

Описание объекта закупки

Код по КТРУ или Код (ы) по классификатору ОКПД2 (ОК 034-2014): 58.29.29.000

Тип объекта закупки: *товар (1 шт.)*

№ п/п	Параметры требований	Конкретные требования
1	Наименование закупки	<i>Оказание услуг по оценке эффективности мер по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных</i>
2	Описание объекта закупки согласно ст.33 Федерального закона №44-ФЗ	<i>В соответствии с Техническим заданием (приложение к «Описанию объекта закупки»).</i> <i>Качество услуг должно соответствовать государственным стандартам и техническим условиям согласно действующему законодательству Российской Федерации.</i>
3	Условия поставки товаров, выполнения работ, оказания услуг	<i>Разовая поставка</i>
4	Требования к гарантии качества товара, работы, услуги, а также требования к гарантийному сроку и (или) объему предоставления гарантий их качества, к гарантийному обслуживанию товара (далее - гарантийные обязательства), к расходам на эксплуатацию товара, к обязанности осуществления монтажа и наладки товара, к обучению лиц, осуществляющих использование и обслуживание товара, устанавливаются заказчиком при необходимости.	<i>- Информация о требованиях к гарантийному обслуживанию товара: НЕ УСТАНОВЛЕНО</i> <i>- Требования к гарантии производителя товара: НЕ УСТАНОВЛЕНО</i> <i>- Срок, на который предоставляется гарантия и (или) требования к объему предоставления гарантий качества услуги: в течении действия контракта.</i> <i>Объем предоставления гарантии качества оказанных Услуг – 100 % в течении гарантийного срока.</i>

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на оказание услуг по оценке эффективности мер по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных

1. ОБЩИЕ СВЕДЕНИЯ**1.1. Перечень сокращений:**

Сокращение	Расшифровка сокращения
АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
ИС	Информационная система
ОС	Операционная система
ОРД	Организационно-распорядительные документы
ПДн	Персональные данные, обрабатываемые в информационной системе персональных данных Заказчика
МЭ	Межсетевой экран
АЗ	Антивирусная защита
САЗС	Средство анализа защищенности сети
СОВ	Средство обнаружения вторжений
ПО	Программное обеспечение
СЗИ	Средство защиты информации
СЗПДн	Система защиты персональных данных, обрабатываемых в информационной системе персональных данных
ТЗ	Техническое задание
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ФСБ России	Федеральная служба безопасности Российской Федерации

2. ОБЩИЕ ТРЕБОВАНИЯ К ОКАЗАНИЮ УСЛУГ

2.1. Оказание услуг осуществляется Исполнителем **удаленно** применительно к ИСПДн Заказчика, имеющей следующие характеристики:

- инфраструктура ИСПДн представляет собой одно АРМ, имеющих подключение к информационным сетям общего пользования «Интернет», согласно таблице № 1.
- общее количество АРМ, включенных в инфраструктуру ИСПДн, и адреса их размещения указано в таблице № 1:

Таблица № 1

№	Адрес местонахождения АРМ	Наименование ОС	Кол-во АРМ
1,		Linux	1

2.2. Требования к гарантийным обязательствам.

2.2.1. На все поставляемые СЗИ должны распространяться обязательства гарантийного обслуживания, предоставляемые Производителем.

2.3. Исполнитель должен обеспечить соблюдение правил действующего внутреннего трудового распорядка, контрольно-пропускного режима, внутренних положений и инструкций, действующих на объекте информатизации Заказчика.

2.4. С целью надлежащего исполнения Исполнителем своих обязательств Заказчик обеспечивает:

2.4.1. Доступ сотрудникам Исполнителя на объекты информатизации на базе, которых развернуты ИСПДн.

2.4.2. Предоставление Исполнителю информации и исходных данных в объеме достаточном для разработки Исполнителем документации, являющейся результатом оказания услуг, а именно:

- данные для связи с должностным лицом со стороны Заказчика, ответственного за взаимодействие с Исполнителем в рамках оказания услуг по настоящему Договору/Контракту: ФИО, мобильный телефон, электронная почта;
- список предполагаемых пользователей для ИСПДн;
- информацию о подключении ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена (имеющие подключение или не имеющие подключение);
- информацию о режиме обработки персональных данных в ИСПДн (многопользовательский или однопользовательский);
- информацию о разграничение прав доступа пользователей для ИСПДн (с разграничением прав доступа или без разграничения прав доступа);

- информацию об уровне обобщения (обезличивания) персональных данных;
- сведения об организации охраны и физической защиты помещений объекта информатизации.

2.4.3. Предоставление Исполнителю АРМ, перечисленных в Таблице № 1, отвечающих следующим требованиям:

- АРМ должны в полном объеме соответствовать системным и иным требованиям, предъявляемым Производителями поставляемых СЗИ;
- **АРМ должны функционировать под управлением операционной системы Linux;**
- **Заказчик самостоятельно устанавливает:**
- **Операционную систему (Приложение № 2. Пункт 2);**
- **Право на использование СДЗ УБ. Бессрочная лицензия. Электронная версия (Приложение № 2. Пункт 5);**
- АРМ должны быть оснащены только лицензионным программным обеспечением, драйверами, компонентами и т.п., полностью совместимыми с устанавливаемыми СЗИ и используемыми в целях обработки ПДн.

2.4.4. Предоставление Исполнителю электронной копии (скан копии) приказа о назначении должностного лица, ответственного за организацию обработки ПДн, и создании комиссии с целью определения уровня защищенности персональных данных.

2.5. Заказчик должен обеспечить выполнение требований п.п 2.4 ТЗ и уведомить об их выполнении Исполнителя в течении 10 (десяти) рабочих дней с даты подписания Договора/Контракта.

2.6. Утверждение/согласование Заказчиком документов осуществляется посредством заверения подписью руководителя или уполномоченного лица и печатью организации документов, оформленных на бумажных носителях.

2.7. Исполнитель вправе поэтапно/досрочно осуществить оказание услуг.

2.8. В случае выявления противоречий в положениях Договора/Контракта и/или его приложениях, положения ТЗ имеют приоритетное значение.

2.9.

3. ТРЕБОВАНИЯ К КАЧЕСТВЕННЫМ ХАРАКТЕРИСТИКАМ ОКАЗЫВАЕМЫХ УСЛУГ

3.1. В рамках оказания услуг Исполнитель обеспечивает:

- сбор и анализ исходных данных (**Удаленно**);
- поставку СЗИ;
- внедрение СЗПДн (**Удаленно**);
- проведение мероприятий по оценке эффективности реализованных мер по обеспечению безопасности ПДн.

3.1.1. Сбор и анализ исходных данных включает:

- обследование ИСПДн (**Удаленно**);
- определение актуальных угроз безопасности ПДн;
- разработка рекомендаций по определению уровня защищенности ПДн;
- формирование требований к СЗПДн;
- разработка комплекта шаблонов организационно-распорядительной документации.

Результатом сбора и анализа исходных данных является документация, разрабатываемая Исполнителем документация:

- «Акт обследования информационной системы персональных данных»;
- «Модель угроз безопасности персональных данных»;
- «проект Акта определения уровня защищенности персональных данных»;
- «Техническое задание на создание системы защиты персональных данных»;
- «Программа и методики оценки эффективности реализованных мер по обеспечению безопасности персональных данных»;
- комплект шаблонов организационно-распорядительной документации.

3.1.2. Поставка СЗИ

Поставка СЗИ осуществляется Исполнителем в соответствии с количественными и качественными характеристиками, указанными в приложении № 2 к Договору/Контракту.

Поставляемые СЗИ в рамках контракта, а также сертификаты активации Исполнитель приобретает исключительно для Заказчика (конечного пользователя) в целях исполнения Договора/Контракта, то есть они являются именными, а, следовательно, не могут быть в дальнейшем реализованы (перепроданы) другим заказчикам (конечным пользователям). В случае отказа Заказчика от исполнения Договора/Контракта, либо его расторжении, либо частичного исполнения Договора/Контракта по вине Заказчика, Заказчик возмещает Исполнителю все расходы, понесенные на их приобретение.

Результатом поставки СЗИ является:

- заверенные сторонами Акты оказанных услуг, фиксирующие факт поставки.

3.1.3. Внедрение СЗПДн.

Удаленное внедрение СЗПДн, осуществляется в соответствии с проектной документацией на СЗПДн, и включает:

- базовую инсталляцию поставляемых СЗИ в соответствии с требованиями эксплуатационной документации;
 - настройку поставляемых СЗИ в объеме достаточном для успешного проведения оценки эффективности системы защиты ПДн;
 - разработку Исполнителем «проект Технического паспорта информационной системы персональных данных».

Для настройки СЗИ, предусмотренных настоящим Техническим заданием, Заказчик обязан предоставить Исполнителю:

- работоспособные файлы дистрибутивов ключей (парольно-ключевую информацию), самостоятельно полученные Заказчиком в соответствии с действующими нормами (правилами). О получении указанных файлов Заказчик уведомляет исполнителя в течение 3 (Трех) дней со дня их получения, путем направления уведомления на электронную почту.

Результатом является внедрения СЗИ является:

- корректно функционирующая СЗПДн;
- «проект Технического паспорта информационной системы персональных данных», разрабатываемый Исполнителем.

В целях соблюдения требований законодательства в области защиты ПДн Заказчик обеспечивает:

- оформление и утверждение документа «Акт определения уровня защищенности персональных данных»;
- оформление и утверждение документа «Технический паспорт информационной системы персональных данных»;
- оформление и согласование документа «Программа и методики оценки эффективности реализованных мер по обеспечению безопасности персональных данных»;
- заполнение и оформление шаблонов организационно-распорядительной документации.

3.1.4. Проведение мероприятий по оценке эффективности реализованных мер по обеспечению безопасности ПДн.

В рамках проведения мероприятий по оценке эффективности реализованных мер по обеспечению безопасности ПДн Исполнителем проводятся комплексные испытания ИСПДн в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки ПДн.

Результатом мероприятий по оценке эффективности реализованных мер по обеспечению безопасности ПДн является разработанная Исполнителем документация:

- «Протокол проведения оценки эффективности реализованных мер по обеспечению безопасности персональных данных»;
- «Заключение по результатам оценки эффективности реализованных мер по обеспечению безопасности персональных данных».

Срок действия «Заключение по результатам оценки эффективности реализованных мер по обеспечению безопасности персональных данных»: 3 года при условии, что Заказчик обеспечивает соответствие ИСПДн, выданному заключению.

4. ПОРЯДОК, УСЛОВИЯ И СРОКИ ОКАЗАНИЯ УСЛУГ

4.1. Срок оказания Исполнителем услуг: с даты заключения контракта по 10.12.2026.

5. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

5.1. Общие требования

Язык оформления документации – русский, за исключением общепринятых названий и оригинальных наименований программно-аппаратных средств импортного производства.

Документы должны быть оформлены Исполнителем в соответствии с требованиями оформленный в соответствии с требованиями «ГОСТ 2.105-95 ЕСКД. Общие требования к текстовым документам».

С целью надлежащего исполнения Сторонами своих обязательств, состав, объем, наименования, требования к содержанию документации могут быть скорректированы Сторонами в ходе оказания услуг.

Комплект документации оформляется Исполнителем на бумажных носителях и передается Заказчику нарочно или направляется почтовым отправлением, за исключением комплекта шаблонов организационно-распорядительной документации.

Комплект шаблонов организационно-распорядительной документации оформляется Исполнителем в электронном виде, редактируемом формате и предоставляется Заказчику посредством отправки на электронную

почту, предоставляемую Заказчиком или опубликованную им на официальном сайте (в случае непредоставления).

6. ТРЕБОВАНИЕ К БЕЗОПАСНОСТИ ОКАЗЫВАЕМЫХ УСЛУГ

6.1. Все сведения о составе и характеристиках объектов информатизации Конечных пользователей и Заказчика являются конфиденциальной информацией.

6.2. Исполнитель обязуется:

7. не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации, циркулирующей и хранящейся на объектах информатизации Заказчика;

8. не осуществлять несанкционированный доступ к информационным ресурсам объектов информатизации Заказчика;

9. не проводить незаконное копирование информации, циркулирующей или хранящейся на объектах информатизации Заказчика;

10. не предпринимать манипулирование информацией, циркулирующей или хранящейся на объектах информатизации (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);

11. не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;

12. не внедрять на объектах информатизации программы-вирусы (загрузочные, файловые и др.);

13. не устанавливать программные и аппаратные закладные устройства в технические средства объектов информатизации Заказчика;

14. не устанавливать в технические средства объектов информатизации программное обеспечение, зараженное вирусами.

14.1. Нарушение настоящих требований влечёт за собою гражданско-правовую, административную или уголовную ответственность в соответствии с законом Российской Федерации.

15. ТРЕБОВАНИЯ СООТВЕТСТВИЯ НОРМАТИВНЫМ ДОКУМЕНТАМ

15.1. Услуги должны быть оказаны в соответствии с требованиями следующих нормативных и правовых актов Российской Федерации в области обеспечения информационной безопасности:

16. Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных»

17. Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

18. Федеральный закон от 04 мая 2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;

19. Постановление Правительства Российской Федерации от 01 ноября 2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

20. Постановление Правительства Российской Федерации от 16 апреля 2012 №313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, 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)»;

21. Постановление Правительства РФ от 03 февраля 2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

22. «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденные Приказом Гостехкомиссии России от 30 августа 2002 № 282;

23. Приказ ФСБ России от 10 июня 2014 г. № 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости»;

24. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

25. Приказ Федеральной службы по техническому и экспортному контролю от 29 апреля 2021 г. № 77 «Об утверждении порядка организации и проведения работ по аттестации работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
26. ГОСТ РО-0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»;
27. ГОСТ РО-0043-003-2013 «Защита информации. Аттестация объектов информатизации. Общие положения».
28. ГОСТ 2.105-95 ЕСКД. Общие требования к текстовым документам
- 28.1. Исполнитель должен соответствовать требованиям, установленным в соответствии с статьей 12 Федерального закона от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности» к лицам, осуществляющим оказание услуг, являющихся объектом закупки, а именно:
29. наличие собственной действующей лицензии ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), при условии наличия в данной действующей лицензии работ (услуг), предусмотренных пунктами «12», «20», «21», «28» Перечня оказываемых услуг и оказываемых услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств, утверждённого постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313.;
30. наличие собственной действующей лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, при условии наличия в данной действующей лицензии работ (услуг), предусмотренных подпунктами «б», «е», «д» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого постановлением Правительства Российской Федерации от 03 февраля 2012 г. № 79.

Требования к количественным и качественным характеристикам поставляемого товара, средствам защиты информации.

№ п.п.	Наименование	Форма	Характеристики	Кол-во
1.	Сервис по разработке ОРД	Лицензия, без НДС	Исполнитель должен разработать и предоставить Заказчику доступ к Веб-сервису Исполнителя. Исполнитель должен предоставить Заказчику лицензию для доступа к веб-сервису по автоматизированному созданию организационно-распорядительных документов в части обработки персональных данных с использованием средств автоматизации и эксплуатации средств криптографической защиты информации и обеспечить его бесперебойное функционирование в режиме «24/7», за исключением нештатных ситуаций (длительное отключение электропитания, сбой работы программных или аппаратных средств и т.п.). Веб-сервис должен иметь клиент – серверную архитектуру, где серверная часть развернута на мощностях Исполнителя. Для предоставления доступа к веб-сервису Исполнитель регистрирует в базе данных нового Конечного пользователя, уполномоченного для работы с веб-сервисом со стороны Заказчика, с произвольными логином и паролем и передает данные учетной записи Конечному пользователю. Исполнитель обязан обеспечить бесплатное техническое сопровождение Пользователей Заказчика в течение всего срока действия лицензии на право использования веб-сервиса по автоматизированному созданию организационно-распорядительных документов в части обработки персональных данных с использованием средств автоматизации и эксплуатации средств криптографической защиты информации (через форму заявки в разделе Техподдержка, в режиме 5x8 с 09:00 до 18:00 МСК в рабочие дни). 1.1. Требования к автоматизированному рабочему месту Пользователя для работы с веб-сервисом. По требованиям законодательства Российской Федерации в области криптографической защиты информации доступ Пользователей к веб-сервису должен предоставляться посредством программного обеспечения на основе браузеров, поддерживающих защищенные протоколы TLS, на базе российских криптографических алгоритмов ГОСТ, например, Яндекс Браузер или аналоги. 1.2. Требования к функциональным возможностям веб-сервиса Процесс заполнения шаблонов документов должен быть максимально автоматизирован. Заполнение сведений об организации должно производиться автоматически по номеру ОГРН на основе данных Единого государственного реестра юридических лиц (ЕГРЮЛ). Заполнение фиксированных видов сведений, перечень которых ограничен, должно производиться путем выбора единственного необходимого значения из выпадающего списка. Остальные виды сведений заполняются Пользователем вручную. Для видов сведений «Фамилия», «Имя», «Отчество», при их вводе в именительном падеже, должно производиться автоматическое заполнение падежных форм «родительный падеж», «дательный падеж», «творительный падеж», «предложный падеж». В дальнейшем веб-сервис должен автоматически подставлять в шаблон нужную падежную форму в зависимости от	

		контекста. В веб-сервисе должна быть предусмотрена шкала прогресса заполнения шаблона (от 0 до 100 %) с помощью которой Пользователь сможет контролировать степень его заполнения. В веб-сервисе при заполнении шаблона должна быть реализована система подсказок для Пользователя. И чек-лист для подготовки к заполнению шагов сервиса. В веб-сервисе должна быть реализована система выбора необходимого шаблона: - комплект ОРД; - комплект применения СКЗИ; - уведомление в Роскомнадзор; В веб-сервисе должен быть реализован функционал позволяющий: - провести анализ сайта компании на наличие файлов cookies и метрических программ. По итогу сформировать отчет с рекомендациями; - проверить расположение сайта и вывести информацию в виде отчета; - рассчитывать Уровень защищенности Информационных систем; - Рассчитывать оценку вреда, который может быть причинен субъектам персональных данных; - Формировать документ Согласие для списка сотрудников. Функционал веб-сервиса должен предоставлять возможность выбора формата (*.docx или *.rtf), в котором будет сохранен итоговый комплект документов. В веб-сервисе должен быть реализован функционал рассылки Пользователям уведомлений с приглашением принять участие в бесплатных вебинарах по направлению «Информационная безопасность». Веб-сервис должен обеспечивать корректное функционирование и отображение интерфейса как при использовании Пользователями персонального компьютера, так и при использовании мобильных устройств. 1.3. Идентификация и аутентификация Пользователей веб-сервиса Доступ Пользователей к веб-сервису должен осуществляться с использованием логина и пароля, выданного Исполнителем. Настройки парольной политики должны предписывать наличие в паролях цифр и букв верхнего и нижнего регистров одновременно, а их длина должна составлять не менее 8 символов. Настройки парольной политики Пользователей должны предусматривать блокировку учетной записи после серии неудачных попыток входа, при этом число попыток не должно превышать 5 (пяти). 1.4. Работа пользователя с Веб-сервисом Заказчик должен иметь возможность внесения изменений в перечень сведений об организации на любом этапе заполнения шаблона. Заказчик должен иметь возможность настройки персонализации. Заказчик должен иметь возможность получать уведомления, рассылки, связанные с изменениями в шаблонах, лицензией, законодательством.	
--	--	--	--

			Веб-сервис должен быть зарегистрирован в Едином реестре российских программ для электронных вычислительных машин и баз данных в соответствии с действующим законодательством. Исполнитель обязан самостоятельно и своевременно отслеживать все изменения в законодательстве РФ в области информационной безопасности и оперативно вносить корректировки в шаблоны документов и состав итогового комплекта документов. Веб-сервис должен представлять собой автоматизированное решение для создания комплектов организационно – распорядительных документов на основе готовых шаблонов в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Веб-сервис должен автоматически заполнять сведения об организации на основе данных Единого государственного реестра юридических лиц (ЕГРЮЛ). Подключение к веб-сервису должно обеспечиваться с применением шифрования информации по действующему алгоритму ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Веб-сервис должен быть совместим с операционными системами Windows 7 и выше, Linux, а также быть доступным для работы на мобильных устройствах, функционирующих на операционных системах android 9.0 и выше и iOS10 и выше. Срок действия лицензии не более – 12 месяцев.	
2.	Операционная система	Лицензия , без НДС	1. Требования соответствия законодательным и нормативным документам 1.1. Операционная система должна соответствовать требованиям Постановления Правительства РФ от 23.12.2024 № 1875 «О мерах по предоставлению национального режима при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, закупок товаров, работ, услуг отдельными видами юридических лиц». 1.2. Эксплуатационная документация на операционную систему должна раскрывать сведения о средствах и способах реализации функций безопасности, предусмотренных требованиями нормативных документов по п.1.3.1, 1.3.4, 1.3.5, 1.3.6. 1.3. Операционная система должна иметь сертификат соответствия требованиям нормативных документов ФСТЭК России: 1.3.1. «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016); 1.3.2. «Профиль защиты операционных систем типа «А» не ниже 4 класса ИТ.ОС.А4.ПЗ (ФСТЭК России, 2017); 1.3.3. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) не ниже 4 уровня; 1.3.4. «Требования по безопасности информации к средствам контейнеризации» (ФСТЭК России, 2022) не ниже 4 класса защиты; 1.3.5. «Требования по безопасности информации к средствам виртуализации» (ФСТЭК России, 2022) не ниже 4 класса защиты; 1.3.6. «Требования по безопасности информации к системам управления базами данных» (ФСТЭК России, 2023) не ниже 4 класса защиты.	1

			2. Требования к встроенному комплексу средств защиты информации операционной системы 2.1. Операционная система должна обеспечивать встроенными сертифицированными средствами: • идентификацию и аутентификацию пользователей; • управление средствами аутентификации; • управление учетными записями пользователей, разграничение полномочий и назначение прав пользователям; • реализацию дискреционного разграничения доступа; • возможность указания параметров настройки комплекса средств защиты во время создания пользователя; • возможность создания среды выполнения контейнеров, обеспечения работы с ними и поддержкой изоляции процессов, выполняемых в контейнерах. 2.2. В составе операционной системы должна быть реализована возможность защиты аутентификационной информации с использованием функции хэширования. 2.3. В составе операционной системы должно быть ядро, поддерживаемое Центром исследования безопасности системного программного обеспечения ИСП РАН. 2.4. Операционная система должна иметь графическое средство настройки ограничений пользователя по запуску программ в изолированном окружении с использованием механизма пространств имён и фильтрации системных вызовов, обеспечивающих: • ограничение прав пользователя на запуск приложений ядром системы; • ограничение прав пользователя средствами графического интерфейса; • разрешение запуска только тех программных компонентов, которые явно разрешены администратором безопасности. 2.5. Обеспечение запрета запуска (исполнения) пользователем созданных самостоятельно (с использованием текстовых редакторов или непосредственно в командной строке) программ с использованием интерпретируемых языков программирования. 2.6. В составе операционной системы должны быть графические средства настройки защиты машинных носителей, обеспечивающие: • идентификацию устройств и сопоставление пользователя с устройством; • управление доступом субъектов доступа к устройствам методами дискреционного управления доступом; • задание правил управления доступом, разрешающих или запрещающих доступ субъектов доступа к устройствам, а также определяющих разрешенные типы доступа, в том числе с использованием атрибутов безопасности; • учет носителей информации и контроль использования интерфейсов ввода и вывода. 2.7. Операционная система должна включать в свой состав программное обеспечение, реализующее задачи аудита и журналирования (регистрации) событий безопасности. Регистрация событий безопасности должна выполняться с учётом требований ГОСТ Р 59548-2022. 2.8. Операционная система должна включать в состав графические средства настройки контроля целостности:	
--	--	--	---	--

		• контроль целостности дистрибутива; • контроль объектов файловой системы; • контроль целостности исполняемых файлов. 2.9. Операционная система должна обеспечивать возможность блокировки: • запуска исполняемых файлов, включая EXE и загрузки библиотек, в том числе DLL, .NET 7/8, целостность которых нарушена; • открытия файлов, в том числе пустых, и самораспаковывающихся 7Z архивов, установленных на контроль, при нарушении их целостности. 2.10. В составе операционной системы должна быть реализована возможность ограничения полномочий пользователей по использованию консолей. 2.11. В операционной системе должна быть реализована возможность очистки и ограничения работы с оперативной памятью. 2.12. Должны быть обеспечены работы по устранению уязвимостей и включению информации об уязвимостях программного обеспечения операционной системы в банк данных угроз безопасности информации ФСТЭК России (https://bdu.fstec.ru/vul). 2.13. Механизмами безопасности операционной системы должна быть обеспечена защита системных и привилегированных процессов от несанкционированного доступа и управления (исключение возможности повышения привилегий пользователей и управления привилегированными процессами в случае использования дефектов/уязвимостей в программном обеспечении информационной системы). 2.14. Операционная система должна обеспечивать запрет операций записи в системные каталоги и файлы (программы, файлы конфигурации), а также установки программного обеспечения, запуска и останова системных процессов операционной системы, вне зависимости от изменения пользователем своих привилегий в текущем сеансе работы. 2.15. Операционная система должна предоставлять средство настройки профиля системы со следующими возможностями: • настройка комплекса средств защиты в соответствии с требованиями о защите информации, предъявляемыми к определенному классу защищенности информационных систем, при помощи графического интерфейса; • импорт и экспорт настроек комплекса средств защиты системы. 2.16. Операционная система должна иметь средства для работы со сторонними устройствами аутентификации - токенами, обеспечивающие следующие возможности: • двухфакторная авторизация; • вход и разблокировка сессии по токену; • блокировка сессии при извлечении токена. 3. Требования к функциональным возможностям операционной системы 3.1. Операционная система должна быть предназначена для функционирования на средствах вычислительной техники с аппаратной платформой x86-64, включая процессоры Intel не ниже 10-го поколения. 3.2. Операционная система должна поддерживать работу на ядре Linux версии не ниже 6.1	
--	--	---	--

		с возможностью обновления до новых версий ядра (в соответствии с документацией на продукт). 3.3. Операционная система должна обеспечивать функционал в графическом исполнении: • наличие графических средств создания, настройки и управления несколькими репозиториями используемого программного обеспечения со следующим функционалом: ○ проверка зависимостей пакетной базы; ○ автоматическая публикация в сети по протоколам http и ftp; ○ выбор конкретных репозиториях, из которых будет произведено обновление пакетов; • наличие средств подключения к операционной системе по протоколу RDP, со следующими возможностями по умолчанию: ○ вход в сессию локально, а затем подключение к этой сессии удаленно с автоматической блокировкой доступа к сессии локально и возможностью одновременной работы локально в графической сессии из-под другого пользователя; ○ вход в сессию удаленно, а затем подключение к этой сессии локально при входе в систему с автоматическим отключением удаленного клиента; ○ проброс нескольких смарт-карт или токенов (eToken, Рутокен, JaCarta) с возможностью их одновременного использования на сервере и клиенте. • наличие графической утилиты управления драйверами nvidia, intel, amd с возможностью выбора драйверов и возможностью восстановления драйверов при неудачной загрузке операционной системы; • наличие графических средств настройки выделяемых ресурсов памяти пользователям (квоты); • наличие графического инструмента для просмотра и редактирования значения переменных окружения (просматривать текущие переменные, изменять значение и описание переменных, удалять и объявлять переменные); • наличие графических средств настройки и изменения ориентации экрана в ручном или автоматическом режиме, с возможностью калибровки поворота, а также задания ориентации по умолчанию; • наличие графического инструмента управления регистрацией событий, включающего в себя управление сервисом системных событий, настройку ротации событий и настройку параметров сбора системных событий, наличие графического средства просмотра системных событий; • наличие графических средств настройки сохранения и восстановления сессии пользователя (восстановление при старте запущенных программ и их расположения после полного отключения электропитания автоматизированного рабочего места); • наличие графических средств настройки потребления электроэнергии (яркость экрана, потухание, выключение монитора, переход в ждущий режим, сон и гибернацию) в случае изменения настроек электропитания (питание от сети, питание от батареи, низкий заряд батареи); • наличие графических средств монтирования usb устройств по сети (usbip или аналог) для	
--	--	---	--

		подключения к нескольким персональным компьютерам; • наличие графических средств настройки одновременной работы нескольких сотрудников на одном персональном компьютере с разделяемыми профилями; • наличие графических средств создания системных отчётов, предназначенных для сбора, сжатия, сохранения и для отправки в службу сопровождения диагностических данных о работе системы; • наличие графических средств запуска работы с удалёнными, отдельными и вложенными графическими сессиями; • наличие графических средств настройки планирования времени завершения работы без участия пользователя (завершение сессии, выключение автоматизированного рабочего места, перехода в энергосберегающие режимы) с настройкой уведомления о событии; • наличие графических средств запуска приложений с изменением приоритета выполнения с возможностью запуска от имени другого пользователя; • наличие графических средств настройки параметров загрузчика операционной системы (загружаемая операционная система по умолчанию, передаваемые параметры ядра, таймаут для ожидания действий пользователя, выбора источника ввода данных при загрузке, выбор терминала для вывода информации); • наличие графических средств расчёта контрольных сумм файлов и их сравнения; • наличие графических средств работы с архивами (zip, rar, 7zip, tar, tgz, tar.gz, tar.bz, tar.xz, iso); • наличие графических средств для оповещения пользователя о конфликте IP-адресов при подключении к сети; • наличие графических средств настройки системы, в том числе: - О установки и синхронизация времени; - О управления пользователями; - О просмотра системных журналов; - О настройки и обслуживания принтеров; • наличие графических средств настройки цветового баланса для каждого монитора по отдельности; • наличие возможности присвоить пользовательские наименования звуковым устройствам при помощи графического интерфейса; • наличие графических средств ввода в домен, в том числе с возможностью добавить компьютер в нужное подразделение (OU, Organizational Unit) для клиента Active Directory; • наличие графического центра уведомлений на рабочем столе с следующими возможностями: - О настройка расположения уведомлений; - О возможность индивидуальных настроек для конкретных приложений; - О настройка отображения уведомлений на экране блокировке и при разблокировке; • наличие графических инструментов глобального поиска по расположению, содержимому,	
--	--	--	--

			времени создания или изменения, размеру файла, с отображением результатов поискового запроса в интерактивном окне со следующими возможностями: - О группировки и фильтрации результатов по найденным категориям (файлы, приложения, папки, архивы); - О отображения свойств найденных файлов (имя, тип, путь, размер); • наличие графического инструмента для настройки частот процессора. 3.4. Операционная система должна поддерживать следующий функционал: • графический интерфейс, адаптированный под использование на портативных устройствах с поддержкой управления настройками системы, приложениями и сервисами (включая контекстные меню) с помощью touchscreen (сенсорный экран) с возможностью автоматического отключения при подключении мышки; • возможность подключения к сети wi-fi до входа в систему, а также аутентификация в сети wi-fi с использованием смарт-карты; • наличие в репозитории операционной системы браузера из единого реестра российских программ для электронных вычислительных машин и баз данных; • возможность ввода аутентификационных данных пользователя при входе в систему и при разблокировке экрана с использованием виртуальной клавиатуры без необходимости дополнительных настроек. 3.5. Операционная система должна обеспечивать поддержку файловых систем и сетевых протоколов: • ext2/3/4, fat, ntfs, iso9660, XFS, ZFS, BTRFS; • TCP/IP, DHCP, DNS, FTP, TFTP, SMTP, IMAP, HTTP(S), NTP, SSH, NFS, SMB; • поддержка стандарта ISO9660; • наличие средств подключения ресурсов WebDAV в качестве локальной файловой системы для возможности использования их стандартными приложениями операционной системы. 3.6. Операционная система должна обеспечивать возможность создания точек восстановления (снапшотов) для последующего возвращения системы к исходному состоянию в случае сбоя, а также иметь возможность возврата к состоянию до начала установки обновлений. 3.7. Операционная система должна обеспечивать среду функционирования для сертифицированных средств криптографической защиты информации, предназначенных для создания и проверки электронной подписи. 3.8. Установщик операционной системы должен иметь следующий функционал: • обеспечивать возможность запуска VNC сервера для удаленного подключения к клиентским машинам и управления ими как на этапе загрузки с установочного диска в главном меню программы установки, так и непосредственно в LiveCD; • возможность автоматической установки при помощи файла конфигурации формата .yaml; • возможность задания параметров для администратора и нескольких локальных пользователей; • предоставлять возможность установки любых пакетов из репозитория операционной	
--	--	--	--	--

			системы во время установки. 3.9. Операционная система должна предоставлять инструмент для обновления между мажорными версиями с сохранением настроек операционной системы и ПО. 3.10. Операционная система должна предоставлять средства для локальной виртуализации (виртуальные машины, созданные на рабочей станции или удаленном сервере и используемые в однопользовательском режиме) с графическим интерфейсом управления и возможностью группировать отображаемые виртуальные машины. 3.11. Операционная система должна предоставлять специальные возможности: • экранный диктор и синтезатор речи для русского языка; • голосовой ввод; • настройка визуальных и звуковых уведомлений на события, связанные со специальными возможностями; • настройка залипающих, замедленных и прыгающих клавиши; • настройка управления курсором мыши с помощью цифровой клавиатуры. 3.12. Дополнительные функциональные компоненты: • клиентское ПО, для осуществления подключения по протоколу RDP; • агенты служб централизованного управления системой; • приложение для сканирования документов с возможностью пропуска пустых страниц и с сохранением размера области сканирования; • средство просмотра и редактирования файлов .pdf; • средство для эмуляции запуска исполняемых файлов .exe; • средства просмотра и редактирования графики и изображений; • средство оптического распознавания символов. 4. Правовая безопасность Документом, подтверждающим право на поставку лицензий, является наличие действующего сублицензионного договора с разработчиком ПО или его партнером. 4. Основные характеристики ОС: Версия – 1.8, «Усиленный» («Воронеж»), электронная, для рабочей станции, обновления Тип 1 на 12 мес.	
3.	СЗИ от СКН, МЭ, СОВ	Лицензия, без НДС	1. Средство контроля съемных машинных (СКН) уровня подключения съемных носителей должно представлять собой программный модуль средства защиты информации в операционных системах семейства Linux и должно быть предназначено для разграничения доступа пользователей информационной системы к сменным накопителям и осуществления контроля подключения накопителей. 2. СКН должно быть предназначено для ПЭВМ типа IBM PC под управлением следующих операционных систем семейства Linux в многопользовательском режиме их эксплуатации: — Альт Рабочая Станция 10.0; — Альт Рабочая Станция 10.1; — Альт Рабочая Станция 10.2; — Альт Рабочая Станция 10.4;	1

			— Альт Рабочая Станция 10.4; — Альт Рабочая Станция 11; — Альт Сервер 10; — Альт Сервер 11; — Альт 8 СП релиз 10; — Альт 8 СП релиз 10 версия 2; — Astra Linux Special Edition 1.7; — Astra Linux Special Edition 1.8; — РЕД ОС 7.3 Муром; — РЕД ОС 8.0; — МСВСфера АРМ 9; — МСВСфера Сервер 9; — Debian 10; — Debian 11; — Debian 12; — Ubuntu 18.04; — Ubuntu 20.04. 3. СКН должно поддерживать 64-битные версии операционных систем. 4. СКН должно быть предназначено для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах и ТС с поддержкой виртуальных сред. 5. Модуль СКН должен быть сертифицирован на соответствие требованиям ФСТЭК России к средствам контроля съемных машинных носителей информации по 4-му классу защиты в соответствии с профилем защиты средств контроля подключения съемных машинных носителей информации (ИТ.СКН.П4.ПЗ). 6. СКН должно иметь возможность быть использовано: — при создании защищенных автоматизированных систем до класса защищенности 1Г включительно; — в государственных информационных системах до 1 класса защищенности включительно; — в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности включительно; — в информационных системах персональных данных до 1 уровня защищенности включительно; — при защите значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно. 7. СКН должно обеспечивать: 7.1. контроль использования интерфейсов ввода/вывода средств вычислительной техники, подключения внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации; 7.2. возможность назначения прав доступа к конкретному накопителю; 7.3. возможность установить описание для сменного накопителя;	
--	--	--	--	--

			7.4. возможность удаленной регистрации аппаратных идентификаторов и управление параметрами СКН при помощи отдельного кроссплатформенного центра управления. 7.1. возможность периодического архивирования журналов событий; 7.2. возможность экспорта журналов безопасности в форматы PDF, ODS и XML; 7.3. возможность локального и удаленного администрирования; 7.4. возможность администрирования через графическую или консольную оболочку, функционирующую в операционных системах на базе ядра Linux, а также через графическую оболочку администрирования, функционирующую в операционных системах семейства Windows; 7.5. возможность установки графической и консольной оболочки СКН из единого файла-установщика; 7.6. возможность проверки корректности функционирования СКН, самотестирования; 7.7. возможность обновления СКН с выполнением сохранения ранее произведенных настроек СКН; 7.8. возможность настройки всех параметров СКН из единой консоли администрирования; 7.9. возможность экспортировать и импортировать файлы конфигурации для восстановления настроек СКН; 7.10. возможность оповещения при событиях. 8. Реализация СКН должна быть полностью программной. 9. Поставка СКН должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения с указанием всех необходимых модулей и требуемого количества лицензий по каждому модулю. Вариант формулировки: — неисключительное право на использование СКН (программное обеспечение). 10. Межсетевой экран (МЭ) должен представлять собой программный модуль средства защиты информации в операционных системах семейства Linux, предназначенный для защиты информации от несанкционированного доступа посредством осуществления контроля и фильтрации проходящих через сетевые интерфейсы рабочих станций сетевых пакетов в соответствии с заданными администратором правилами. 11. МЭ должна быть предназначена для ПЭВМ типа IBM PC под управлением следующих операционных систем семейства Linux в многопользовательском режиме их эксплуатации: — Альт Рабочая Станция 10.0; — Альт Рабочая Станция 10.1; — Альт Рабочая Станция 10.2; — Альт Рабочая Станция 10.4; — Альт Рабочая Станция 10.4; — Альт Рабочая Станция 11; — Альт Сервер 10; — Альт Сервер 11; — Альт 8 СП релиз 10;	
--	--	--	---	--

			— Альт 8 СП релиз 10 версия 2; — Astra Linux Special Edition 1.7; — Astra Linux Special Edition 1.8; — РЕД ОС 7.3 Муром; — РЕД ОС 8.0; — МСВСфера АРМ 9; — МСВСфера Сервер 9; — Debian 10; — Debian 11; — Debian 12; — Ubuntu 18.04; — Ubuntu 20.04. 12. МЭ должен поддерживать 64-битные версии операционных систем. 13. МЭ должен быть предназначен для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах и ТС с поддержкой виртуальных сред. 14. Модуль МЭ должен быть сертифицирован на соответствие требованиям ФСТЭК России к межсетевым экранам по 4-му классу защиты в соответствии с профилем защиты межсетевых экранов типа «В» четвертого класса защиты (ИТ.МЭ.В4.ПЗ). 15. МЭ должен иметь возможность быть использован: — при создании защищенных автоматизированных систем до класса защищенности 1Г включительно; — в государственных информационных системах до 1 класса защищенности включительно; — в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности включительно; — в информационных системах персональных данных до 1 уровня защищенности включительно; — при защите значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно. 16. Должен быть реализован модуль межсетевого экрана (МЭ), предназначенный для операционных систем с ядром Linux версии 5.6 и новее. Модуль МЭ должен обеспечивать: 16.1. контроль и фильтрацию проходящих через сетевые интерфейсы ПК сетевых пакетов в соответствии с заданными правилами (такими, как направление передачи, IP-адреса, порты, протоколы); 16.2. возможность настройки приоритета обработки правил МЭ; 16.3. фильтрацию трафика по протоколам 7-го (прикладного) уровня и командам этих протоколов; 16.4. фильтрацию сетевого трафика на основе наличия в сетевом пакете мобильного кода; 16.5. фильтрацию сетевого трафика на основе прямого соответствия содержимому сетевого пакета;	
--	--	--	--	--

		16.6. фильтрацию сетевого трафика на основе типа сетевого или транспортного протокола; 16.7. фильтрацию сетевого трафика на основе черного и белого списков приложений; 16.8. возможность выполнения групповых операций над правилами МЭ; 16.9. возможность автоматической блокировки адресов при установленном количестве срабатываний запрещающих правил МЭ в течении установленного периода времени; 16.10. разграничение доступа к управлению МЭ на основе ролевой модели управления доступом; 16.11. возможность для администраторов изменения значений по умолчанию, модификации, удаления, добавления содержимого правил МЭ и содержимого профилей МЭ; 16.12. возможность сбора событий, связанных с событиями безопасности и управления МЭ, и запись таких событий в соответствующие журналы; 16.13. возможность выполнять сортировку и поиск данных аудита; 16.14. возможность просмотра списка текущих сетевых соединений с отображением детальной информации по каждому соединению; 16.15. возможность принудительного завершения соединения по команде администратора; 16.16. идентификацию и аутентификацию администраторов и каждого пользователя до разрешения любого действия, выполняемого при посредничестве МЭ от имени этого пользователя; 16.17. фильтрацию SSL/TLS трафика; 16.18. возможность обеспечения перехода в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному режиму функционирования; 16.19. возможность тестирования (самотестирования) функций безопасности МЭ; 16.20. возможность настройки автоматического переключения профилей МЭ при отсутствии на АРМ антивирусов Dr.Web и Kaspersky либо при их деактивации; 16.21. выдачу предупреждающих сообщений при обнаружении возможного нарушения безопасности; 16.22. возможность централизованного управления политиками и правилами МЭ при помощи отдельного кроссплатформенного средства централизованного управления; 16.23. возможность периодического архивирования журналов событий; 16.24. возможность экспорта журналов безопасности в форматы PDF, ODS и XML; 16.25. возможность локального и удаленного администрирования; 16.26. возможность администрирования через графическую или консольную оболочку, функционирующую в операционных системах на базе ядра Linux, а также через графическую оболочку администрирования, функционирующую в операционных системах семейства Windows; 16.27. возможность установки графической и консольной оболочки МЭ из единого файла-установщика; 16.28. возможность проверки корректности функционирования МЭ, самотестирования; 16.29. возможность обновления МЭ с выполнением сохранения ранее произведенных настроек МЭ;	
--	--	--	--

			16.30. возможность настройки всех параметров МЭ из единой консоли администрирования; 16.31. возможность экспортировать и импортировать файлы конфигурации для восстановления настроек МЭ; 16.32. возможность оповещения при событиях. 17. Реализация МЭ должна быть полностью программной. 18. Поставка МЭ должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения с указанием всех необходимых модулей и требуемого количества лицензий по каждому модулю. Вариант формулировки: — неисключительное право на использование МЭ (программное обеспечение). 19. Система обнаружения и предотвращения вторжений (СОВ) должна представлять собой программный модуль средства защиты информации в операционных системах семейства Linux и должна быть предназначена для обнаружения и блокирования основных угроз безопасности информации, выполняя одновременно функции и сетевой, и хостовой системы обнаружения вторжений. 20. СОВ должна быть предназначена для ПЭВМ типа IBM PC под управлением следующих операционных систем семейства Linux в многопользовательском режиме их эксплуатации: — Альт Рабочая Станция 10.0; — Альт Рабочая Станция 10.1; — Альт Рабочая Станция 10.2; — Альт Рабочая Станция 10.4; — Альт Рабочая Станция 10.4; — Альт Рабочая Станция 11; — Альт Сервер 10; — Альт Сервер 11; — Альт 8 СП релиз 10; — Альт 8 СП релиз 10 версия 2; — Astra Linux Special Edition 1.7; — Astra Linux Special Edition 1.8; — РЕД ОС 7.3 Муром; — РЕД ОС 8.0; — МСВСфера АРМ 9; — МСВСфера Сервер 9; — Debian 10; — Debian 11; — Debian 12; — Ubuntu 18.04; — Ubuntu 20.04. 21. СОВ должна поддерживать 64-битные версии операционных систем. 22. СОВ должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах и ТС с поддержкой виртуальных сред.	
--	--	--	--	--

			23. Модуль СОВ должен быть сертифицирован на соответствие требованиям ФСТЭК России к системам обнаружения вторжений по 4-му классу защиты в соответствии с профилем защиты систем обнаружения вторжений уровня узла четвертого класса защиты (ИТ.СОВ.У4.ПЗ). 24. СОВ должна иметь возможность быть использовано: — при создании защищенных автоматизированных систем до класса защищенности 1Г включительно; — в государственных информационных системах до 1 класса защищенности включительно; — в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности включительно; — в информационных системах персональных данных до 1 уровня защищенности включительно; — при защите значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно. 25. СОВ должна обеспечивать: 25.1. обнаружение и блокировку сетевых атак с использованием предустановленных сигнатур и эвристических методов анализа сетевого трафика; 25.2. автоматизированное или ручное обновление базы сигнатур и правил обнаружения вторжений из централизованных или локальных источников; 25.3. настройку параметров СОВ с использованием консольной и графической оболочек администрирования; 25.4. возможность создания, редактирования и управления профилями настроек СОВ, позволяющих изменять параметры в зависимости от уровня угроз; 25.5. блокировку IP-адресов, инициировавших подозрительные действия, с возможностью ручного или автоматического снятия блокировки через заданный период времени; 25.6. хранение и управление журналами событий СОВ с возможностью их экспорта; 25.7. проведение автоматического тестирования (самотестирования) функций системы обнаружения вторжений для проверки её работоспособности; 25.8. возможность запуска ПО в замкнутой программной среде; 25.9. возможность периодического архивирования журналов событий; 25.10. возможность экспорта журналов безопасности в форматы PDF, ODS и XML; 25.11. возможность локального и удаленного администрирования; 25.12. возможность администрирования через графическую или консольную оболочку, функционирующую в операционных системах на базе ядра Linux, а также через графическую оболочку администрирования, функционирующую в операционных системах семейства Windows; 25.13. возможность установки графической и консольной оболочки СОВ из единого файла-установщика; 25.14. возможность проверки корректности функционирования СОВ, самотестирования; 25.15. возможность обновления СОВ с выполнением сохранения ранее произведенных настроек СОВ;	
--	--	--	---	--

			25.16. возможность настройки всех параметров СОВ из единой консоли администрирования; 25.17. возможность экспортировать и импортировать файлы конфигурации для восстановления настроек СОВ; 25.18. возможность оповещения при событиях. 26. Реализация СОВ должна быть полностью программной. 27. Поставка СОВ должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения с указанием всех необходимых модулей и требуемого количества лицензий по каждому модулю. Вариант формулировки: — неисключительное право на использование СОВ (программное обеспечение). Срок действия лицензии – бессрочно. Годовое гарантийное сопровождение.	
4.	Установочный комплект ПО реализующего функции СКН, МЭ, СОВ	Товар, с НДС	Установочный комплект должен состоять из: • компакт-диска с дистрибутивом ПО; • копии сертификата ФСТЭК России на ПО; • формуляра на ПО.	1
5.	Средство доверенной загрузки	Лицензия, без НДС	28. СДЗ УБ должно являться средством доверенной загрузки уровня базовой системы ввода-вывода и представлять собой программно-техническое средство, которое встраивается в базовую систему ввода-вывода и осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы. 29. СДЗ УБ должно выполнять свои функции (включая администрирование параметров изделия и просмотр журнала) до начала загрузки штатной операционной системы (ШОС). 30. СДЗ УБ должно быть предназначено для использования в составе различных технических средств (ТС), в том числе на ноутбуках, моноблоках и серверах, работающих под управлением ОС версий x86-64, поддерживающих наиболее распространенные файловые системы, включая FreeBSD UFS/UFS2, Solaris UFS, FAT16, FAT32, NTFS, Ext2, Ext3, Ext4, VMFS3. 31. СДЗ УБ должно поддерживать аппаратную идентификацию при помощи аппаратных ключей и смарт-карт: – USB-ключей и смарт-карт Aladdin (Aladdin eToken Pro/Java); – USB-ключей и смарт-карт Рутокен (Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0, Рутокен Lite); – электронных ключей Touch Memory (iButton); – USB-ключей и смарт-карт ESMART (ESMART Token, ESMART Token ГОСТ); – USB-ключей и смарт-карт eSmart (ESMART Token, ESMART Token ГОСТ); – USB-ключей и смарт-карт JaCarta (JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta PKI); – USB-ключи Guardant ID 2.0. 32. СДЗ УБ должно разрабатываться и производиться на основании лицензии федеральных органов, имеющих полномочия в указанной сфере. 33. СДЗ УБ должно быть сертифицировано на соответствие: 33.1. требованиям документа «Требования по безопасности информации,	1

		устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020 г.) по 2 уровню доверия; 33.2. требованиям документов «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013 г.) и «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты» ИТ.СДЗ.УБ2.ПЗ (ФСТЭК России, 2013 г.). 34. СДЗ УБ может быть использовано при создании: – защищенных автоматизированных систем до класса защищенности 2А включительно (1Б включительно); – защищенных государственных информационных систем до 1 класса защищенности включительно; – защищенных автоматизированных систем управления производственными и технологическими процессами до 1 класса защищенности включительно; – защищенных информационных систем персональных данных до 1 уровня защищенности включительно; – защищенных значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно. 35. В СДЗ УБ должна быть обеспечена автоматическая проверка целостности контролируемых объектов, осуществляемая после авторизации пользователя в изделии и по запросу уполномоченного пользователя. Должен быть реализован вывод результатов контроля загрузчика ШОС в окно проверок после авторизации пользователя. 36. СДЗ УБ должно иметь механизм тестирования (самотестирования) критичных функций безопасности. 37. В СДЗ УБ должен быть реализован программный «сторожевой таймер». 38. Управление СДЗ УБ должно осуществляться через удобную графическую оболочку. 39. СДЗ УБ должен поддерживать возможность установки средствами программатора на технические средства, на которых невозможна программная установка. 40. СДЗ УБ должен включать утилиту для автоматизированного создания раздела, предназначенного для ее работы, с поддержкой как физических, так и логических разделов (LVM). 41. В комплект СДЗ УБ должна входить UEFI-утилита, выполняющая тестирование и оценку совместимости с ТС перед установкой. 42. СДЗ УБ должно обеспечивать: 42.1. блокирование загрузки ОС при выявлении попыток загрузки нештатной ОС; 42.2. блокирование загрузки ОС при превышении числа неудачных попыток аутентификации пользователя; 42.3. блокирование загрузки ОС при нарушении целостности изделия, загружаемой программной среды, состава аппаратных компонентов; 42.4. блокирование загрузки ОС при критичных типах сбоев и ошибок, для которых требуется аварийная поддержка и восстановление;	
--	--	---	--

			42.5. возможность сохранения в файл (на носитель информации) и последующего восстановления из файла конфигурации СДЗ УБ (выбор параметров сохранения конфигурации); 42.6. выбор алгоритма расчета контрольной суммы из CRC32, ГОСТ Р 34.11-94, MD5 для объектов ФС, реестра, областей жесткого диска, программного обеспечения СДЗ УБ. 42.7. очистка оперативной памяти ТС при перезагрузке с целью исключения возможности доступа к ресурсам изделия и памяти ТС после завершения работы изделия; 42.8. идентификацию и аутентификацию пользователя до выполнения действий по загрузке ОС или администратора до выполнения действий по управлению СДЗ УБ; 42.9. возможность регистрации (заведения) пользователей различных ролей (категорий учетных записей пользователей — «Администратор», «Аудитор», «Пользователь»); 42.10. возможность авторизации в СДЗ УБ с использованием доменных учетных записей: Microsoft Active Directory, FreeIPA, Samba, РЕД АДМ, ALD Pro; 42.11. возможность определить минимальную длину пароля для учетных записей пользователей не менее 8 символов; 42.12. настройку сложности паролей: необходимость наличия специальных символов, наличия строчных и прописных букв в пароле, отсутствия цифр в первом и последнем символах пароля; 42.13. блокировку учетной записи пользователя при превышении количества попыток авторизации, предусмотренных настройками; 42.14. работу со списком заблокированных пользователей (возможность просмотра списка заблокированных пользователей и разблокировка конкретного пользователя или всех пользователей одновременно); 42.15. возможность использования при авторизации пользователя как идентификационной, так и аутентификационной информации, записанной на аппаратном идентификаторе пользователя; 42.16. возможность установки принудительной двухфакторной идентификации; 42.17. возможность управления аппаратными идентификаторами; 42.18. возможность установки ограничений на время действия аутентификационной информации пользователя. При превышении ограничений авторизация в СДЗ УБ должна быть невозможна; 42.19. возможность установления «расписания» работы пользователя; 42.20. контроль целостности загружаемой ОС (объектов файловой системы, областей жесткого диска, реестра) и блокировку загрузки ОС при нарушении целостности контролируемых объектов; 42.21. контроль состава компонентов аппаратного обеспечения ТС и блокировку загрузки ОС при обнаружении несанкционированного изменения состава аппаратных компонентов ТС; 42.22. контроль целостности ПО, в том числе BIOS (CMOS), SMBIOS, и компонентов ТС; 42.23. контроль целостности ПО СДЗ УБ; 42.24. возможность настройки списка контролируемых объектов; 42.25. регистрацию событий доверенной загрузки ТС в журнале событий СДЗ УБ;	
--	--	--	--	--

			42.26. возможность хранения в журналах аудита до 30 000 записей; 42.27. возможность экспорта журналов безопасности в форматы CSV, HTML, XML; 42.28. возможность выборочного просмотра данных аудита; 42.29. возможность просмотра записи журнала событий доверенной загрузки в отдельном окне; 42.30. самодиагностику и реакцию на выявление критических сбоев (отображение информационного сообщения и выключение ТС); 42.31. возможность сформировать отчет о текущей конфигурации в формате txt или html; 42.32. возможность сформировать паспорт аппаратного обеспечения рабочей станции (система, оперативная память, PCI-устройства, накопители, USB-устройства); 42.33. возможность принудительно задать загрузочное устройство; 42.34. поддержку двух и более сетевых карт с возможностью выбрать ту, через которую должна осуществляться связь с модулем централизованного управления; 42.35. возможность централизованного управления СДЗ УБ на ТС с помощью дополнительного программного модуля, установленного на отдельном ТС под управлением ОС семейств Windows или Linux, который обеспечивает (в части СДЗ УБ): - возможность ввода/вывода клиента в/из домена безопасности; - сбор журналов аудита в единую систему хранения программного модуля или базу данных; - отображение текущего статуса/состояния клиента СДЗ УБ; - синхронизация политик/учетных записей; - выполнение заданий от программного модуля (получение отчетов, сохранение и применение конфигураций на клиенте, тестирование функций СДЗ УБ); - включение/выключение/перезагрузка клиента; - разблокировка учетных записей; - сигнализация о событиях НСД в реальном времени; - запись в память токенов информации о пользователе в формате, поддерживаемом СДЗ УБ. 42.36. возможность перезагрузки удаленной рабочей станции с установленным СДЗ УБ посредством программного модуля централизованного управления. 43. Поставка СДЗ УБ должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения. Вариант формулировки: неисключительное право на использование Средства доверенной загрузки уровня базовой системы ввода-вывода (программное обеспечение). Срок действия лицензии – бессрочно. Электронная версия.	
6.	Антивирусная защита	Лицензия, без НДС	Наименование: Система антивирусной защиты (далее - Система) 1 Общие требования 1.1 Участники конкурса на использование антивирусного программного продукта должны иметь статус официального партнера компании производителя, что является подтверждением их квалификации и прав на поставку антивирусных продуктов и/или лицензий. При заключении контракта необходимо предоставить копии документов, подтверждающих статус официального партнера компании производителя.	5

			1.2 Участник должен принять во внимание, что ссылка на наименование продукции носит описательный, а не обязательный характер. В случае если Участником предлагаются эквивалент требуемого Заказчиком ПО, то в составе своей конкурсной заявки он должен в обязательном порядке предоставить следующую информацию: 1.2.1 в Техническом предложении – подробное техническое описание предлагаемого к поставке эквивалента, с указанием полного соответствия (или превосходящего) всем техническим характеристикам, указанным в данной спецификации, заверенное у производителя предлагаемого программного продукта Отсутствие в составе конкурсной заявки подробного технического описания аналогов продукции и/или письма о согласовании может являться причиной отклонения конкурсной заявки Участника. 1.3 Все компоненты Системы должны принадлежать одной торговой марке с единой службой технической поддержки на русском языке. Техническая поддержка должна предоставляться непосредственно производителем поставляемых программных продуктов. 1.4 В рамках всей организации должны использоваться единые антивирусные средства независимо от степени конфиденциальности обрабатываемой информации. Отдельно стоящие ПК, не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от проникновения и активации всех типов вредоносных программ (антивирус), спама (персональный антиспам) и обеспечивать возможность их включения в единую систему антивирусной защиты. 1.5 Поставляемые средства защиты должны представлять масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети заказчика. 1.6 Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке. 1.7 Все антивирусные средства, функционирующие под операционной системой типа Windows, включая средства управления, должны обладать контекстной справочной системой на русском языке. 1.8 Участник конкурса должен предоставить единый серийный номер для всех поставляемых по условиям конкурса продуктов. 1.9 Поставляемый серийный номер должен иметь возможность отложенной активации. Срок действия лицензионных ключевых файлов на все поставляемые по условиям конкурса программные продукты должен начинаться с момента активации серийного номера. 1.10 Система лицензирования не должна иметь привязку к используемому на защищаемых объектах аппаратному обеспечению. Система должна позволять перенос лицензий с одних защищаемых объектов (в том числе рабочих станций и серверов) на иные без необходимости перепривязки или получения дополнительных лицензий 1.11 Антивирусные средства должны включать: • программные средства защиты рабочих станций; • программные средства защиты файловых серверов;	
--	--	--	--	--

			• программные средства защиты почтовых серверов; • программные средства защиты почтовых шлюзов; • программные средства защиты интернет шлюзов; • программные средства централизованного управления, мониторинга и обновления; • обновляемые базы данных сигнатур вредоносных программ всех типов и атак; • эксплуатационную документацию на русском языке. 2. Требования к программным средствам 2.1. Общие требования к системе антивирусной защиты 2.1.1. Программные средства Системы должны обеспечивать определение угроз следующих типов: 2.1.1.1. классических вирусов; 2.1.1.2. троянских программ; 2.1.1.3. руткитов; 2.1.1.4. сетевых червей; 2.1.1.5. рекламных программ; 2.1.1.6. программ автодозвона на платные сайты; 2.1.1.7. потенциально опасных приложений; 2.1.1.8. прочих вредоносных программ. 2.1.2. Антивирусная защита должна обеспечивать: 2.1.2.1. обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE и т.п.; 2.1.2.2. обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками; 2.1.2.3. обнаружение вирусов внутри контейнеров и архивных файлов формата ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (включая NRG, образы с нестандартным форматом сектора и не имеющие сигнатур), ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER с зашифрованными контейнерами и т.д. без ограничений на уровень вложенности проверяемых объектов; 2.1.2.4. обнаружение вирусов внутри контейнеров, не имеющих строгого формата (HTML, MIME); 2.1.2.5. обнаружение вирусов внутри контейнеров с нечетким значением размера объекта (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES и т.д.); 2.1.2.6. антивирусную проверку файлов и объектов, имеющих формат SmartInstallMaker (SIM); DMG, HFS, XAR, UniversalBinary (MacOS); SIS (Symbian 9); INNOSETUP (5.3.9 и выше); SETUPFACTORY (линейки 7,8); XENOCODE; TARMAINSTALL (линейка 3); XZ (UNIX); COMPRESS; SQUAHFS; CHILKATZIP; пакеты LHA (AWARDBIOS); 2.1.2.7. антивирусную проверку самораспаковывающихся архивов: AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy; 2.1.2.8. проверку исполняемых файлов, упакованных следующими упаковщиками: PELOCK,	
--	--	--	---	--

		ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT, атакжепочтовыхфайлов Mozilla Thunderbird-внезависимостиотихразмера; 2.1.2.9. разбор неформатированных почтовых баз и обработка писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW), поддержка формата TNEF; 2.1.2.10. защиту от вредоносных программ,принадлежащих семействам вредоносных программ, информация о которых имеется в антивирусных базах, созданных после занесения соответствующей информации в антивирусные базы и еще не попавших на анализ в антивирусные лаборатории - как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле; 2.1.2.11. обнаружение вредоносных объектов в HTML- и PDF-документах, включая обфусцированные эксплойты в JavaScript, находящиеся в документах данных типов. Возможностьизвлечения и анализа «невидимых» IFRAME-элементов. Возможностьизвлечения для проверки скриптов любой сложности и снятие с них защиты; 2.1.2.12. обнаружение угроз по лицензионным данным (ASPROTECT, PEP и ENIGMA); 2.1.2.13. обнаружение угроз направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля 2.1.2.14. обнаружение вредоносных объектов в DEX-файлах (Android). 2.1.3. Используемое антивирусное ядро: 2.1.3.1. не должно допускать снижение скорости проверки при увеличении размера антивирусных баз; 2.1.3.2. в связи с возможностью исчерпания ресурсов ОС (в том числе места на диске, памяти) в ходе обработки специальным образом сформированных архивов автоматически выбирать уровень анализа упакованных объектов, а также механизм уменьшения размера промежуточных файлов. При выборе уровня анализа должен учитываться уровень загрузки системы 2.1.3.3. в целях ускорения проверки архивов и упакованных файлов должно обеспечивать опознание вредоносных программ без запуска распаковщика; 2.1.3.4. должно обеспечивать защиту от так называемых «почтовых бомб»; 2.1.3.5. должно обеспечивать работу с файлами размером как менее, так и больше 2 ГБ; 2.1.3.6. должно поддерживать работу с дисками с LBA-адресацией; 2.1.3.7. в целях исключения «утечки» оперативной памяти должно использовать механизм распределениядинамической памяти уровня антивирусного ядра. 2.2. Требования к системе управления антивирусной защитой (далее - Сервер управления) 2.2.1. Система управления должна быть построена по клиент-серверной архитектуре с возможностью построения иерархической системы серверов – с возможностью использования в системе антивирусного управления как главных, так подчиненных серверов.	
--	--	---	--

		2.2.2. Система управления должна быть реализована на основе Web-интерфейса, поддерживающего Web-браузеры, используемые как в корпоративной сети, так и Web-браузеры, используемые на устройствах и компьютерах, имеющих доступ к сервисам управления антивирусной защитой извне корпоративной сети - в том числе Mozilla Firefox или Internet Explorer. Управление через данные браузеры должно быть доступно с любых ОС, имеющих возможность их установки и запуска. 2.2.3. Система должна включать поддержку кластерного протокола, с помощью которого координируются действия над агентами защиты с разных антивирусных серверов 2.2.4. Система управления должна быть доступной с любой операционной системы, поддерживающей браузеры Mozilla Firefox или Internet Explorer (в том числе с ОС Microsoft Windows и ОС типа UNIX (Linux, FreeBSD, Solaris)), без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения как на стороне сервера управления, так и на стороне администратора Системы. Контроль работы Системы должен быть также возможен консоли управления, функционирующей на мобильных устройствах iPhone 2.2.5. В целях безопасности все ПО, входящее в состав антивирусного сервера (в том числе необходимое для доступа с помощью браузера) должно поставляться в виде единого дистрибутива и принадлежать одной торговой марке. 2.2.6. Система управления должна включать систему управления лицензиями, позволяющую распределять между серверами в рамках иерархической сети необходимое количество лицензий 2.2.7. Установка антивирусного сервера Системы, сертифицированного на соответствии требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна быть возможна на: 2.2.7.1. Microsoft Windows Server 2003; 2.2.7.2. Microsoft Windows Server 2008; 2.2.7.3. Microsoft Windows Server 2012; 2.2.7.4. Microsoft Windows Server 2016; 2.2.7.5. Microsoft Windows 7; 2.2.7.6. Microsoft Windows 10; 2.2.7.7. FreeBSD 10; 2.2.7.8. Debian GNU/Linux 7; 2.2.7.9. RedHat Enterprise Linux 6; 2.2.7.10. Ubuntu 14; 2.2.7.11. CentOS 6; 2.2.7.12. CentOS 7; 2.2.7.13. AstraLinux 1.7, 1.8. 2.2.8. Система управления должна иметь возможность: 2.2.8.1. просмотра и сравнения состава аппаратно-программного обеспечения на станциях антивирусной сети 2.2.8.2. контроля неактивных станций антивирусной сети	
--	--	---	--

		2.2.8.3. просмотра сессий пользователей антивирусной сети 2.2.8.4. замены системного DNS 2.2.8.5. использования как внутренней СУБД (поставляемой в составе дистрибутива антивирусного сервера), так и внешней (устанавливаемой отдельно до или после развертывания антивирусного сервера). При использовании внешней СУБД Система должна иметь возможность работы с ней как без установки дополнительного ПО (с СУБД MS SQL, Oracle), так и с помощью драйверов ODBC для операционных систем Windows и Linux (в том числе с СУБД PostgreSQL). Система должна иметь возможность замены типа используемой СУБД после установки серверной части – без необходимости переустановки серверной части Системы 2.2.8.6. управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа, выполнения произвольных SQL-запросов 2.2.8.7. экспорта и импорта базы данных антивирусного сервера в XML-файл. 2.2.8.8. создания иерархической сети антивирусных серверов. В случае реализации иерархической сети Система должна иметь возможность: 2.2.8.8.1. объединения информации от нескольких серверов на одном. 2.2.8.8.2. распределения рабочих станций между серверами для получения обновлений в целях снижения общей нагрузки на сеть. 2.2.8.8.3. обмена статистикой в рамках одной иерархической сети между антивирусными серверами различных версий 2.2.8.8.4. контроля отсутствия связанных серверов в расписании антивирусного сервера. 2.2.8.9. построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне; 2.2.8.10. установки антивирусных агентов в сети, не использующей единого пароля доступа к рабочим станциям; 2.2.8.11. централизованной настройки параметров защиты, уникальных для различных групп, в том числе для рабочих станций, находящихся в режиме off-line. 2.2.8.12. централизованного сбора и просмотра статистической информации и создания отчетов о состоянии антивирусной защиты и их консолидации; 2.2.8.13. интеграции в системы управления и информационные системы с помощью встроенного в систему API 2.2.8.14. наличия множественных путей уведомления пользователей и администраторов путем отправки почтового сообщения, звукового оповещения, всплывающего окна, записи в журнал событий, SNMP-trap; 2.2.8.15. оповещения о возникновении эпидемий (множественных инфекций) 2.2.8.16. оповещения о наличии обновлений сервера 2.2.8.17. отправки информационных сообщений пользователям по сети в режиме реального времени через Web-интерфейс Системы; 2.2.8.18. обеспечения связи антивирусного сервера и клиентских частей через встроенный модуль в случае, когда они расположены в различных сетях, работающих по протоколам TCP/IP	
--	--	---	--

		(в т.ч. IPv6), между которыми отсутствует маршрутизация пакетов 2.2.8.19. самостоятельного написания обработчиков событий на языке Lua, а также выполнения произвольных Lua-скриптов с помощью средств системы управления. 2.2.9. В случае интеграции с внешними подсистемами с помощью встроенного Web API, должна иметься возможность аудита действий, произведенных с помощью функций данного Web API 2.2.10. Вне зависимости от типа антивирусного агента и защищаемой системы, Система должна обеспечивать реализацию следующих функциональных возможностей 2.2.10.1. экспорта, импорта и распространения конфигураций групп, станций антивирусной сети или компонентов антивирусной защиты на другие группы, станции и компоненты, в том числе в целях изменения политик, применения их к определенным группам 2.2.10.2. скачивания конфигурационных файлов с настройками подключения антивирусных агентов для ОС Android, Mac OS X и ОС семейства UNIX 2.2.10.3. восстановления рабочих станций, случайно удаленных из системы защиты; 2.2.10.4. централизованного обновления антивирусных баз на всех защищенных рабочих станциях, в том числе мобильных и находящихся в режиме off-line. Доставки обновлений на рабочие места пользователей как по расписанию, так сразу после их получения; 2.2.10.5. обновления программных средств и антивирусных баз из разных источников, доставляемые как автоматически по каналам связи в пределах антивирусной сети, так и на отчуждаемых машинных носителях информации – путем ручной синхронизации информации между серверами и рабочими станциями 2.2.10.6. обновления программных средств и антивирусных баз с помощью мобильного сервера обновлений, представляющего собой Сервер управления, развернутый на flash-диске; 2.2.10.7. управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая откат обновлений 2.2.10.8. контроля результатов обновления антивирусного ПО на станциях антивирусной сети. 2.2.10.9. организации межсерверного обмена согласно расписанию 2.2.10.10. ограничения канала связи по группам 2.2.10.11. наличия возможности групповых обновлений 2.2.10.12. обновлений по защищенному каналу с использованием SSL-сертификатов 2.2.10.13. организации отложенного обновления 2.2.10.14. проверки обновлений на выбранных администратором компьютерах/группах перед распространением их на все клиентские компьютеры 2.2.10.15. автоматического перехода установленного ПО на более новые версии, в том числе с возможностью выбора обновляемых компонентов; 2.2.11. Программные средства управления для всех защищаемых ресурсов, реализованных на платформах ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей: 2.2.11.1. централизованной удаленной установки и деинсталляции программных средств, антивирусных баз и антивирусного ядра на защищаемые узлы сети – в том числе на	
--	--	--	--

		станции, находящиеся в разных доменах. 2.2.11.2. создания инсталляционных пакетов для конкретных защищаемых рабочих станций; 2.2.11.3. выбора и настройки устанавливаемых компонентов до начала установки антивирусного пакета на клиентские части; 2.2.12. Система должна обладать специальной политикой для мобильных пользователей (ноутбуки), при применении которой, мобильные пользователи должны иметь возможность редактирования настроек антивирусного пакета и обновления через Интернет при отсутствии доступа к антивирусному серверу. Применение политики должно происходить через Web-интерфейс, без необходимости использования файлов конфигурации типа *.xml. 2.2.13. Система управления должна поддерживать возможность: 2.2.13.1. создания точки восстановления перед установкой антивирусного пакета на защищаемые рабочие станции и сервера; 2.2.13.2. восстановления удаленных станций. 2.2.14. Система должна поддерживать множественную возможность установки своих компонентов на защищаемые рабочие станции – в том числе с помощью: 2.2.14.1. прямого их указания в системе управления в результате сканирования локальной сети, Microsoft Active Directory, 2.2.14.2. политик Microsoft Active Directory 2.2.14.3. установки с помощью дистрибутива, содержащего все компоненты защиты 2.2.14.4. рассылки инсталляционных файлов из системы управления по электронной почте 2.2.14.5. возможностей службы распределенной файловой системы (DFS). 2.2.15. Система должна поддерживать возможность настройки правил автоматического распределения станций по пользовательским группам, а также возможность изменения первичной группы при автоматическом подтверждении доступа станций к антивирусному серверу 2.2.16. Система управления должна обладать возможностью встроенного автоматического резервного копирования критически важных данных и конфигурации антивирусного сервера по заранее заданному расписанию, а также опцию восстановления сервера из резервной копии без использования файлов конфигурации типа *.xml. 2.2.17. Система должна иметь возможность минимизации трафика: 2.2.17.1. за счет применения специальных алгоритмов сжатия; 2.2.17.2. ограничения трафика по пропускной способности и по времени в определенных IP-подсетях. 2.2.18. Система должна иметь возможность интеграции с платформой Microsoft® Network Access Protection (NAP), обеспечивающей автоматическую систему реагирования на инциденты безопасности. 2.2.19. Система должна иметь возможность выбора уровня подробности протоколирования своих компонентов. система управления должна иметь возможность загрузки архивированных файлов журнала работы всех антивирусных серверов иерархической сети 2.2.20. В целях ограничения использования серверного пространства должна иметься	
--	--	---	--

			возможность ротации файлов журнала антивирусного сервера по времени (час, день, неделя) 2.2.21. Система управления должна обеспечивать защиту от несанкционированного доступа. Авторизация должна обеспечиваться парой логин/пароль. 2.2.22. Администраторы Системы должны иметь возможность авторизации с помощью ActiveDirectory, LDAP, RADIUS, PAM. Система управления должна иметь возможность предварительного тестирования настроек авторизации внешних администраторов Active Directory, LDAP и RADIUS 2.2.23. Система должна иметь журнал аудита действий администраторов Системы, позволяющий просматривать журнал событий и изменений, осуществленных администраторами при помощи системы управления. 2.2.24. Система должна обеспечивать: 2.2.24.1. возможность экспорта выбранных файлов из карантина рабочей станции и/или файлового сервера на антивирусный сервер для дальнейшего анализа; 2.2.24.2. возможность задания групповых политик в зависимости от группы IP-адресов. 2.2.24.3. возможность просмотра новостей безопасности, в том числе информирующих об актуальных угрозах 2.2.25. В случае включения какого-либо компонента Системы в единую систему управления антивирусной защиты локальной сети: 2.2.25.1. обновления компонента Системы должны происходить через сервер обновления системы управления антивирусной защиты; 2.2.25.2. статистика работы компонентов Системы должна: 2.2.25.2.1. собираться на сервере системы управления антивирусной защиты; 2.2.25.2.2. быть доступной с любой операционной системы, поддерживающей браузеры Mozilla Firefox, Internet Explorer, Safari, Opera без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения за исключением устанавливаемого автоматически с антивирусного сервера модуля, необходимого для отображения статистики. 2.2.25.2.3. Иметь возможность экспорта в формат PDF 2.2.25.2.4. Иметь возможность отправки по электронной почте согласно расписанию работы антивирусного сервера 2.2.26. Система должна обеспечивать реализацию следующих функциональных возможностей по обновлению: 2.2.26.1. получения ежедневных обновлений вирусных баз не менее 10 раз в сутки независимо от того, рабочий, либо выходной день, что должно подтверждаться созданным Системой отчетом (файлом протокола). Система также должна поддерживать возможность получения экстренных обновлений, связанных с выходом новых типов вредоносного ПО, а также возможность мгновенного распространения этих обновлений; 2.2.26.2. возможность множественности путей обновления, в том числе по каналам связи и на съемных электронных носителях информации; 2.2.26.3. возможность обновления через прокси-серверы, в том числе прокси-серверы MS	
--	--	--	---	--

		ISA/TMG. 2.2.26.4. проверка целостности и подлинности обновлений средствами электронной цифровой подписи. 2.2.26.5. обновления компонентов и вирусных баз по защищенному каналу, с использованием протокола HTTPS. 2.2.27. В случае размещения антивирусных серверов во внутренней сети без доступа к сети Интернет получение обновлений должно быть возможно с помощью специальной утилиты автономной загрузки репозитория; 2.2.28. Система должна иметь возможность перезагрузки защищаемой станции через систему управления 2.2.29. Система должна иметь возможность шифрования трафика между серверами и защищаемыми рабочими станциями в целях предотвращения утечки конфиденциальной информации. 2.3. Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows 2.3.1. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей: 2.3.1.1. осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях. 2.3.2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов: 2.3.3. Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию ПО, сертифицированного на соответствии требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна обеспечивать защиту рабочих станций под управлением операционных систем: 2.3.3.1. Microsoft Windows XP Professional; 2.3.3.2. Microsoft Windows 7; 2.3.3.3. Microsoft Windows 8.1; 2.3.3.4. Microsoft Windows 10. 2.3.4. Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки. 2.3.5. Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур. 2.3.6. Система должна поставляться в конфигурации, обеспечивающей антивирусную	
--	--	---	--

		защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов. 2.3.7. В случае наличия системы централизованного управления права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля. 2.3.8. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках имеющихся у них прав. 2.3.9. В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов. 2.3.10. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы. 2.3.11. Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях: 2.3.11.1. поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера; 2.3.11.2. непрерывное фоновое сканирование в целях нейтрализации активных угроз 2.3.11.3. проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора; 2.3.11.4. проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам; 2.3.11.5. блокировку опасных макросов VBA в реальном времени; 2.3.11.6. защиту от вредоносных сценариев, загружаемых с Web-страниц; 2.3.11.7. защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевого экрана; 2.3.11.8. проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО; 2.3.11.9. защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе отдельным типам сменных	
--	--	---	--

		носителей информации, локальным файлам и каталогам, сайтам в сети Интернет; 2.3.11.10. ограничения доступа к сети Интернет или к компьютеру в определенный момент времени по расписанию 2.3.11.11. помещение найденных зараженных файлов в специальное место на жестком диске -«карантин»; 2.3.11.12. просмотр местоположения станций и серверов на карте, если заданы географические координаты станции 2.3.11.13. автоматический запуск антивирусного программного обеспечения и других необходимыхкомпонентов вместе с загрузкой ОС; 2.3.11.14. запуск задач по расписанию и/или сразу после загрузки операционной системы; 2.3.11.15. возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке. 2.3.12. Система защиты рабочих станций должна обеспечивать проверку протоколов: 2.3.13. HTTP; 2.3.14. IMAP, SMTP, POP3 независимо от используемого почтового клиента; 2.3.15. NNTP (только проверка на вирусы), независимо от почтового клиента. 2.3.16. Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством: 2.3.17. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию; 2.3.18. проверки объектов«на лету», при доступе к ним с помощью антивирусной резидентной программы. 2.3.19. В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы. 2.3.20. Система должна обеспечивать защиту от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) с помощью превентивной защиты, отслеживающей попытки внедрения вредоносных файлов 2.3.21. В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения. 2.4. Требования к программным средствам антивирусной защиты рабочих станций и домашних компьютеров под управлением ОС семейства Microsoft Windows, не входящих в систему централизованного управления 2.4.1. Программные средства системы защиты (далее Системы) должны обеспечивать реализацию следующих функциональных возможностей:	
--	--	---	--

			2.4.1.1. осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях; 2.4.1.2. создание резервных копий папок, указанных пользователем, а также восстановление данных из хранилища - в том числе самим пользователем. 2.4.2. Система, используя актуальную на момент проведения тендера версию ПО, сертифицированного на соответствиетребованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна обеспечивать защиту рабочих станций под управлением операционных систем: 2.4.2.1. Microsoft Windows XP; 2.4.2.2. Microsoft Windows 7; 2.4.2.3. Microsoft Windows 8.1; 2.4.2.4. Microsoft Windows 10. 2.4.3. В целях противодействия вредоноснымпрограммам, блокирующим запуск известногоПО - для установки системы защиты не должнатребоваться установка стороннего инсталлятора - включая Microsoft Windows Installer, либо использование служб, дополнительных к ранее используемым. 2.4.4. В связи с необходимостью автоматизации развертывания системы защиты установка должна быть возможна в том числе в режиме командной строки - указанием необходимых параметров установки. В том числе установки в фоновом режиме, необходимости перезагрузки и состава устанавливаемых компонент; 2.4.5. В связи с возможными ограничениями канала доступа в сеть Интернет установка системы защиты должна быть возможной без доступа в сеть Интернет - дистрибутив должен содержать все компоненты системы защиты, а также базы данных признаков вредоносных программ и вредоносных ресурсов сети Интернет, доступ к которым может регулироваться системой защиты. 2.4.6. Для работы системы защиты не должны использоваться внешние библиотеки, а также среда .Net Framework, целостность которых не находится под контролем системы самозащиты и компрометация которых может привести к ошибкам отображения информации системы защиты или иным проблемам, связанным с интерфейсом системы защиты 2.4.7. С целью противодействия вредоносным программам, запущенным на компьютере, система установки должна быть интегрирована с антируткитом - обнаружение и удаление угроз должно быть доступно во время установки. 2.4.8. Система установки должна поддерживать импорт настроек, содержания карантина и хранилища резервных копий папок, сохраненных после удаления ранее установленного антивируса - в случае наличия совместимости версий. 2.4.9. Дистрибутив, использованный для установки, должен после завершения установки использоваться для автоматического восстановления работы сервисов. В целях поддержания дистрибутива в актуальном состоянии должно быть реализовано инкрементированное обновление установочного пакета. В целях исключениянеправомерного доступа к дистрибутиву в целях удаления или изменения доступ должен контролироваться системой самозащиты	
--	--	--	--	--

		антивирусной Системы. 2.4.10. Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки. 2.4.11. Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур. 2.4.12. Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов. 2.4.13. В случае наличия системы централизованного управления права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля. 2.4.14. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках имеющихся у них прав. 2.4.15. Обновление системы защиты должно быть возможно (по выбору администратора системы защиты) с серверов компании поставщика системы защиты, размещенных в сети Интернет, локальной или сетевой папки, компьютеров локальной сети, на которых установлена аналогичная система защиты и создано зеркало обновлений; 2.4.16. В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов. 2.4.17. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы. 2.4.18. По умолчанию система защиты должна работать в так называемом пользовательском (ограниченном) режиме. Пользователю системы, не являющемуся администратором защиты, не должны быть доступны настройки компонентов системы защиты, а также возможность отключения системы защиты. При работе в данном режиме в интерфейсе системы защиты не должны показываться пункт меню или иконка, нажатие на которые открывает окно или раздел	
--	--	---	--

		интерфейса с настройками системы защиты. Администратор должен иметь возможность ограничить доступ к настройкам с помощью пароля; 2.4.19. Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях: 2.4.19.1. поиск и удаление вредоносных программ всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера; 2.4.19.2. обнаружение вредоносных программ, не обнаруживаемых средствами антивирусного ядра, с помощью превентивной защиты, отслеживающей поведение запущенных процессов, а также вредоносных объектов, внедренных в запущенные процессы; 2.4.19.3. проверки ссылок на видоизменение, скрипты и фреймы; 2.4.19.4. проверки файлов по ссылкам до скачивания из сети Интернет на локальный компьютер; 2.4.19.5. проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора; 2.4.19.6. выявления вредоносных объектов в HTML- и PDF-документах; 2.4.19.7. выявления и анализа «невидимых» IFRAME-элементов на страницах сайтов и HTML-документах; 2.4.19.8. проверку всех скриптов, обрабатываемых в Microsoft InternetExplorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам; 2.4.19.9. блокировку опасных макросов VBA в реальном времени; 2.4.19.10. блокировку перехода по внешним ссылкам в социальных сетях; 2.4.19.11. защиту от вредоносных сценариев, загружаемых с Web-страниц; 2.4.19.12. защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевого экрана; 2.4.19.13. проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО; 2.4.19.14. защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе отдельным типам сменных носителей информации, локальным файлам и каталогам, сайтам в сети Интернет; 2.4.19.15. помещение найденных зараженных файлов, а также резервных копий объектов, к которым были применены действия, отличные от «Поместить в карантин», в специальное место на жестком диске -«карантин»; 2.4.19.16. просмотр местоположения станций и серверов на карте, если заданы географические координаты станции; 2.4.19.17. автоматический запуск антивирусного программного обеспечения и других необходимыхкомпонентов вместе с загрузкой ОС; 2.4.19.18. запуск задач по расписанию и/или сразу после загрузки операционной системы;	
--	--	--	--

			2.4.19.19. возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке 2.4.19.20. защиту возникновения претензий от правообладателей контента путем использования специальной базы данных признаков ресурсов, доступ к которым ограничен по требованию правообладателей. 2.4.20. Администратор системы должен иметь возможность: 2.4.20.1. настройки правил защиты от намеренных/непреднамеренных действий посредством блокировки доступа к локальным и сетевым ресурсам (локальным файлам и каталогам, сайтам в сети Интернет) для конкретных пользователей; 2.4.20.2. копировать настройки между учетными записями пользователей; 2.4.20.3. запрещать возможность отправки заданий на печать; 2.4.20.4. запрещать возможность передачи данных по сети; 2.4.20.5. запрещать возможность изменения системного времени и часового пояса; 2.4.20.6. отключать ранее заданные ограничения для конкретной учетной записи; 2.4.20.7. назначать месторасположения карантина при обнаружении зараженных файлов на съемных носителях; 2.4.20.8. используя возможности менеджера карантина, осуществлять повторную проверку объектов, помещенных в карантин; 2.4.20.9. иметь возможность очистки карантина для отдельного диска. 2.4.21. Система защиты рабочих станций должна обеспечивать проверку протоколов: 2.4.21.1. HTTP независимо от используемого браузера или иного приложения, получающего трафик; 2.4.21.2. IMAP, SMTP, POP3 независимо от используемого почтового клиента; 2.4.21.3. NNTP (только проверка на вирусы), независимо от почтового клиента. 2.4.22. Система защиты рабочих станций должна обеспечивать проверку почтовых сообщений, передаваемых по протоколу MAPI для Microsoft Outlook 2000 (Outlook 9)/2002 (Outlook 10 или Outlook XP)/2003 (Outlook 11)/2007/2010/2013. 2.4.23. Система защиты рабочих станций должна автоматически обеспечивать проверку трафика передаваемого по поддерживаемым системой защиты протоколам: 2.4.23.1. вне зависимости от порта, через который передается трафик - без необходимости указания списка проверяемых портов для конкретных протоколов; 2.4.23.2. включая проверку трафика, передаваемого по зашифрованному соединению SSL. 2.4.24. Система защиты рабочих станций должна обеспечивать фильтрацию трафика в мгновенных сообщениях Mail.Ru Agent, ICQ, Jabber, QIP, Pidgin и другие, включая антивирусную проверку пересылаемых вложений, а также автоматическое удаление из сообщений ссылок, ведущих на вредоносные и фишинговые сайты. 2.4.25. Система защиты рабочих станций должна обеспечивать фильтрацию выдачи результатов поисковых систем Google, Yandex, Yahoo!, Bing, Rambler с показом только безопасных с точки зрения поисковых систем и системы защиты ресурсов. 2.4.26. Система должна обеспечивать проверку файлов и системных областей на предмет	
--	--	--	---	--

		наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством: 2.4.26.1. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию; 2.4.26.2. проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы; 2.4.26.3. непрерывного фонового сканирования и нейтрализации активных угроз. В том числе в критических областях Windows, оперативной памяти, запущенных процессах, MBR/VBR дисков, BIOS; 2.4.26.4. проверки ссылок и файлов с помощью репутационного сервиса облачной защиты - в том числе с помощью базы данных алгоритмов работы вредоносных программ. 2.4.27. В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы. 2.4.28. С целью защиты от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) Система должна: 2.4.28.1. обеспечивать защиту критически важных частей системы (в том числе папок и ветвей реестра) от модификаций вредоносными программами, в том числе блокировать попытки: 2.4.28.1.1. изменения вредоносными программами загрузочных областей диска; 2.4.28.1.2. изменения нежелательным образом пользовательских файлов (в том числе действия троянцев-шифровальщиков) ; 2.4.28.1.3. изменения файла HOSTS; 2.4.28.1.4. добавления новых задач в логику работы операционной системы; 2.4.28.1.5. изменения правил запуска ранее установленных программ; 2.4.28.1.6. изменения параметров работы системных служб, в том числе процесса создания резервных копий файлов; 2.4.28.1.7. загрузки новых или неизвестных драйверов без ведома пользователя, установки новых виртуальных устройств, загрузки в браузер вредоносных плагинов, в том числе блокировщиков браузера; 2.4.28.1.8. автозапуска вредоносных программ; 2.4.28.1.9. получения низкоуровневого доступа к диску; 2.4.28.1.10. регистрации вредоносных программ в реестре для последующего запуска; 2.4.28.1.11. отключения безопасного режима Windows путем блокировки изменения реестра; 2.4.28.1.12. сокрытия присутствия троянской программы в контролируемой системе в виде руткита.	
--	--	--	--

		2.4.28.2. блокировать попытки установления каналов связи между вредоносным ПО, ранее установленным на компьютер и удаленными серверами злоумышленников; 2.4.28.3. с помощью превентивной защиты, отслеживающей работу всех процессов системы в поисках действий, характерных для процессов вредоносных программ не позволяющей вредоносным объектам внедриться в процессы других программ или каким-либо способом разместить вредоносные файлы в защищаемой системе, выявлять и прекращать работу вредоносных, подозрительных или ненадежных сценариев и процессов; 2.4.28.4. обеспечивать защиту от эксплойтов (программ, эксплуатирующих как уже известные, так и еще неизвестные уязвимости) путем внедрения специального модуля защиты в контролируемые процессы; 2.4.28.5. ограничивать время работы конкретного сотрудника на защищаемом компьютере - с целью исключения доступа у компьютеру в остальное время неопределенного круга лиц. Система ограничения доступа должна позволять: 2.4.28.5.1. задавать время работы на компьютере для выходных и будних дней для каждого сотрудника, а также ограничения по доступу в сеть Интернет; 2.4.28.5.2. задавать суммарное время работы на компьютере для конкретного сотрудника; 2.4.28.5.3. автоматически блокировать доступ к защищаемому компьютеру в ночное время. 2.4.28.6. ограничивать доступ к определенным ресурсам сети Интернет - согласно белым и черным спискам ресурсов сети, предопределенным группам ресурсов; 2.4.28.7. ограничивать доступ к определенным файлам и папкам - с указанием типа доступа объектам (блокировать доступ или разрешать только чтение); 2.4.28.8. обеспечивать возможность использования на защищаемом компьютере только устройств, входящих список разрешенных. Администратор Системы должен иметь возможность: 2.4.28.8.1. контроля доступа к таким типам устройств, как дисковые накопители, приводы DVD/CD-ROM, клавиатуры, компьютерные мыши, сетевые карты, игровые устройства, USB-устройства; 2.4.28.8.2. импорта и экспорта правил использования устройств (в том числе с помощью функционала управления удаленными компьютерами антивирусной сети), а также формирования правил блокировки шин и классов устройств, создания списка разрешенных устройств для заблокированных шин и классов устройств; 2.4.28.8.3. задать уровень доступа к устройству осуществляется в форме полного запрета доступа всем процессам операционной системы или в форме интерактивного режима, в котором пользователю выводится оповещение о попытке доступа к устройству. Для устройств. с файловой системой администратор Системы должен иметь возможность задать тип доступа - разрешать полный доступ к устройству или доступ только на чтение. 2.4.28.9. обеспечивать возможность полного запрета использования USB-устройств и CD/DVD-приводов; 2.4.28.10. обеспечивать создание резервных копий папок, указанных пользователем, а также восстановление данных из хранилища как системой защиты, так и самим пользователем в	
--	--	---	--

		любой момент времени. 2.4.29. модуль превентивной защиты должен: 2.4.29.1. поддерживать возможность создания профилей - групп настроек, применяемых пользователем или администратором защищаемой системы - как для системы превентивной защиты в целом, так и для конкретных приложений с целью исключения потенциальных конфликтов при их работе. 2.4.30. система создания резервных копий папок должна поддерживать возможность: 2.4.30.1. выбора защищаемых каталогов; 2.4.30.2. выбора диска для хранения защищаемых копий; 2.4.30.3. настройки расписаний копирования; 2.4.30.4. создания защищенных копий по требованию. 2.4.31. С целью ускорения проверки Система должна поддерживать возможность исключения из проверки различными компонентами системы защиты: 2.4.31.1. данных, передаваемых по защищенным протоколам (в том числе HTTPS), а также трафика доверенных приложений (имеющих валидную цифровую подпись) ; 2.4.31.2. файлов и папок; 2.4.31.3. ресурсов сети Интернет; 2.4.31.4. почтовых адресов; 2.4.31.5. доверенных программ; 2.4.32. С целью ускорения проверки Брандмауэр (файрвол) должен поддерживать базу доверенных приложений, а также позволять создавать правила работы для приложений. 2.4.33. В случае отсутствия централизованного управления системой защиты Система защиты рабочей станции должна поддерживать возможность удаленного управления Системами защиты, установленными на компьютерах в пределах одной локальной сети. 2.4.34. Подсистема показа статистики Системы защиты должна: 2.4.34.1. отображать время возникновения (детектирования) угроз; 2.4.34.2. списки запрещенных сайтов, доступ к которым был запрошен с защищаемого компьютера. 2.4.35. Подсистема статистики должна иметь возможность отображения только необходимых для анализа сообщений - в том числе создания выборки сообщений отдельных компонентов системы защиты, сообщений с определенными кодами 2.4.36. В Системе должна быть реализована защита работы собственных модулей от сбоя и случайного изменения. 2.5. Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows 2.5.1. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей: 2.5.1.1. Осуществление антивирусной защиты на серверах, включая защиту от руткит-технологий. 2.5.2. Программные средства Системы должны обеспечивать определение в объектах	
--	--	--	--

		файловой системы вредоносных программ всех типов. 2.5.3. Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию ПО, сертифицированного на соответствиетребованиям к средствам антивирусной защиты(Приказ ФСТЭК России от 20.03.2012 г. № 28), должна обеспечивать защиту серверов под управлением операционных систем: 2.5.3.1. Microsoft Windows Server 2003; 2.5.3.2. Microsoft Windows Server 2008; 2.5.3.3. Microsoft Windows Server 2012; 2.5.3.4. Microsoft Windows Server 2016. 2.5.4. Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства. 2.5.5. Антивирусное программное обеспечение должно по умолчанию иметь оптимальные настройки с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления,должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках имеющихся у них прав. 2.5.6. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением системы. 2.5.7. В Системе должна быть реализована возможность выбора приоритета сканирования, а также остановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов. 2.5.8. Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора. 2.5.9. Система должна обеспечивать: 2.5.9.1. поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера; 2.5.9.2. проверку всех скриптов, обрабатываемых в Microsoft InternetExplorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам; 2.5.9.3. блокировку опасных макросов VBA в реальном времени; 2.5.9.4. защиту от вредоносных сценариев, загружаемых с веб-страниц; 2.5.9.5. помещение найденных зараженных файлов в специальное место на жестком диске —«карантин»; 2.5.9.6. автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;	
--	--	---	--

		2.5.9.7. запуск задач по расписанию и/или сразу после загрузки операционной системы. 2.5.10. Система защиты серверов под управлением семейства ОС Microsoft Windows должна обеспечивать реализацию следующих функциональных возможностей: 2.5.10.1. проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов посредством: 2.5.10.1.1. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию; 2.5.10.1.2. проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы. 2.5.11. В Системе должна быть реализована самозащита для всех ее объектов, в том числе критических файлов, процессов, окон, ключей и прочего, от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы. 2.6. Требования к программным средствам антивирусной защиты почтовых систем на платформе Microsoft Exchange 2.6.1. Программные средства Системы должны обеспечивать защиту всей входящей и исходящей электронной корреспонденции, поступающей для обработки на почтовый сервер, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов из следующих элементов электронных писем: 2.6.1.1. тело письма; 2.6.1.2. прикрепленные файлы (включая архивированные и упакованные); 2.6.1.3. вложенные OLE-объекты. 2.6.2. В случае интеграции с почтовым сервером Microsoft Exchange с помощью интерфейса Microsoft Virus Scanning Application Interface (VSAPI) программные средства Системы должны обеспечивать возможность проверки документов, хранящихся в базе данных, а также проверки при доступе к письму. 2.6.3. Система должна обеспечивать: 2.6.3.1. проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе из сети Интернет; 2.6.4. Система должна обеспечивать исключение из проверки отдельных типов объектов, в том числе потенциально опасных. 2.6.5. Система должна обеспечивать возможность выбора желаемых действия для неизлечимых и подозрительных объектов. В качестве таких действий должны быть доступны удаление объекта или перемещение прикрепленных файлов в карантин. Для подозрительных объектов также должна быть доступна возможность пропуска. 2.6.6. Система должна иметь возможность добавления к зараженному или отфильтрованному письму файла до того, как программа совершит над ним выбранное	
--	--	--	--

		действие. Администратор системы должен иметь возможность редактирования содержания этого файла и использования в нем predefined макросов. 2.6.7. Система должна обеспечивать возможность выбора желаемых действий для отфильтрованных спам-сообщений. В качестве таких действий должны быть доступны блокировка, пропуск или перемещение в специальную папку. Система должна иметь возможность модификации заголовка проверенных сообщений и добавления префикса к теме спам-сообщения. 2.6.8. Система, используя актуальную на момент проведения тендера версию ПО, сертифицированного на соответствиетребованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна функционировать на почтовых серверах: 2.6.8.1. Microsoft Exchange Server 2007 SP1 x64; 2.6.8.2. MicrosoftExchangeServer 2010 x64, включаяMicrosoftExchange 2010 использующий унифицированную инфраструктуру отказоустойчивости на основе групп доступности баз данных; 2.6.8.3. MicrosoftExchangeServer 2013 установленнымSP1. 2.6.9. Компоненты Системы должны устойчиво функционировать на серверах класса Pentium133 МГц в условиях их минимальной и максимальной загрузки без существенного снижения производительности серверов, в том числе за счет проведения проверки непосредственно в буферах памяти, а также за счет управления приоритетами обработки сообщений. 2.6.10. Система должна поддерживать возможность ускорения процесса сканирования почтовых сообщений за счет пропуска объектов, проверенныххране в транспортной системе организации через другие почтовые серверы MExchange. 2.6.11. Система должна иметь возможность администрирования с помощью консоли управления. 2.6.12. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. Система должна обеспечивать возможность автоматического определения параметров производительности – без необходимости тонкой настройки их администраторами Системы через интерфейс управления. 2.6.13. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей: 2.6.13.1. В случае интеграции с почтовым сервером Microsoft Exchange с помощью интерфейса Microsoft Virus Scanning Application Interface (VSAPI)- проверку всех почтовых ящиков, включая служебные почтовые ящики SystemMailbox, System Attendant; 2.6.13.2. фильтрацию и блокировку сообщений в зависимости от вероятности принадлежности их к спаму – по категориям <i>спам,вероятно, спам и маловероятно спам</i>; 2.6.13.3. обеспечение фильтрации почтового трафика на спам исключительно с использованиемсистемы анализа на основе правил, не требующей постоянного обучения системы антиспама; 2.6.13.4. фильтрацию по определенным типам сообщений и предотвращение массовых	
--	--	--	--

		рассылок. Система должна поддерживать возможность создания правил фильтрации, в том числе фильтрацию по расширению, маске, размеру файла, максимальному количеству получателей писем. 2.6.13.5. создание белых и черных списков адресов; 2.6.13.6. исключения сообщений от доверенных отправителей из проверки на спам и вирусы 2.6.13.7. запуск задания на фоновую проверку в целях обнаружения ранее неизвестных вредоносных программ; 2.6.13.8. изоляцию инфицированных и подозрительных объектов в специальное место на жестком диске —«карантин»; 2.6.13.9. разбиение клиентов на группы для упрощения администрирования и задание с помощью профилей защиты, реализующих применение различных правил для групп, включая приоритет обработки; 2.6.13.10. обеспечение возможности управления работой Системы с разными уровнями доступа; 2.6.13.11. уведомление о вирусных событиях; 2.6.13.12. регистрацию ошибок и происходящих событий как в журнале регистрации событий операционной системы (Event Log), так и в текстовом журнале регистрации событий программы установки; 2.6.13.13. ведение журнала событий, в том числе с указанием необходимой степени детализации для определенного типа событий; 2.6.13.14. сбор статистики; 2.6.13.15. автоматическое обновление вирусных баз. 2.6.14. Система должна иметь возможность управления карантином, в том числе восстановления сохраненных объектов. 2.7. Требования по комплектности поставки 2.7.1. В состав Системы должны входить: 2.7.1.1. программные средства антивирусной защиты, необходимые для выполнения требований данного технического задания; 2.7.1.2. программные средства защиты пользователей от нежелательных массовых почтовых рассылок – спама; 2.7.1.3. программные средства централизованного управления, мониторинга и обновления; 2.7.1.4. обновляемые базы данных сигнатур всевозможных вредоносных программ. 2.7.2. Комплект поставки должен содержать: 2.7.2.1. необходимый набор серийных номеров либо ключевых файлов; 2.7.2.2. дистрибутив Системы; 2.7.2.3. файлы эксплуатационной документации в формате pdf (Adobe Acrobat Reader), в том числе руководство пользователя (администратора). Поставляемая документация должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты. 2.7.3. В соответствии с требованиями заказчика комплект поставки ПО должен содержать дистрибутивы продуктов, сертифицированные ФСТЭК России на соответствие требованиям к	
--	--	---	--

		средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28) по Профилю защиты средств антивирусной защиты типа «А» второго класса защиты, Профилю защиты средств антивирусной защиты типа «Б» второго класса защиты, Профилю защиты средств антивирусной защиты типа «В» второго класса защиты», Профилю защиты средств антивирусной защиты типа «Г» второго класса защиты. Комплект поставки, сертифицированный ФСТЭК России, должен содержать: DVD-диск в фирменном конверте, содержащий верифицированные дистрибутивы сертифицированных продуктов документацию и материалы в формате PDF для настройки поставляемого программного обеспечения в соответствии с сертифицированными параметрами, приведенными в технической документации; формуляр с голографической наклейкой, содержащий эталонные значения контрольных сумм сертифицированных продуктов; лицензионный сертификат, удостоверяющий законное приобретение программного изделия; заверенную копию сертификата соответствия ФСТЭК России. 2.8. Требования по технической поддержке Системы 2.8.1. Техническая поддержка должна предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет. 2.8.2. Техническая поддержка должна включать возможность предоставления выделенного специалиста, доступного в режиме 5/8 2.8.3. Техническая поддержка должна включать возможность проведения расследования компьютерных инцидентов 2.8.4. Техническая поддержка должна включать возможность написания специального ПО, предназначенного для устранения последствий воздействия вредоносного ПО на зараженную систему. В том числе утилит расшифровки файлов, если данная операция является возможной 2.8.5. Техническая поддержка должна обеспечивать возможность получения специалистами и пользователями Заказчика информационной помощи по установке Системы и ее компонентов, в том числе: 2.8.5.1. ответов на вопросы, а также получение инструкций относительно процесса установки и применения программного обеспечения; 2.8.5.2. ответов на вопросы о наличии проблем в работе программного обеспечения, а также помощи в определении того, является ли данная проблема результатом сбоя программного обеспечения, ошибок настройки или же она вызвана проблемами, связанными с внешними условиями существования или установкой программного обеспечения. 2.8.6. Web-сайт производителя Системы должен быть на русском языке, иметь специальный раздел, посвященный технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов производителя. Срок использования лицензии - 1 (Один) год;	
--	--	--	--

			Лицензии на 1 установку, для 1 (Одного) АРМ.	
7.	Установочный комплект ПО реализующего функции АЗ	Товар, с НДС	Установочный комплект АЗ должен состоять из: • компакт-диска с дистрибутивом ПО; • копии сертификата ФСТЭК России на ПО; • формуляра на ПО.	1
8.	Средство криптографической защиты информации (средство электронной подписи)	Лицензия, без НДС	Требования к реализации криптографических стандартов: Применяемое средство криптографической защиты информации (средство электронной подписи) должно обеспечивать применение электронной подписи (ЭП) и шифрования в соответствии с нормами действующего законодательства Российской Федерации и осуществлять выполнение следующих основных функций: • генерацию и управление ключевой информацией; • формирование электронной подписи в соответствии с ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018); • подтверждение подлинности электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018); • подсчет значения хэш-функции в соответствии с ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018); • шифрование и расшифрование данных в соответствии с ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018), ГОСТ 28147-89; • формирование ключей электронной подписи и ключей проверки электронной подписи, а также ключей шифрования; • идентификацию, аутентификацию, шифрование, имитозащиту TLS соединений в соответствии с МР 26.2.001-2013, Р 1323565.1.020-2020 (TLS 1.2) и Р 1323565.1.030-2020 (TLS 1.3); • реализацию набора протоколов IPsec в соответствии с особенностями использования отечественных криптографических алгоритмов. Требования к реализации программного интерфейса встраивания Средство криптографической защиты информации (средство электронной подписи) должно соответствовать криптографическому интерфейсу компании Microsoft - Cryptographic Service Provider (CSP). Встраивание средства криптографической защиты информации (средства электронной подписи) в прикладную информационную систему должно предусматривать возможность: • Применения в операционных системах семейства Microsoft Windows интерфейса функций: - CAPICOM; - Certificate Enrollment Control; - Certificate Enrollment API; - Certificate Services. • вызова функций средства криптографической защиты информации (средства электронной подписи);	1

• применения в стандартном прикладном программном обеспечении операционных систем семейства Microsoft Windows MS Outlook Express; MS IE; MS IIS; Outlook, и т.д. (для поддержки MS Office Word, Excel может требоваться дополнительное ПО от разработчика средства криптографической защиты информации (средства электронной подписи)).

Требования к алгоритмам, сертификатам открытых ключей и поддерживаемым форматам криптографических сообщений

Применяемое средство криптографической защиты информации (средство электронной подписи) должно реализовывать ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Информационная технология. Криптографическая защита информации. Блочные шифры», ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018) «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».

Применяемое средство криптографической защиты информации (средство электронной подписи) должно реализовывать ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018).

Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать сертификаты открытых ключей стандарта X.509v3 согласно рекомендаций по стандартизации Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) «Использование алгоритмов ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509».

Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать формат защищенных сообщений в формате CMS с использованием алгоритмов ГОСТ 28147-89, ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018), ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018) и ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018), реализованного в соответствии с методическими рекомендациями МР 26.2.002-2013. «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.10 и ГОСТ Р 34.11 в криптографических сообщениях формата CMS» и рекомендациями по стандартизации Р 1323565.1.025–2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами».

Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать возможность создания форматов криптографических сообщений типа CAdES в соответствии с ETSI TS 101 733 (Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)):

- формата CAdES-BES;
- формата CAdES-T;
- формата CAdES-X Long Type 1;
- формата CAdES-A,

а также формата XMLDSig согласно RFC 3075 «XML-Signature Syntax and Processing» с учетом

документа Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) «Информационная технология. Криптографическая защита информации. Использование российских алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML» для формирования электронной подписи в XML при встраивании в прикладные информационные системы с использованием программных библиотек (SDK) от разработчика средства криптографической защиты информации (средства электронной подписи). Отдельные компоненты таких программных библиотек могут лицензироваться дополнительно.

Требования к составу

Комплектация исполнения средства криптографической защиты информации (средства электронной подписи) должна включать:

- модуль сетевой аутентификации TLS, обеспечивающий реализацию сетевого протокола TLS с использованием российских криптографических стандартов (возможности модуля TLS определяются типом лицензии на средство криптографической защиты информации (средство электронной подписи));
- модуль реализации набора протоколов IPsec с использованием отечественных криптографических алгоритмов, включая библиотеки IKE, ESP, AH (лицензируется отдельно);
- модуль Winlogon для аутентификации пользователей в домене Microsoft Windows (лицензируется дополнительно);
- модуль, обеспечивающий реализацию криптографических операций в Java-приложениях, посредством использования средства криптографической защиты информации (средства электронной подписи) (лицензируется дополнительно);
- модуль клиентского компонента службы актуальных статусов сертификатов, обеспечивающий работу по протоколу OCSP с использованием российских криптографических алгоритмов (лицензируется дополнительно);
- модуль клиентского компонента службы штампов времени, обеспечивающий работу по протоколу TSP с использованием российских криптографических алгоритмов (лицензируется дополнительно);
- модуль создания и проверки электронной подписи файлов в формате криптографических сообщений типа CAdES, XMLDsig и XAdES с использованием отечественных криптографических алгоритмов;
- приложение командной строки, обеспечивающее формирование запросов на создание сертификатов, хэширование, шифрование и расшифрование файлов, создание и проверку электронной подписи файлов, в том числе в формате криптографических сообщений типа CAdES (лицензируется дополнительно);
- модуль построения защищенного TLS-канала между произвольными серверами и рабочими местами пользователей с установленным средством криптографической защиты информации (средством электронной подписи), реализует прием (инкапсуляцию) незащищенного трафика от произвольного приложения или службы на клиентском компьютере (рабочем месте или сервере), его шифрование и дальнейшую передачу по протоколу TLS с последующем расшифровыванием на удаленном компьютере (сервере);

			• модуль работы с криптографическими функциями без инсталляции средства криптографической защиты информации (средства электронной подписи) в ОС семейства Microsoft Windows; • модуль управления установкой средства криптографической защиты информации (средства электронной подписи); • инструментарий разработчика, обеспечивающий встраивание средства криптографической информации (средства электронной подписи) в прикладные информационные системы, в том числе включающий модуль встраивания в различные веб-браузеры в среде различных операционных систем. Функциональные требования Средство криптографической защиты информации (средство электронной подписи) должно предоставлять программный интерфейс для выполнения следующих основных функций: • формирование электронной подписи на рабочем месте пользователя и (или) сервере (в зависимости от типа лицензии); • подтверждение подлинности электронной подписи на серверах и рабочих местах пользователей; • подсчет значения хэш-функции данных на серверах и рабочих местах пользователей; • шифрование и расшифрование данных на рабочем месте пользователя и (или) сервере (в зависимости от типа лицензии); • формирование ключей электронной подписи и ключей проверки электронной подписи на рабочем месте пользователя и (или) сервере (в зависимости от типа лицензии); • реализация функций по созданию и проверке электронной подписи, шифрованию/расшифрованию данных в режиме клиентского компонента программно-аппаратных комплексов централизованного создания и хранения неизвлекаемых ключей электронной подписи (типа ПАКМ «КриптоПро HSM» версии 2.0 R3). Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать выполнение следующих сервисных функций: • возможность построения защищенного TLS-соединения на сервере под управлением ОС семейства Linux с использованием ГОСТ-алгоритмов с помощью вызова функций СКЗИ на nginx сервере, на Apache сервере, Apache Tomcat и Bellsoft Libercat без проведения исследований по оценке влияния указанных серверов на СКЗИ (лицензируется дополнительно); • встраивание средства криптографической защиты информации в прикладную информационную систему должно предусматривать возможность использования программного интерфейса СКЗИ в мобильных приложениях (в том числе для построения защищенного TLS-соединения) без проведения дополнительных тематических исследований этих приложений; • установка личных сертификатов и ключей проверки электронной подписи на рабочем месте/сервере с обеспечением связи сертификата открытого ключа с соответствующим указанному сертификату закрытым ключом;	
--	--	--	--	--

		• копирование и удаление ключей электронной подписи; • установка, изменение и удаление пароля на доступ к закрытому ключу. • создание и проверка электронной подписи в формате CMS (присоединенной и отсоединенной) с использованием графического интерфейса пользователя; • установка параметров работы в режиме клиентского компонента программно-аппаратных комплексов централизованного создания и хранения неизвлекаемых ключей электронной подписи, включая определение сетевых адресов подключения, установку сертификатов ключей проверки электронной подписи, хранящихся в «облачном токене». Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать эксплуатацию на следующих операционных системах (иметь клиентскую лицензию): • Windows 7/8/8.1/10 (x86/x64); • Windows 11 (x64). Требования к общесистемному программному обеспечению Средство криптографической защиты информации (средство электронной подписи) должно включать варианты исполнений, функционирующих в среде следующих операционных систем: <u>Windows</u> • Windows 7/8/8.1/10/Server 2008 (x86, x64); • Windows Server 11/2008 R2/2012/2012 R2/2016/2019/2022 (x64). <u>LSB Linux</u> Включает дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x: • CentOS 6 (x86, x64); • CentOS 7 (x86, x64, POWER, ARM, ARM64); • CentOS 8 (x64, POWER, ARM64); • ОСь (OS-RT) (x64); • ТД ОС АИС ФССП России (GosLinux) (x86, x64); • РЕД ОС 7.1/7.2/7.3/8 (x86, x64, ARM64); • Oracle Linux 6 (x86, x64); • Oracle Linux 7 (x64); • Oracle Linux 8/9 (x64, ARM64); • OpenSUSE Leap 42, 15 (x86, x64, ARM, ARM64); • AlterOS (x64); • SUSE Linux Enterprise Server 11SP4 (x86, x64); • SUSE Linux Enterprise Server 12/15, Desktop 12/15 (x64, POWER, ARM64); • Red Hat Enterprise Linux 6 (x86, x64); • Red Hat Enterprise Linux 7/8/9 (x64, POWER, ARM64); • Check Point GAIa (x86, x64); • Синтез-ОС.РС (x86, x64); • ПК «СинтезМ-Клиент» в составе КП «ЗОС «СинтезМ» (x64);	
--	--	---	--

		• ПК «СинтезМ-Сервер» в составе КП «ЗОС «СинтезМ» (x64); • КП «ОС «СинтезМ-К» (x64); • Ubuntu 14.04/16.04 (x86, x64, ARM, ARM64); • Ubuntu 18.04/20.04/22.04 (x64, ARM, ARM64); • Halo OS (x64); • Linux Mint 18/19/20/21 (x86, x64); • Debian 8/9/10/11/12 (x86, x64, ARM, ARM64, MIPS); • Лотос (x86, x64); • Astra Linux Special Edition, Common Edition (x86, x64, ARM, ARM64, MIPS, Эльбрус); • МСВСфера 6.3 Сервер (x64, ARM64); • ThinLinux 2 (x64); • ЕМИАС 1.0 (x64); • Мурена 1.4 (ARM9); • ОС ОН «Стрелец» (x64); • ОС «Атлант» (x64); • ОС ОН «ОСнова» 2.0 (x64). <u>Unix:</u> • ОС Эльбрус версия 3 (Эльбрус); • ALT Linux 7 (x86, x64, ARM); • Альт 8 СП Сервер, Альт 8 СП Рабочая станция (x86, x64, Эльбрус); • Альт Сервер 8, Альт Рабочая станция 8, Альт Образование 8 (x86, x64); • Альт Сервер 9, Альт Рабочая станция 9, Альт Образование 9 (x86, x64, ARM64, MIPS, Эльбрус); • ROSA Enterprise Desktop (RED X4) (x86, x64); • ROSA Enterprise Linux Desktop, Enterprise Linux Server (x64); • РОСА «КОБАЛЬТ», РОСА «НИКЕЛЬ» (x64); • FreeBSD 11/12/13, pfSense 2.x (x86, x64); • AIX 6/7 (POWER); • Mac OS X 10.9/10.10/10.11/10.12/10.13/10.14/10.15/11/12/13 (x64, ARM64) (только для класса KC1). <u>Solaris:</u> • Solaris 10 (SPARC, x86, x64); • Solaris 11 (SPARC, x64); <u>Аврора:</u> • ОС «Аврора» 4.0/4.1 (ARMv7). <u>iOS (только для класса KC1):</u> • Apple iOS (включая iPadOS) 8/9/10/11/12/13/14/15/16 (ARMv7, ARM64). <u>Android (только для класса KC1):</u> • Android 8/9/10/11/12/13 (ARMv7, ARM64, x86, x86_64). <u>Программно-аппаратные виртуальные среды (только для класса KC1):</u>	
--	--	---	--

		• Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016/2019 (x64); • Microsoft Hyper-V 8/8.1/10 (x64); • Citrix XenServer 7 (x64); • VMWare WorkStation 11/12/14/15/16 (x86, x64); • VMWare WorkStation Player 12/14/15 (x86, x64); • VMWare vSphere ESXi/Hypervisor 5.5/6.0/6.5/6.7/7.0 (x64); • Oracle VirtualBox 5.2 (x86, x64); • RHEV 4 (x64); • ROSA Virtualization (x64); • Альт Сервер Виртуализации 9 (x64, ARM64); • ПК «Средства виртуализации «БРЕСТ» в составе ОС «Astra Linux Special Edition»; • KVM из состава поддерживаемых ОС (x64), в т.ч. совместно с Libvirt 6/7/8 (x64); • QEMU 4.2/5.2/6.2/7 (x64); • Yandex KVM YC 5.10 (x64); • Yandex QEMU YC 5.0.1 (x64); • Proxmox VE 7 (x64) в режиме администрирования ВМ. <u>Программные виртуальные среды (только для класса КС1):</u> • Docker Engine 20.10 (x64, ARM); • Kubernetes 1.24, 1.25 (x64); • OpenShift Container Platform 4.10, 4.11 (x64). Требования к поддерживаемым ключевым носителям Средство криптографической защиты информации (средство электронной подписи) должно поддерживать следующие носители: 1. Пассивные носители, предназначенные для хранения ключей электронной подписи и их передачи в операционную систему с установленным средством криптографической защиты информации (средством электронной подписи) для создания электронной подписи и выполнения прочих операций (типа USB-токены и смарт карты Рутокен Lite). 2. Активные носители, предназначенные для хранения неизвлекаемых ключей электронной подписи без возможности их передачи в операционную систему с установленным средством криптографической защиты информации (средством электронной подписи) (типа Рутокен ЭЦП 2.0); 3. Функциональные ключевые носители, предназначенные для хранения неизвлекаемых ключей электронной подписи с защитой канала связи с ключевым носителем с помощью протокола выработки общего ключа с аутентификацией на основе пароля – протокола SESPake (типа Рутокен ЭЦП 2.0 3000); 4. Сетевые программно-аппаратные комплексы для централизованного хранения неизвлекаемых ключей и создания электронной подписи, типа ПАКМ «КриптоПро HSM» версии 2.0 R3. <u>Примечание:</u> Для ключевых носителей с неизвлекаемыми ключами и защитой канала связи необходимо положительное заключение ФСБ России.	
--	--	---	--

			Требования к поддерживаемым стандартным приложениям и службам операционных систем Средство криптографической защиты информации (средство электронной подписи) должно поддерживаться следующими стандартными приложениями и службами операционных систем: • Центр Сертификации - Microsoft Certification Authority, входящий в состав Windows Server 2008 R2/2012/2012 R2/2016/2019/2022. • Клиент электронной почты - Microsoft Outlook (из состава Microsoft Office 2007/2010/2013/2016/2019/2021). • Клиент электронной почты - Microsoft Outlook Express в составе Internet Explorer/Microsoft Edge, Почта Windows Mail, Live Mail. • Microsoft Word, Excel из состава Microsoft Office 2003/2007/2010/2013/2016/2019/2021 (с помощью специализированного плагина от производителя средства криптографической защиты информации (средства электронной подписи) для Microsoft Office – лицензируется дополнительно). • Microsoft Exchange Server 2010/2013/2016/2019. • Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode. • Службы терминалов для Microsoft Windows Server 2008 R2/2012/2012 R2/2016/2019/2022 (включая шлюз служб терминалов) и клиент (RDP). • Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Microsoft Internet Explorer/Microsoft Edge – web-сервер IIS, TLS-сервер, TLS-клиент (IE). • Служба доменной аутентификации Winlogon в составе Microsoft Windows (с помощью специализированного модуля в составе средства криптографической защиты информации (средства электронной подписи) – лицензируется дополнительно). • Microsoft ISA сервер. • Сервер Microsoft TMG. • Сервер Microsoft UAG. • Стандартная служба шифрования данных на жестком диске компьютера (рабочего места или сервера) Microsoft Encrypt File System (Microsoft EFS) (с помощью специализированного ПО от производителя средства криптографической защиты информации (средства электронной подписи) для Microsoft Windows – лицензируется дополнительно). Требования к сертификации Средство электронной подписи (средство криптографической защиты информации) должно быть сертифицировано или иметь положительное Заключение ФСБ России по требованиям: - к средствам электронной подписи; - к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, по классам КС1, КС2. Версия 5.0 на одном рабочем месте. Срок действия лицензии – бессрочно.	
9.	Установочный комплект ПО	Товар, с	Установочный комплект должен состоять из:	1

	реализующего функции СКЗИ (средство электронной подписи)	НДС	• компакт-диска с дистрибутивом ПО; • копии сертификата ФСТЭК России на ПО; • формуляра на ПО.	
10.	Средство анализа защищенности сети	Лицензия , без НДС	Требования к средствам анализа защищенности (САЗ): 1 Требования к механизмам сетевого аудита САЗ 1) САЗ должно обеспечивать сканирование TCP и UDP портов в диапазоне 1...65535, а также определение состояния сетевых портов. 2) САЗ должно обеспечивать инвентаризацию ресурсов вычислительной сети, включая идентификацию узлов вычислительной сети, определение сервисов, запущенных на узле, идентификацию ОС и приложений. 3) САЗ должно обнаруживать уязвимости кода и конфигурации программного обеспечения. Для выявления (поиска) уязвимостей САЗ должно использовать встроенную базу данных уязвимостей кода и уязвимостей конфигурации программного обеспечения. База данных уязвимостей САЗ должна содержать унифицированные описания уязвимостей, аналогичные содержащимся в следующих общедоступных источниках: банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru), база данных «Common Vulnerabilities and Exposures» (https://cve.mitre.org). САЗ должно осуществлять тестирование на проникновение путем эксплуатации уязвимостей, выявленных и содержащихся в базе данных уязвимостей. 4) САЗ должно осуществлять обновление базы данных уязвимостей через сервис обновлений САЗ. 5) САЗ должно обеспечивать идентификацию UDP-сервисов: exosee (1027/udp), netbios-ns (137/udp), ntp (123/udp). 6) САЗ должно обеспечивать идентификацию TCP-сервисов: imap (143/tcp), http (80/tcp), http-alt (8080/tcp), smtp (25/tcp), ermap (135/tcp), blackjack (1025/tcp), ssh (22/tcp), microsoft-ds (445/tcp), netbios-ssn (139/tcp), ldaps (636/tcp), msft-gc-ssl (3269/tcp), cap (1026/tcp), activesync (1034/tcp), ldap (389/tcp), ftp (21/tcp), https (443/tcp), mysql (3306/tcp). 7) САЗ должно осуществлять аудит безопасности беспроводных сетей и имитацию атак на них. 8) САЗ должно осуществлять перехват, анализ и фильтрацию сетевых пакетов локальной и внешней сетей информационной системы и извлечение из сетевого трафика парольной информации (для протоколов ftp, pop3, http, https, telnet), а также, проверку возможности атак подмены MAC-адресов. 9) САЗ должно обеспечивать контроль за установкой обновлений ОС Microsoft Windows: Vista, 7, 8, 10. 10) САЗ должно обеспечивать контроль за настройками комплекса средств защиты ОС специального назначения «Astra Linux Special Edition». 11) САЗ должно обеспечивать формирование отчетов по результатам проверок. 2 Требования к механизмам локального аудита САЗ 1) САЗ должно осуществлять поиск остаточной информации на различных носителях информации и гарантированное уничтожение информации путем записи случайной	1

			последовательности символов поверх стираемой информации, а также записи случайной последовательности символов в освободившееся пространство накопителей на жестких магнитных дисках, накопителей на основе флэш-памяти и съемных носителей информации. 2) САЗ должно осуществлять локальный подбор паролей по словарю для учетных записей пользователей ОС Microsoft Windows: Vista, 7, 8, 10. 3) САЗ должно обеспечивать контрольное суммирование заданных файлов, папок, подпапок, съемных носителей и НЖМД. Срок использования лицензии - 1 (Один) год; Лицензия на 1 IP адрес, для 1 (Одного) АРМ; Электронная поставка.	
--	--	--	---	--

