop 14;
* Oracle VM VirtualBox 6.x.
* Программные средства централизованного управления, мониторинга и обновления должны 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;
* Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная;
* MySQL Standard Edition 5.7 32-разрядная / 64-разрядная;
* MySQL Enterprise Edition 5.7 32-разрядная / 64-разрядная;
* Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;
* MariaDB Server 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB.
* В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:
* выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
* возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
* возможность настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в 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;
* возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего Ipv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
* возможность иерархии триггеров, по которым происходит перераспределение;
* тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* инвентаризация установленного ПО и оборудования на компьютерах пользователей;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* функция управления мобильными устройствами через сервер Exchange ActiveSync;
* функция управления мобильными устройствами через сервер iOS MDM;
* возможность отправки SMS-оповещений о заданных событиях;
* централизованная установка сертификатов на управляемые мобильные устройства;
* возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
* возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
* построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* поддержка Windows Failover Clustering;
* поддержка интеграции с Windows сервисом Certificate Authority;
* наличие веб-консоли управления приложением;
* наличие портала самообслуживания пользователей;
* портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
* наличие системы контроля возникновения вирусных эпидемий;
* возможность установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
* возможность интеграции по OpenAPI;
* возможность управления антивирусной защитой с использованием WEB консоли.
* автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
* наличие преднастроенных ролей пользователей средств централизованного управления;
* должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей;
* возможность подключения по RDP или штатными средствами из консоли управления;
* пользователю должен выводиться запрос на разрешение дистанционного подключения;
* наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на «голое железо» (bare metal);
* должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;
* возможность запускать скрипты или 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 или 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 или CEF\ LEEF.

**Требования к программным средствам антивирусной защиты и фильтрации спама для серверов Microsoft Exchange:**

* Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
* Microsoft Windows Server 2019 Standard или Datacenter.
* Microsoft Windows Server 2016 Standard или Datacenter.
* Microsoft Windows Server 2012 R2 Standard или Datacenter.
* Microsoft Windows Server 2012 Standard или Datacenter.
* Microsoft Windows Small Business Server 2011 SP1 Standard.
* Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise или Datacenter.
* Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать с программным обеспечением Microsoft Exchange Server следующих версий:
* Microsoft Exchange Server 2019, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт.
* Microsoft Exchange Server 2016, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт.
* Microsoft Exchange Server 2013 SP1, развернутый как минимум в одной из следующих ролей: Почтовый ящик, Пограничный транспорт или Сервер клиентского доступа (CAS).
* Microsoft Exchange Server 2010 SP3, развернутый как минимум в одной из следующих ролей: Транспортный концентратор, Почтовый ящик или Пограничный транспорт.
* Консоль управления программными средствами антивирусной защиты для серверов Microsoft Exchange должна быть реализована с использованием Microsoft Management Console и должна функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
* Microsoft Windows 10;
* Microsoft Windows 8.1;
* Microsoft Windows 8;
* Microsoft Windows 7 SP1 Professional, Enterprise или Ultimate;
* Microsoft Windows Server 2016;
* Microsoft Windows Server 2012 R2 Standard или Datacenter;
* Microsoft Windows Server 2012 Standard или Datacenter;
* Microsoft Windows Small Business Server 2011 SP1 Standard;
* Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise или Datacenter;
* Microsoft Windows Server 2019 Standard или Datacenter.
* Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны обеспечивать реализацию следующих функциональных возможностей:
* совместимость с DAG в Microsoft Exchange;
* поиск и удаление по требованию всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
* поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в хранящихся на сервере Microsoft Exchange (в том числе в общих папках) сообщениях, включая вложения;
* наличие эвристических методов детектирования;
* проверка почтовых хранилищ и общих папок на сервере, в фоновом режиме для гарантированной обработки всех объектов с использованием самой актуальной версии антивирусных баз без заметного увеличения нагрузки на сервер;
* возможность лечить зараженные архивы;
* возможность выявления и удаления не только однозначно вредоносных, но и потенциально опасных приложений, таких как: рекламные программы, программы-сборщики информации, программы автоматического дозвона на платные сайты и другие утилиты, которые могут использоваться злоумышленниками в своих целях;
* возможность детектирования вредоносных и фишинговых ссылок в теле письма;
* сохранение копий изменяемых сообщений в резервном хранилище, что позволяет восстановить важную информацию в случае некорректного лечения объекта;
* набор параметров поиска для удобства нахождения объекта в резервном хранилище;
* дополнительный уровень проверки с помощью репутационных облачных сервисов;
* возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;
* наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз;
* проверка различных параметров письма, таких как адреса отправителей и получателей, размер письма, а также поля заголовка сообщения;
* фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
* проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);
* проверка IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF);
* проверка с помощью сервиса SPAM URI Realtime Block lists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
* использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и файлов вложений);
* возможность использовать роли пользователей/администраторов для разграничения доступа к настройкам безопасности;
* аудит изменения параметров программы по событиям в журнале событий Windows;
* мониторинг состояния программы, получение статистики работы программы и управление белыми и черными списками адресов Анти-Спама с помощью команд в среде Windows PowerShell;
* использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и имён файлов);
* возможность фильтрации файлов Microsoft Office, содержащих макросы;
* возможность проверки и удаления сообщений, являющихся спамом или содержащих фишинговые и вредоносные ссылки;
* проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
* создание отчетов по работе системы защиты;
* возможность автоматической рассылки отчетов администраторам по расписанию;
* возможность обновления антивирусных баз как с сайтов производителя, так и с внутренних сетевых ресурсов организации;
* возможность фоновой проверки почтовых ящиков и общих папок с использованием Exchange Web Services;
* детальные отчеты в формате HTML;
* наличие возможности отправки отчётов и уведомлений на указанные адреса электронной почты;
* мониторинг работы программы с помощью System Center - Operations Manager;
* интеграция с Active Directory;
* централизованный просмотра состояния защиты;
* возможность распределять роли администраторов системы.

**Требования к обновлению антивирусных баз:**

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

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

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

проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

**Требования к эксплуатационной документации:**

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

**«Руководство пользователя (администратора)»:**

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

**Требования к технической поддержке:**

Техническая поддержка антивирусного программного обеспечения должна:

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

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

* 1. **Технические требования на Acronis** **Защита Данных Расширенная**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Количество** |
| 1 | Сертификат на техническую поддержку Acronis Защита Данных Расширенная для физического сервера | 28 |
| 2 | Сертификат на техническую поддержку Acronis Защита Данных Расширенная для рабочей станции | 8 |

* + 1. **Требования к технической поддержке**

Подписка на техническую поддержку должна предоставлять следующие возможности:

4.1. Контакт со службой технической поддержки посредством телефона, электронной почты.

4.2. Техническая поддержка должна быть доступна на русском языке в рабочие часы, в будни.

4.3. Обозначение критичности проблемы при создании заявке в службе технической поддержке.

4.4. В критичных случаях при обращении в службу технической поддержки первая реакция инженера должна последовать в течение нескольких часов.

4.5. Подписка на техническую поддержку в период своего действия должна гарантировать бесплатные обновления продукта, в том числе переход на новую версию продукта.

5. ПО должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных.

* 1. **Технические требования к предоставлению неисключительных (пользовательских) прав на Программу для ЭВМ «Автоматизация формирования и актуализации внутренней документации учреждений и организаций (АльфаДок) версия 1.0» на срок 1 (один) год. Тариф КИИ.ПДн.Эксперт. Клиентская лицензия "КИИ.ПДн.Эксперт" на срок 1 (один) год**

Исполнитель должен обеспечить передачу неисключительного права на использование программы для ЭВМ «Автоматизация формирования и актуализации внутренней документации учреждений и организаций (Альфа-док) версия 1.0». Клиентская лицензия «КИИ.ПДн.Эксперт» на срок 1 (один) год (далее – Программа Автоматизации) в составе:

* Разработка организационно-распорядительной документации по категорированию объектов КИИ;
* Разработка организационно-распорядительной документации по обработке и защите ПДн, отправка уведомления и информационных писем в Роскомнадзор, генерация согласий на обработку ПДн;
* Разработка моделей угроз и действий нарушителя;
* Разработка документации по эксплуатации криптосредств;
* Ведение электронных журналов;
* Учет проверок регуляторов, информирование о плановых проверках Роскомнадзора;
* Планирование внутренних проверок режима защиты информации;
* Самооценка готовности к проверкам регуляторов Роскомнадзора, ФСБ России;
* Разработка технической документации по защите информации: технических паспортов на информационные системы, технических заданий на создание системы защиты информации, матрицы доступа;
* Анализ технической защищенности информационных систем;
* Формирование аналитических отчетов;
* Самооценка готовности к проверкам ФСТЭК России.

Информационная поддержка:

* консультации по вопросам обеспечения безопасности информации, а также по вопросам пользования Программой Автоматизации (online-консультант, e-mail, телефон);
* предоставление возможности участия в периодических бесплатных вебинарах по обеспечению безопасности информации, использованию и новым возможностям Программы Автоматизации (в течение срока действия лицензии)
  + 1. **Требования к Программе Автоматизации в целом.**

Программа Автоматизации должна быть включена в Единый реестр российских программ для электронных вычислительных машин и баз данных (<https://reestr.minsvyaz.ru/reestr/>).

Программа Автоматизации должна включать в себя следующие функциональные подсистемы:

* Подсистема внесения/изменения исходных данных;
* Подсистема пользовательских стилей документации;
* Подсистема генерации и выгрузки документации;
* Подсистема управления профилем пользователя;
* Подсистема информационной поддержки пользователя (консультирования);
* Подсистема планирования событий и постановки/контроля выполнения задач, получения уведомлений;
* Подсистема регистрации заявок на участие в вебинарах;
* Подсистема ведения журналов по информационной безопасности в электронном виде;
* Подсистема оценки готовности к проверкам Роскомнадзора;
* Подсистема оценки готовности к проверкам ФСБ России;
* Подсистема оценки готовности к проверкам ФСТЭК России;
* Подсистема получения информации о плановых проверках надзорных органов;
* Подсистема ведения перечня внутренних проверок;
* Подсистема автоматической подачи уведомления/информационного письма в Роскомнадзор;
* Подсистема быстрого доступа к формам документов в области информационной безопасности;
* Подсистема базы знаний;
* Подсистема оперативного мониторинга состояния защиты информации в организации по данным в Программе Автоматизации;
* Подсистема быстрой обработки «рабочих ситуаций»
* Подсистема автоматического формирования согласий на обработку ПДн, адаптированных под категории субъектов ПДн;
* Подсистема ведения реестра информационных систем;
* Подсистема формирования отчетности по данным организации;
* Подсистема категорирования объектов критической информационной инфраструктуры.

Доступ к подсистемам должен быть реализован в виде тематических рабочих столов с соответствующими ярлыками для перехода к какой-либо подсистеме. Перечень доступных пользователю рабочих столов:

* Избранное;
* Панель управления;
* Документы;
* Операционная деятельность;
* Рабочие ситуации;
* Органайзер;
* Обучение;
* Аналитика.

Программа Автоматизации должна обеспечивать централизованное хранение и обработку информации в СУБД.

В Программе Автоматизации должна быть реализована защита канала связи посредством протокола https (по умолчанию) и предусмотрена возможность защиты канала связи сертифицированными криптографическими средствами защиты информации с встроенными функциями межсетевого экранирования.

Программа Автоматизации должна поддерживать следующие режимы функционирования:

* Основной режим, в котором все функциональные подсистемы выполняют все свои основные функции;
* Профилактический режим, в котором одна или все подсистемы не выполняют своих функций.

В основном режиме функционирования Программа Автоматизации должна обеспечивать возможность работы пользователей с учетом их возможного нахождения в командировках (в других часовых поясах) в режиме 24 часа в сутки 7 дней в неделю (24х7).

В профилактическом режиме Программа Автоматизации должна обеспечивать возможность проведения следующих мероприятий:

* регламентное техническое обслуживание;
* модернизацию информационно-телекоммуникационной инфраструктуры;
* устранение аварийных ситуаций.

Общее время проведения профилактических работ не должно превышать 2% от общего времени работы Программы Автоматизации в основном режиме.

* + - 1. **Требования к обеспечению информационной безопасности**

В Программе Автоматизации должны быть выполнены требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, что должно быть подтверждено аттестатом соответствия Программы Автоматизации требованиям безопасности.

Исполнитель не должен разглашать и использовать конфиденциальную информацию, принадлежащую Заказчику, которая может стать ему известной в ходе Поставки. Исполнитель несет ответственность за соблюдение этого требования в соответствии с законодательством Российской Федерации.

* + - 1. **Требования к функциям, выполняемым Программой Автоматизации**
         1. **Подсистема внесения/изменения исходных данных**

Подсистема внесения/изменения исходных данных должна быть реализована в виде пошагового Мастера опроса с возможностью сохранения введенной информации на текущем шаге, перехода на следующий и предыдущий шаги.

Мастер опроса должен предполагать переход на следующий шаг только в том случае, если заполнены все обязательные поля предыдущего. При попытке перехода на недоступный шаг должен быть предусмотрен вывод сообщения о недостающей для перехода информации. Для перехода на произвольный доступный шаг должна быть предусмотрена навигация в виде списка шагов в Мастере опроса.

На каждом шаге должны быть предусмотрены краткие справочные комментарии, которые позволяют облегчить процесс ввода данных в Программу Автоматизации.

В Программе Автоматизации должны быть предусмотрены информационные справки, которые помогут пользователю внести правильную информацию в поля Мастера опроса.

Для вводимых параметров при необходимости должны быть предусмотрены:

* предварительное заполнение падежных форм;
* возможность выбора значений из справочников.

Должна быть предусмотрена возможность импорта перечня сотрудников и структурных подразделений из файлов \*.xls, \*.xlsx и \*.csv.

Подсистема должна обеспечивать сбор аналитических данных для формирования комплекта организационно-распорядительной документации по вопросам обеспечения безопасности информации, а также модели угроз безопасности информации (включая модель нарушителя).

Моделирование угроз безопасности должно реализовываться на основании опроса о реализованных мерах, об особенностях и условиях обработки информации.

* + - * 1. **Подсистема пользовательских стилей документации**

Должна быть предусмотрена возможность настройки стилей следующих типов документации:

* Приказ/распоряжение;
* Положение/политики/акты.

При настройке стилей всех типов документации должны быть доступны для редактирования следующие параметры:

* Шрифт (Times New Roman, Arial, Calibri, Courier New);
* Размер шрифта (11пт, 12пт, 13пт, 14пт);
* Междустрочный интервал (1, 1.15, 1.5);
* Верхнее поле;
* Нижнее поле;
* Левое поле;
* Правое поле.

Для документации типа Приказ/распоряжение должны быть доступны для редактирования следующие параметры:

* Шапка документа;
* Написание названия документа (Распоряжение, приказ или постановление, выравнивание, стиль шрифта);
* Написание номера, даты документа и населённого пункта (с возможностью выбора расположения и выравнивания);
* Написание слова «приказываю»
* Параметры списков в документе;
* Параметры блока подписи и согласования документа;
* Параметры названия приложений;
* Параметры списков в приложении;
* Параметры нумерации разделов приложений;
* Параметры маркированных списков;
* Параметры названий таблиц в приложениях;
* Параметры нумерации строк в таблицах.

Для документации типа Положение/политики/акты должны быть доступны для редактирования следующие параметры:

* Написание названия документа (стиль шрифта);
* Параметры блока утверждения документа;
* Параметры заголовков документов;
* Параметры нумерации разделов;
* Параметры маркированных списков;
* Параметры названий таблиц в приложениях;
* Параметры нумерации строк в таблицах.

В данной подсистеме должно быть предусмотрено отображение типового документа для просмотра и изменения настроек документа.

* + - * 1. **Подсистема генерации и выгрузки документации**

На момент предоставления неисключительных (пользовательских) прав на Программу Автоматизации портфель документов, генерируемых Программой Автоматизации, должен иметь следующий состав:

* Приказ/распоряжение о комиссии по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных;
* Приказ/распоряжение об ответственном за организацию обработки персональных данных;
* Приказ/распоряжение об ответственном за обеспечение безопасности персональных данных в информационных системах персональных данных;
* Приказ/распоряжение об утверждении перечня информационных систем персональных данных и перечня персональных данных, содержащихся в программных комплексах, входящих в состав информационных систем персональных данных;
* Приказ/распоряжение об утверждении перечня персональных данных;
* Приказ/распоряжение об утверждении перечней сотрудников, осуществляющих обработку персональных данных и имеющих доступ к обрабатываемым персональным данным;
* Приказ/распоряжение о сотрудниках, которым разрешены действия по внесению изменений в базовую конфигурацию информационных систем и системы защиты персональных данных (в случае, если установленный уровень защищенности ПДн при их обработке в ИС имеет значение 1, 2 или 3);
* Приказ/распоряжение о сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них (в случае, если установленный уровень защищенности ПДн при их обработке в ИС имеет значение 1 или 2);
* Приказ/распоряжение о сотрудниках, имеющих доступ к содержанию электронного журнала сообщений (в случае, если установленный уровень защищенности ПДн при их обработке в ИС имеет значение 1 или 2);
* Приказ/распоряжение об обеспечении безопасности материальных носителей персональных данных;
* Приказ/распоряжение об обеспечении безопасности помещений, в которых размещены информационные системы персональных данных и сохранности носителей персональных данных;
* Приказ/распоряжение об утверждении форм документов, необходимых в целях выполнения требований законодательства в области персональных данных;
* Приказ/распоряжение об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты;
* Приказ/распоряжение об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации при ведении журнала, содержащего персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию организации (в случае наличия пропускного режима);
* Приказ/распоряжение о системе разграничения доступа в информационных системах персональных данных;
* Приказ/распоряжение о комиссии по уничтожению ПД;
* Политика в отношении обработки персональных данных;
* Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
* Порядок хранения, использования и передачи персональных данных сотрудников;
* Акт определения уровня защищенности персональных данных в информационных системах;
* Модель угроз безопасности персональных данных в информационных системах персональных данных (на каждую информационную систему);
* Рекомендации по внесению изменений в Должностные инструкции персонала в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
* Рекомендации по выполнению требований по обеспечению безопасности персональных данных в информационных системах персональных данных;
* Технический паспорт (на каждую информационную систему);
* Техническое задание;
* Памятка по работе с пакетом документов (в Библиотеке уникальных документов);
* План мероприятий по реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и принятых в соответствии с ним нормативных правовых актов;
* Распоряжение об утверждении Положения о комиссии по категорированию объектов критической информационной инфраструктуры;
* Распоряжение об утверждении комиссии по категорированию объектов критической информационной инфраструктуры;
* Распоряжение об утверждении перечня объектов критической информационной инфраструктуры, подлежащих категорированию (в том числе форма отправки сведений во ФСТЭК России);
* Акт категорирования объекта критической информационной инфраструктуры (на каждый объект);
* Модель угроз безопасности информации в автоматизированной системе управления (на каждую АСУ);
* Сопроводительное письмо в ФСТЭК с перечнем объектов критической информационной инфраструктуры, подлежащих категорированию;
* Форма утверждения перечня объектов критической информационной инфраструктуры с ФСТЭК;
* Сопроводительное письмо в ФСТЭК с результатами категорирования объектов критической информационной инфраструктуры;
* Форма о результатах присвоения объекту критической информационной инфраструктуры категории значимости (на каждый объект).

Наименования отдельных документов могут быть изменены по согласованию с Заказчиком.

Должна быть предусмотрена возможность сохранения утвержденных версий документа.

Должна быть предусмотрена возможность подписания утвержденной версии документа (в формате \*.docx) с помощью электронной подписи, встраиваемой в тело документа, с применением алгоритма ГОСТ Р 34.10-2012 (Национальный стандарт Российской Федерации ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 215-ст)).

Должно быть предусмотрено отображение общей информации о портфеле документов, включая наименования документов и их статусов.

Должны быть предусмотрены следующие статусы документов:

* Сформирован;
* Выгружен;
* Утвержден;
* Изменения в данных;
* Изменения в оформлении;
* Изменения в шаблоне;
* Не заполнены данные.

Должна быть предусмотрена возможность предварительного просмотра сформированных документов.

Должна быть предусмотрена выгрузка актуальных версий документов, как конкретного документа (в формате \*.docx, \*.pdf ), так и всех документов одним архивом (в формате \*.zip).

Должно быть предусмотрено автоматическое изменение состава пакета документов в ходе эксплуатации Программы Автоматизации в целях приведения в соответствие с новыми требованиями законодательства Российской Федерации с сохранением утвержденных версий документов. Состав портфеля документов должен учитывать условия обработки защищаемой информации.

Должна быть предусмотрена возможность пользования библиотекой уникальных документов (не генерируемых автоматически), с возможностью самостоятельной загрузки документов пользователем. Должна быть обеспечена возможность скачать и просмотреть документы, а для документов, загруженных пользователем – и удаления документов. Должна отображаться следующая информация о документах:

* Наименование;
* Описание;
* Состояние;
* Источник.

Подсистема должна обеспечивать генерацию комплекта организационно-распорядительной документации и моделей угроз безопасности информации (включая модели нарушителя) на основании собранных ранее аналитических данных. Моделирование угроз безопасности должно реализовываться на основании опроса экспертов о реализованных мерах, об особенностях и условиях обработки информации. Генерация моделей угроз (включая модели нарушителя) должна быть выполнена в строгом соответствии с методическими документами ФСТЭК России и ФСБ России в области определения актуальных угроз безопасности информации.

* + - * 1. **Подсистема управления профилем пользователя**

Должна быть предусмотрена возможность управления следующими параметрами профиля пользователя:

* Фамилия, Имя, Отчество пользователя;
* Фотография (графическое изображение);
* Должность;
* Номер телефона;
* Часовой пояс;
* Местоположение;
* Подписка на информационные рассылки.

Должна отображаться следующая информация:

* Логин;
* Адрес электронной почты;
* Наименование организации;
* Тариф;
* Срок действия тарифа.

Должна быть предусмотрены следующие возможности управления профилем:

* Смена адреса электронной почты;
* Смена пароля;
* Смена ФИО.

Подсистема информационной поддержки пользователя (консультирования)

Должны быть предусмотрены следующие возможности информационной поддержки пользователя:

* онлайн-консультант (Онлайн-консультант должен обеспечивать ведения нескольких диалогов пользователя со службой поддержки. Каждый диалог должен определяться темой и типом вопроса);
* заказ звонка (Заявка на звонок должна содержать Фамилию, Имя, Отчество, город, номер телефона, удобное время для звонка, тему звонка);
* задать вопрос (должен содержать Фамилию, Имя, Отчество, город, адрес электронной почты для ответа и текст сообщения).

Для зарегистрированных пользователей должно быть доступно описание работы с Программой Автоматизации, а также ответы на часто задаваемые вопросы.

* + - * 1. **Подсистема планирования событий и постановки/контроля выполнения задач, получения уведомлений**

В Программе Автоматизации должна быть предусмотрена возможность внесения информации о предстоящих событиях, как произвольных, запланированных самим пользователем, так и событий, генерируемых Программой Автоматизации.

Запланированные события должны отображаться на всех «рабочих столах» пользователя в календаре, а также списком, который состоит из ближайших событий. Дополнительно, должна быть предусмотрена возможность перехода в расширенный календарь с режимами отображения год, месяц, неделя, день. Должна быть обеспечена возможность фильтрации событий по их категории, а также получения уведомлений/напоминаний о событии в Программе Автоматизации.

При создании события заполняется следующая информация:

* Название;
* Место;
* Начало;
* Окончание;
* Повтор;
* Напоминание;
* Календарь;
* Отметка о важности события;
* Заметки.

В Программе Автоматизации должна быть предусмотрена возможность создания задач, изменения статусов задач и закрытия/удаления задач, как произвольных, запланированных самим пользователем, так и задач, генерируемых Программой Автоматизации. Пользователь должен иметь возможность получать уведомления в системе о новых задачах и напоминания о сроке задач.

При создании задачи заполняется следующая информация:

* Тема;
* Текст задачи;
* Дата исполнения;
* Напоминание;
* Комментарий;
* Исполнитель.

Возможные статусы задач:

* Новый;
* В работе;
* Решено;
* Закрыт.
  + - * 1. **Подсистема регистрации заявок на участие в вебинарах**

В Программе Автоматизации должна быть предусмотрена возможность просмотра перечня периодических бесплатных вебинаров по обеспечению безопасности информации, использованию и новым возможностям Программы Автоматизации (в течение срока действия лицензии), с указанием наименования вебинара, даты и времени его проведения, а также целевой аудитории.

Для каждого вебинара должна быть доступна кнопка отправки заявки на участие в вебинаре, по нажатию на которую пользователю должна предоставляться для заполнения форма заявки.

* + - * 1. **Подсистема ведения журналов по информационной безопасности в электронном виде**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому для пользователя доступен перечень журналов для ведения в электронном виде. Должна быть предусмотрена возможность добавления записей в журнал и выгрузки печатной формы журнала по нажатию на кнопку «Выгрузка».

Для каждой записи в журнале должны фиксироваться дата последнего изменения записи и логин пользователя, который произвел эти изменения.

Перечень журналов, доступных для тарифа:

* Журнал поэкземплярного учета средств защиты информации;
* Журнал поэкзмеплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов;
* Журнал учета обращений субъектов персональных данных;
* Лицевой счет пользователя криптосредств;
* Журнал учета хранилищ (сейфов);
* Журнал учета нештатных ситуаций информационных систем персональных данных, выполнения профилактических работ, установки и модификации программных средств на ПЭВМ;
* Журнал учета отчуждаемых машинных носителей персональных данных;
* Журнал проверок электронных журналов;
* Журнал учета передачи персональных данных;
* Журнал периодического тестирования средств защиты информации.
* Журнал обучения пользователей правилам работы с криптосредствами.
  + - * 1. **Подсистема оценки готовности к проверкам Роскомнадзора**

В Программе Автоматизации на рабочем столе «Аналитика» должен быть предусмотрен ярлык, при переходе по которому пользователю доступна возможность оценки готовности к проверке Роскомнадзора. Оценка готовности состоит из списка необходимых пунктов, которые необходимо выполнить для того, чтобы подготовиться к проверке. При этом часть пунктов проставляется пользователем вручную, часть пунктов проставляется автоматически Программой Автоматизации.

Для пользователя должна быть доступна возможность отметить выполненными пункты, которые доступны для отметки вручную. По результатам отметки пунктов подсчитывается общий процент готовности к проверке, а также пользователю доступен список рекомендаций для прохождения проверки.

* + - * 1. **Подсистема оценки готовности к проверкам ФСБ России**

В Программе Автоматизации на рабочем столе «Аналитика» должен быть предусмотрен ярлык, при переходе по которому пользователю доступна возможность оценки готовности к проверке ФСБ России. Оценка готовности состоит из списка необходимых пунктов, которые необходимо выполнить для того, чтобы подготовиться к проверке. При этом часть пунктов проставляется пользователем вручную, часть пунктов проставляется автоматически Программой Автоматизации.

Для пользователя должна быть доступна возможность отметить выполненными пункты, которые доступны для отметки вручную. По результатам отметки пунктов подсчитывается общий процент готовности к проверке, а также пользователю доступен список рекомендаций для прохождения проверки.

* + - * 1. **Подсистема оценки готовности к проверкам ФСТЭК России**

В Программе Автоматизации на рабочем столе «Аналитика» должен быть предусмотрен ярлык, при переходе по которому пользователю доступна возможность оценки готовности к проверке ФСТЭК России. Оценка готовности состоит из списка необходимых пунктов, которые необходимо выполнить для того, чтобы подготовиться к проверке. При этом часть пунктов проставляется пользователем вручную, часть пунктов проставляется автоматически Программой Автоматизации.

Для пользователя должна быть доступна возможность отметить выполненными пункты, которые доступны для отметки вручную. По результатам отметки пунктов подсчитывается общий процент готовности к проверке, а также пользователю доступен список рекомендаций для прохождения проверки.

* + - * 1. **Подсистема получения информации о плановых проверках надзорных органов**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому пользователю доступна информация о плановых проверках надзорных органов. Пользователь должен иметь возможность добавить внеплановую проверку вручную, а также отмечать пройденной проверку из списка проверок с возможностью прикрепить результат прохождения проверки в виде файла.

При создании проверки пользователь может заполнить следующие поля:

* Дата проверки;
* Срок проведения проверки;
* Орган контроля;
* Цель;
* Наименование проверяемого подразделения, филиала;
* Причина проверки;
* Замечания по результатам проверки;
* Срок устранения замечания;
* Штрафы;
* Отметка о прохождении проверки;
* Комментарий;
* Наименование документа по результатам проверки.
  + - * 1. **Подсистема ведения перечня внутренних проверок**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому пользователю доступно управление внутренними проверками в организации. Также здесь должна быть возможность отметить проверку выполненной и ввести дополнительную информацию о проверке.

Добавление или изменение перечня внутренних проверок в организации должно быть доступно в Мастере опросов на отдельном шаге. По умолчанию Программой Автоматизации должен быть введен список рекомендуемых проверок с возможностью изменения. При добавлении проверки должна быть обеспечена возможность выбора наименования проверки из справочника или ввода наименования проверки вручную. Перечень проверок, введенный на шаге, должен отображаться в соответствующем документе в Портфеле документов.

* + - * 1. **Подсистема автоматической подачи уведомления/информационного письма в Роскомнадзор**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому пользователь имеет возможность автоматической отправки уведомления/информационного письма в Роскомнадзор. Должна быть возможность проверки статуса поданного уведомления/информационного письма в Программе Автоматизации, а также возможность просмотра поданного уведомления/информационного письма по переходу на сайт Роскомнадзора.

* + - * 1. **Подсистема быстрого доступа к формам документов в области информационной безопасности**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому пользователю доступен перечень форм, которые необходимо подписать сотрудникам организации, а также перечень дополнительных форм, которые необходимо подписать сотрудникам в случае появления соответствующих прецедентов. Должна быть возможность скачивания указанных форм (в формате \*.docx, \*.pdf) и их просмотра.

Список форм, доступных пользователю:

* Разъяснение субъекту персональных данных (работнику) юридических последствий отказа предоставить свои персональные данные;
* Типовая форма согласия субъекта персональных данных на обработку персональных данных;
* Форма согласия субъекта персональных данных на поручение обработки персональных данных третьему лицу;
* Обязательство о соблюдении конфиденциальности персональных данных;
* Уведомление о факте обработки персональных данных без использования средств автоматизации;
* Форма ознакомления с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных.

Список дополнительных форм, доступных пользователю:

* Акт на списание и уничтожение машинных (бумажных) носителей информации;
* Уведомление о получении персональных данных от третьих лиц;
* Уведомление об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке персональных данных.
  + - * 1. **Подсистема базы знаний**

В Программе Автоматизации для пользователя должен быть доступен раздел База знаний, в котором содержится расширенная информация о Программе Автоматизации. Должна быть предусмотрена возможность просмотра содержащейся информации, а также навигации по разделам Базы знаний.

* + - * 1. **Подсистема оперативного мониторинга состояния защиты информации в организации по данным в Программе Автоматизации**

В Программе Автоматизации должен быть предусмотрен отдельный рабочий стол «Панель управления», который отображает текущий статус процесса организации информационной безопасности в организации, исходя из введенных данных, в виде отдельных тематических виджетов. Из каждого виджета должна быть предусмотрена возможность перехода к соответствующей подсистеме в Программе Автоматизации.

На рабочем столе «Панель управления» на момент поставки доступны следующие виджеты:

* Заполнение данных;
* Документы;
* Проверки регуляторов;
* Внутренние проверки;
* Список задач;
* Защищенность информационных систем.

Виджеты «Документы» и «Проверки регуляторов» должны иметь возможность индивидуальной настройки виджетов.

Запланированные и прошедшие события должны быть отображены в виде таймлайна с возможность масштабирования. Из таймлайна должна быть предусмотрена возможность перехода к календарю событий организации в Программе Автоматизации.

Количественное отображение введенных данных должно быть показано в виде статистики по имеющимся ресурсам организации в отдельном блоке «Ресурсы».

Для отслеживания вносимых изменений пользователями в систему и происходящих событий в системе должен быть доступен «Журнал событий». Просмотр событий в Журнале должен быть возможен отдельно по событиям пользователей и по событиям системы.

* + - * 1. **Подсистема быстрой обработки «рабочих ситуаций».**

В Программе Автоматизации должен быть предусмотрен тематический рабочий стол «Рабочие ситуации», который содержит перечень доступных для пользователя ярлыков, разделенных по тематическим блокам: «Сотрудники», «Оборудование и ПО» и «СЗИ».

На рабочем столе «Рабочие ситуации» на момент поставки доступны следующие «рабочие ситуации»:

* Приём нового сотрудника;
* Назначение ответственных;
* Доступ сотрудников;
* Добавление программного комплекса;
* Добавление АРМ/сервера;
* Добавление сетевого оборудования;
* Установка СЗИ.

Каждая «рабочая ситуация» должна представлять из себя опросник, по результатам которого пользователь должен получить список рекомендаций и сформированных документов с возможностью скачивания.

Должна быть предусмотрена возможность перехода к незавершенной «рабочей ситуации», а также просмотра результатов завершенной «рабочей ситуации».

* + - * 1. **Подсистема автоматического формирования согласий на обработку ПДн, адаптированных под категории субъектов ПДн**

В Программе Автоматизации на рабочем столе «Операционная деятельность» должен быть предусмотрен ярлык, при переходе по которому пользователь имеет возможность сформировать согласия на обработку ПДн, поручение обработки ПДн, передачу ПДн, согласие на включение ПДн в общедоступные источники для каждой категории субъектов ПДн, по которым Организация обрабатывает ПДн, а также для их законных представителей. Согласия должны формироваться на основе данных, введенных пользователем в Мастере опроса, а также в Программе Автоматизации.

Должны быть предусмотрены следующие статусы согласий:

* Сформировано;
* Выгружено;
* Изменения в данных;
* Изменения в оформлении;
* Не создано;
* Не заполнены данные;
* Не требуется.

Должна быть предусмотрена возможность предварительного просмотра сформированных согласий.

Должна быть предусмотрена выгрузка сформированных согласий в формате \*.docx, \*.pdf.

* + - * 1. **Подсистема ведения реестра информационных систем**

В Программе Автоматизации на рабочем столе «Аналитика» должен быть предусмотрен ярлык, при переходе по которому пользователю доступен перечень ИСПДн организации, содержащий общую информацию об ИСПДн, сведения об аттестации, количество актуальных угроз и процент технической защищенности, а также состояние защищенности каждой ИСПДн требуемыми средствами защиты информации.

Для каждой информационной системы из реестра ИСПДн должен быть возможен переход в Карточку ИСПДн, в которой пользователю доступны следующие блоки:

* характеристики ИСПДн;
* состав ИСПДн;
* состояние защищенности АРМ/серверов требуемыми средствами защиты информации;
* угрозы безопасности информации.

Пользователю должны быть доступны возможности просмотра рекомендаций по устранению актуальных угроз и проставления отметок о выполнении необходимых мер по закрытию угрозы. Проставление мер в Программе автоматизации должно выполняться синхронно с Мастером опроса.

Для каждой ИСПДн на основе состояния защищенности ИСПДн требуемыми средствами защиты информации и количества актуальных угроз в ИСПДн должен быть определен процент технической защищенности ИСПДн.

Должна быть возможность скачивания карточки ИСПДн (в формате \*.docx).

* + - * 1. **Подсистема формирования отчетности по данным организации**
* В Программе Автоматизации на рабочем столе «Аналитика» должен быть предусмотрен ярлык, при переходе по которому пользователь имеет возможность ознакомится со сводной информацией по ресурсам организации и сформировать аналитические отчеты. Отчеты должны формироваться на основе данных, введенных пользователем в Мастере опроса, а также в Программе Автоматизации.

На рабочем столе «Отчёты» на момент поставки доступны следующие отчёты:

* Эксплуатируемые информационные системы;
* Используемые СЗИ;
* Сотрудники.

Каждый отчет должен иметь возможность настройки по выбранным параметрам.

Должна быть предусмотрена выгрузка сформированных отчетов в формате \*.docx, \*.pdf.

* + - * 1. **Подсистема категорирования объектов критической информационной инфраструктуры**

В Программе Автоматизации имеется возможность обозначения уже имеющихся информационных систем как объектов критической информационной инфраструктуры и ввода информации о новых объектах (в том числе – автоматизированных систем управления). Для категорирования предусмотрена возможность назначения комиссии. Категория значимости объекта критической информационной инфраструктуры высчитывается автоматически по введенным данным.

По введенным и вычисленным автоматически данным формируется пакет документов по категорированию объектов критической информационной инфраструктуры.

1. **Требования по обеспечению режима конфиденциальности при оказании услуг**

В период оказания услуг и после их окончания Исполнитель не должен разглашать и использовать конфиденциальную информацию, принадлежащую Заказчику, перечень которой определен внутренним распорядительным документом Заказчика, которая может стать ему известной в ходе оказания услуг. Исполнитель несет ответственность за соблюдение этого требования в соответствии с Законодательством Российской Федерации.

|  |  |
| --- | --- |
| **ЗАКАЗЧИК:**  МУП ЕРКЦ г.Уфы  450098 г.Уфа, ул.Комсомольская, 165/1  ИНН 0276069810  КПП 027601001  р/сч 40702810206020100020  ОТДЕЛЕНИЕ №8598 СБЕРБАНКА РОССИИ  БИК 048073601  к/сч 30101810300000000601  Подпись:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Винникова А.Н./  М.П. | **ИСПОЛНИТЕЛЬ:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_/  М.П. |