Контракт № ЭМ24/661/01

Оказание услуг по поставке программного обеспечения для ГБОУ школа № 661 Приморского района Санкт-Петербурга.

(ИКЗ: 242781410622478140100100030000000244)

Санкт-Петербург **20. 01. 2024**

Государственное бюджетное общеобразовательное учреждение средняя общеобразовательная школа № 661 Приморского района Санкт-Петербурга (ГБОУ школа № 661 Приморского района Санкт-Петербурга), именуемое в дальнейшем «Заказчик», в лице директора Даниловой Елены Александровны, действующего на основании Устава, с одной стороны, и **Общество с ограниченной ответственностью «Цифровые технологии»** (ООО «Цифровые технологии») , именуемое в дальнейшем «Исполнитель», в лице Терентьевой Юлии Александровны , действующего на основании Устава, с другой стороны, вместе именуемые в дальнейшем «Стороны», в соответствии с *п. 5 ч. 1 ст. 93* Федерального закона от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее - ФЗ № 44) заключили настоящий Контракт (далее - Контракт) о нижеследующем:

1. ПРЕДМЕТ КОНТРАКТА

1.1. Заказчик поручает, а Исполнитель принимает на себя обязательство **оказание услуг по поставке программного обеспечения для ГБОУ школа № 661 Приморского района Санкт-Петербурга** в объеме, установленном в Приложении № 2 к настоящему контракту (*Техническое задание*), а Заказчик обязуется оплатить оказанные услуги в порядке и на условиях, определенных настоящим контрактом.
1.2. Сроки оказания услуг: 10 рабочих дней с даты подписания контракта.
1.3. Место оказания услуг: услуги оказываются по адресу *Заказчика*:
197372, Санкт-Петербург, ул. Яхтенная, д.33, корп.3, лит. А

2. ЦЕНА КОНТРАКТА И ПОРЯДОК РАСЧЕТОВ

2.1. Цена контракта составляет **54 320 рублей 00 копеек** (пятьдесят четыре тысячи триста двадцать рублей 00 копеек), *НДС не облагается* и определяется в Приложении № 1 к контракту *(Расчет цены контракта).*
2.2. Цена является твердой и не может изменяться в ходе исполнения контракта, кроме случаев, предусмотренных настоящим пунктом.
Изменение цены настоящего контракта допускается только в следующих случаях:
- при снижении цены контракта без изменения предусмотренных контрактом объема услуг, качества услуг и иных условий контракта;
- *если по предложению Заказчика увеличиваются предусмотренные контрактом объем услуг не более чем на десять процентов или уменьшаются предусмотренные контрактом объем оказываемых услуг не более чем на десять процентов. При этом по соглашению сторон допускается изменение с учетом положений бюджетного законодательства Российской Федерации цены контракта пропорционально дополнительному объему услуг исходя из установленной в контракте цены единицы услуги, но не более чем на десять процентов цены контракта. При уменьшении предусмотренного контрактом объема услуг стороны контракта обязаны уменьшить цену контракта исходя из цены единицы услуги;*
- *по соглашению Сторон допускается изменение существенных условий Контракта, если при исполнении Контракта возникли независящие от Сторон обстоятельства, влекущие невозможность его исполнения. Предусмотренное настоящим пунктом изменение осуществляется с соблюдением положений частей 1.3 - 1.6 статьи 95 Федерального закона от 05.04.2013 № 44-ФЗ (то есть в пределах доведенных в соответствии с бюджетным законодательством Российской Федерации лимитов бюджетных обязательств на срок исполнения контракта) на основании решения Правительства Санкт-Петербурга.*
2.3. Оплата производится по факту оказания услуг путем безналичного перечисления денежных средств на расчетный счет Исполнителя в течение ***10 рабочих дней*** со дня подписания акта сдачи-приемки оказанных услуг. Исполнитель выставляет счет, *счет-фактуру (если облагается НДС)*.
2.4. В случае нарушения Исполнителем условий настоящего Контракта Заказчик вправе удержать сумму неустоек из суммы, подлежащей оплате Исполнителю.
2.5. Выплата аванса по контракту не предусмотрена.

2.6. Финансирование по настоящему контракту осуществляется за счет *Внебюджетные средства. Средства бюджетных учреждений.*
2.7. Сумма, подлежащая уплате заказчиком юридическому лицу или физическому лицу, в том числе зарегистрированному в качестве индивидуального предпринимателя, уменьшается на размер налогов, сборов и иных обязательных платежей в бюджеты бюджетной системы Российской Федерации, связанных с оплатой контракта, если в соответствии с законодательством Российской Федерации о налогах и сборах такие налоги, сборы и иные обязательные платежи подлежат уплате в бюджеты бюджетной системы Российской Федерации заказчиком.

3. СРОК ДЕЙСТВИЯ КОНТРАКТА

3.1. Настоящий контракт вступает в силу после подписания Сторонами и действует по 31.12.2024.
3.2. Прекращение срока действия контракта не влечет прекращение обязательств, принятых на себя Сторонами при его исполнении.

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН

4.1. Обязанности и права Исполнителя:
4.1.1. Оказать услуги лично.
4.1.2. Исполнять полученные в ходе оказания услуг указания Заказчика, если такие указания не противоречат условиям контракта и действующему законодательству.
4.1.3. При оказании услуг соблюдать требования закона и иных правовых актов об охране окружающей среды.
4.1.4. Качество услуг должно соответствовать требованиям, обычно предъявляемым к услугам такого рода.
4.1.5. Исполнитель имеет другие обязанности, вытекающие из настоящего Контракта.
4.1.6. Исполнитель вправе требовать полной оплаты по настоящему Контракту в случае надлежащего его исполнения.
4.2. Обязанности и права Заказчика:
4.2.1. Оплатить оказанные Исполнителем услуги на условиях контракта.
4.2.2. В любое время проверять ход и качество оказания услуг Исполнителем, не вмешиваясь при этом в его деятельность.
4.3. После завершения оказания Исполнителем услуг уполномоченные представители Заказчика и Исполнителя подписывают акт об оказанных услугах, который служит основанием для взаимных расчетов между ними.

5. СДАЧА-ПРИЕМКА УСЛУГ

5.1. При приемке Услуг Заказчик проводит экспертизу оказанных услуг на соответствие условиям Контракта. Экспертиза проводится Заказчиком своими силами за свой счет или к проведению экспертизы могут быть привлечены эксперты или экспертные организации. Приемка услуг по акту сдачи-приемки свидетельствует о проведении Заказчиком экспертизы своими силами и не требует составления отдельного документа по результатам экспертизы.
5.2. После завершения оказания Исполнителем услуг по контракту Исполнитель в течение 3 рабочих дней после окончания оказания услуг направляет Заказчику для подписания акт сдачи-приемки оказанных услуг.
Заказчик обязан в течение 3 рабочих дней после получения акта сдачи-приемки оказанных услуг от Исполнителя подписать такой акт при отсутствии претензий либо направить Исполнителю мотивированный отказ от его подписания.
5.3. При обнаружении Заказчиком в ходе приемки услуг недостатков в оказанных услугах Заказчиком незамедлительно составляется соответствующий акт и выдается предписание Исполнителю со сроками устранения выявленных нарушений, которые фиксируются в акте.
Акт и предписание составляются в двух идентичных экземплярах и подписываются Заказчиком и Исполнителем.
При отказе (уклонении) Исполнителя от подписания акта или получения предписания об этом делается отметка в акте. При этом второй экземпляр акта и предписания направляются Заказчиком Исполнителю по почте заказным письмом с уведомлением о вручении.

5.4. Исполнитель обязан устранить все обнаруженные недостатки за свой счет в сроки, указанные в предписании Заказчика.
5.5. Устранение Исполнителем в установленные сроки выявленных Заказчиком недостатков не освобождает его от уплаты неустойки, предусмотренной контрактом.
5.6. Заказчик, принявший услуги без проверки, не лишается права ссылаться на недостатки, которые могли быть установлены при приемке.
5.7. Заказчик вправе отказаться от приемки оказанных услуг в случае обнаружения недостатков, которые не могут быть устранены Исполнителем без несоразмерных затрат времени.
5.8. Датой приемки услуг считается дата, указанная в акте сдачи-приемки оказанных услуг. Акт подписывается не ранее устранения всех недостатков.

6 .ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. Стороны несут ответственность за неисполнение и/или ненадлежащее исполнение Контракта в соответствии с действующим законодательством, в частности, в соответствии с Федеральным законом от 05.04.2013 № 44-ФЗ, а также с постановлением Правительства РФ от 30.08.2017 № 1042.
6.2. Ответственность Исполнителя:
6.2.1. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, Исполнитель уплачивает Заказчику штраф в размере 10 процентов цены контракта (этапа).
6.2.2. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательства, предусмотренного Контрактом, которое не имеет стоимостного выражения, Исполнитель уплачивает Заказчику штраф в размере 1000 рублей.
6.2.3. В случае просрочки исполнения Исполнителем обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, Заказчик направляет Исполнителю требование об уплате пеней. Пеня начисляется за каждый день просрочки исполнения Исполнителем обязательства, предусмотренного Контрактом, начиная со дня, следующего после дня истечения установленного Контрактом срока исполнения обязательства, и устанавливается в размере одной трехсотой действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от цены Контракта, (отдельного этапа исполнения контракта), уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных контрактом (соответствующим отдельным этапом исполнения контракта) и фактически исполненных Исполнителем.
6.3. Ответственность Заказчика:
6.3.1. За каждый факт неисполнения Заказчиком обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств, предусмотренных контрактом, размер штрафа составляет 1000 рублей.
6.3.2. В случае просрочки исполнения заказчиком обязательств, предусмотренных Контрактом, Исполнитель вправе потребовать уплаты пеней. Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного Контрактом, начиная со дня, следующего после дня истечения установленного Контрактом срока исполнения обязательства. Такая пеня устанавливается контрактом в размере одной трехсотой действующей на дату уплаты пеней ключевой ставки Центрального банка Российской Федерации от не уплаченной в срок суммы.
6.4. Общая сумма начисленных штрафов за ненадлежащее исполнение Заказчиком обязательств, предусмотренных Контрактом, не может превышать цену Контракта.
6.5. Общая сумма начисленных штрафов за неисполнение или ненадлежащее исполнение Исполнителем обязательств, предусмотренных Контрактом, не может превышать цену Контракта.
6.6. Взыскание неустойки может быть осуществлено в порядке, предусмотренном п. 2.4. настоящего Контракта.
6.7. Случаи и порядок списания начисленных исполнителю, но не списанных заказчиком сумм неустоек (штрафов, пеней) в связи с неисполнением или ненадлежащим исполнением обязательств, предусмотренных контрактом, устанавливаются Правительством Российской Федерации.

7. ИЗМЕНЕНИЕ И РАСТОРЖЕНИЕ КОНТРАКТА

7.1. Контракт может быть расторгнут по соглашению сторон, по решению суда по основаниям, предусмотренным действующим законодательством, или в одностороннем порядке.

7.2. Заказчик вправе в одностороннем порядке отказаться от исполнения контракта в соответствии с частью 2 статьи 407 и статьей 450 Гражданского кодекса РФ и потребовать возмещения причиненных убытков в случае существенных нарушений Исполнителем условий контракта:
- нарушение сроков окончания оказания услуг более чем на 10 рабочих дней не по вине Заказчика;
- в случаях, если выявленные в ходе приемки услуг недостатки не устранены Исполнителем в установленные сроки или являются существенными и неустранимыми.
7.3. Исполнитель вправе в одностороннем порядке отказаться от исполнения настоящего Контракта в случаях, предусмотренных Гражданским кодексом РФ.
7.4. Порядок одностороннего расторжения контракта (одностороннего отказа от исполнения контракта) регулируется действующим на момент исполнения контракта законодательством.
7.6. Изменения и дополнения к контракту имеют силу только в том случае, если они оформлены в письменном виде, подписаны Сторонами.

8. ПОРЯДОК РАССМОТРЕНИЯ СПОРОВ

8.1. Все споры, возникающие в связи с контрактом, а также из него вытекающие стороны пытаются решить путем соглашения. Срок ответа на претензию составляет 10 дней со дня, следующего за днем получения претензии. Если договоренности не достигнуты, спор подлежит рассмотрению Арбитражным судом города Санкт-Петербурга и Ленинградской области.

9. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

9.1. Стороны освобождаются от ответственности за частичное или неполное исполнение своих обязательств по Контракту, если оно явилось следствием возникновения обстоятельств непреодолимой силы, возникших после заключения Контракта в результате событий чрезвычайного характера, которые стороны не могли ни предвидеть, ни предотвратить разумными мерами.
К обстоятельствам непреодолимой силы относятся события, на которые стороны не могут оказать влияния и за возникновение которых не несут ответственности. Таковыми являются, в том числе, но не исключительно: землетрясения, пожары, наводнения, забастовки, эпидемии, изменения действующего законодательства, влияющие на исполнение обязательств по настоящему Контракту, другие непредвиденные обстоятельства. Наступление указанных в настоящем пункте обстоятельств должно подтверждаться соответствующими документами.
9.2. В случае наступления обстоятельств, указанных в п.9.1. Контракта, сторона, которая не в состоянии исполнить обязательства, взятые на себя по настоящему Контракту, должна в течение 5 рабочих дней сообщить об этих обстоятельствах другой стороне в письменной форме.
9.3. С момента наступления обстоятельств непреодолимой силы действие Контракта приостанавливается до дня, определяемого сторонами. Изменение существенных условий Контракта допускается в случаях, предусмотренных пунктом 2.2 настоящего Контракта.

10. АНТИКОРРУПЦИОННАЯ ОГОВОРКА

10.1 При исполнении своих обязательств по Контракту Стороны обязуются
не совершать, а также обязуются обеспечивать, чтобы их аффилированные лица, сотрудники и
посредники не совершали прямо или косвенно следующих действий:
- платить или предлагать уплатить денежные средства или предоставить иные ценности, безвозмездно выполнить работы (оказать услуги) публично-правовым образованиям, должностным лицам публично-правовых образований, близким родственникам таких должностных лиц, либо лицам, иным образом связанным с государством, в целях неправомерного получения преимуществ для сторон по контракту, их аффилированных лиц, работников или посредников, действующих по контракту;
- платить или предлагать уплатить денежные средства или предоставить иные ценности, безвозмездно выполнить работы (оказать услуги) сотрудникам другой стороны по контракту, ее аффилированным лицам, с целью обеспечить совершение ими каких-либо действий в пользу стимулирующей стороны (предоставить неоправданные преимущества, предоставить какие-либо гарантии и т.д.);
- не совершать иных действий, нарушающих антикоррупционное законодательство РФ.

11. ПРОЧИЕ УСЛОВИЯ

11.1. По вопросам, не предусмотренным контрактом, стороны руководствуются действующим законодательством Российской Федерации.
11.2. Стороны обязаны в течение 3-х дней сообщать друг другу об изменении своего места нахождения, почтового адреса, номеров телефонов, факсов и банковских реквизитов
11.3. К контракту прикладывается и является его неотъемлемой частью:
Приложение № 1 – Расчет цены контракта
Приложение № 2 – Техническое задание

12. Адреса, банковские реквизиты, подписи Сторон

ЗАКАЗЧИК:

Государственное бюджетное общеобразовательное учреждение средняя общеобразовательная школа № 661 Приморского района Санкт-Петербурга

Адрес:197082, Санкт-Петербург, ул. Яхтенная, 33 корп. 3, литер А;
ОГРН 1027807583132
ИНН 7814106224 КПП 781401001
ОКПО 52212929 ОКВЭД 85.13
л/с 0641080
Северо-Западное ГУ Банка России//УФК по г. Санкт-Петербургу,
г. Санкт-Петербург
БИК 014030106, к/с 40102810945370000005
р/с 03224643400000007200
тел/факс (812) 246-29-55
Адрес электронной почты: school661spb@yandex.ru

ИСПОЛНИТЕЛЬ:

Общество с ограниченной ответственностью «Цифровые технологии» (ООО «Цифровые технологии»)
Юридический адрес (совпадает с почтовым и фактическим адресом) 191036, город Санкт-Петербург, проспект Невский, дом 111/3, Литер А, пом/ком 19Н/27
ИНН 7842176640 КПП 784201001
ОГРН 1197847226939
ОКПО 42215507 ОКОПФ 12300 ОКФС 16
ОКАТО 40298000000 ОКТМО 40912000000
Банковские реквизиты
Р/с 40702810655000056317
в Северо-Западный банк ПАО СБЕРБАНК
БИК 044030653
К/с 30101810500000000653
тел/факс +7-965-766-90-72

от Заказчика:
Директор

_____ Е.А.Данилова

Подписано ЭЦП

от Исполнителя
Директор

_____/ Ю.А.Терентьева. /

Подписано ЭЦП

Приложение № 1
к Контракту № ЭМ24/661/01
от 20.01.2024

Расчет цены контракта

№	Наименование товара	Ед. изм.	Кол-во	Сумма с/без НДС, руб.	Сумма с/без НДС (руб.)
1	Неисключительное право (универсальная лицензия) на использование Dallas Lock Linux (СЗИ НСД, СКН)/Dallas Lock 8.0-К (СЗИ НСД, СКН) (программное обеспечение)	шт.	**5**	9 300,00	46 500,00
2	Сертифицированный комплект для установки Dallas Lock Linux	шт.	**1**	500,00	500,00
3	Dallas Lock 8.0-К. Сертифицированный комплект для установки	шт.	**1**	500,00	500,00
4	Лицензия: Kaspersky Endpoint Security для бизнеса – Стандартный. 3 year Educational Special License	шт.	**11**	620,00	6 820,00
				Итого	54 320,00
				НДС не облагается	0,00
				ВСЕГО К ОПЛАТЕ	54 320,00

Итого: **54 320 рублей 00 копеек** (пятьдесят четыре тысячи триста двадцать рублей 00 копеек)**,** *НДС не облагается.*

Заказчик:
Директор

_____ / Е.А.Данилова/

(подписано ЭЦП)

Исполнитель :
Директор

_____/ Ю.А.Терентьева. /

(подписано ЭЦП)

Приложение №2
к Контракту № ЭМ24/661/01
от __ _____ 2024г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
Требования к оказываемым услугам

№	Наименование услуги	Технические характеристики	Количество, шт.
1	Неисключительное право (универсальная лицензия) на использование Dallas Lock Linux (СЗИ НСД, СКН)/Dallas Lock 8.0-К (СЗИ НСД, СКН) (программное обеспечение)	ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ к СЗИ НСД DALLAS LOCK LINUX 1. СЗИ НСД должна представлять собой программный комплекс средств защиты информации в операционных системах семейства Linux с возможностью подключения аппаратных идентификаторов для усиления механизма аутентификации. 2. СЗИ НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением следующих операционных систем семейства Linux в многопользовательском режиме их эксплуатации: — Альт Рабочая Станция 9.0 x64 (версия ядра СЗИ НСД 4.19); — Альт Рабочая Станция 9.1 x64 (версия ядра СЗИ НСД 5.10); — Альт Рабочая Станция 9.2 x64 (версия ядра СЗИ НСД 5.10); — Альт Рабочая Станция 10.0 x64 (версия ядра СЗИ НСД 5.10); — Альт Рабочая Станция 10.1 x64 (версия ядра СЗИ НСД 5.10); — Astra Linux Common Edition (Орёл) 2.12.29 x64 (версия ядра СЗИ НСД 4.19); — Astra Linux Common Edition (Орёл) 2.12.40 x64 (версия ядра СЗИ НСД 5.10); — Debian 10 x64 (версия ядра СЗИ НСД 5.10); — Debian 11 x64 (версия ядра СЗИ НСД 5.10); — CentOS 7 x64 (версия ядра СЗИ НСД 3.16); — Red Hat Enterprise Linux 7 x64 (версия ядра СЗИ НСД 3.16); — Ubuntu 18.04 x64 (версия ядра СЗИ НСД 4.19); — Ubuntu 20.04 x64 (версия ядра СЗИ НСД 5.10); — РЕД ОС 7.1, 7.2 Муром x64 (версия ядра СЗИ НСД 4.19); — РЕД ОС 7.3 Муром x64 (версия ядра СЗИ НСД 5.10); — ROSA Enterprise Linux Desktop/Server 7.3 x64 (версия ядра СЗИ НСД 5.10). 3. СЗИ НСД должна поддерживать 64-битные версии операционных систем. 4. СЗИ НСД должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах и ТС с поддержкой виртуальных сред. 5. СЗИ НСД должна быть сертифицирована на соответствие требованиям руководящих документов к 5-му классу защищенности от НСД для СВТ (РД СВТ, Гостехкомиссия России, 1992) и 4-му уровню доверия («Требования по безопасности информации, устанавливающие уровни доверия к СТЗИ и СОБИТ» ФСТЭК России, 2020) разрабатываться и производиться на основании лицензии федеральных органов, имеющих полномочия в указанной сфере. 6. 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). 7. СЗИ НСД может быть использована: — 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. 8. СЗИ НСД должна обеспечивать: 8.1. регистрацию пользователей. Возможность задать пароль пользователя. Определение количества одновременных сеансов для пользователя. Возможность	5

		ограничения количества сессий пользователей на одном компьютере; 8.2. возможность принудительной блокировки пользователей и автоматической блокировки в случае нарушения политик безопасности; 8.3. идентификацию и проверку подлинности пользователей при входе в операционную систему. Возможность двухфакторной аутентификации по паролю и аппаратному идентификатору; 8.4. возможность сохранения авторизационных данных пользователя на аппаратном идентификаторе; 8.5. возможность назначить роль администрирования учетной записи (Администратор, Аудитор, Пользователь ОС); 8.6. возможность задавать расписание работы пользователей; 8.7. возможность авторизации доменных пользователей при отсутствии связи с доменом (Microsoft Active Directory, FreeIPA, Samba); 8.8. возможность сквозной авторизации доменных пользователей на внешних ресурсах; 8.9. возможность управления доменными учетными записями (регистрация , ограничение количества сессий, блокировка, расписание работы, запрос нового пароля, управление аппаратной идентификацией, разграничение доступа к объектам файловой системы, разграничение доступа к блочным устройствам, устройствам вывода на печать); 8.10. реализацию настроек сложности паролей (длины парольной строчки, контроля наличия цифр и специальных символов) и срока их действия; 8.11. возможность настройки разграничения прав доступа к объектам файловой системы, съемным накопителям, разграничения прав на доступ к устройствам печати; 8.12. возможность контроля целостности аппаратной конфигурации компьютера; 8.13. регистрацию и учет (аудит) действий пользователей (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, вывод на печать информации, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки записей; 8.14. возможность периодического архивирования журналов событий; 8.15. возможность экспорта журналов безопасности в форматы PDF, ODS и XML; 8.16. возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов); 8.17. возможность администрирования через графическую оболочку или консоль СЗИ НСД, функционирующую в операционных системах на базе ядра Linux, а также через графическую консоль или оболочку администрирования, функционирующую в операционных системах семейства Windows; 8.18. возможность контроля целостности программно-аппаратной среды (в том числе отдельных каталогов) и произвольных объектов файловой системы при загрузке ПЭВМ, по команде администратора или периодически. Возможность восстановления объекта доступа в случае обнаружения нарушения его целостности; 8.19. контроль целостности объектов СЗИ; 8.20. очистку остаточной информации (освобождаемого дискового пространства, освобождаемых областей оперативной памяти, зачистку определенных файлов и папок по команде пользователя или АИБ); 8.21. возможность проверки корректности функционирования СЗИ НСД, самотестирования; 8.22. возможность обновления СЗИ НСД с выполнением сохранения ранее произведенных настроек СЗИ и экспорта журналов безопасности в форматы PDF, ODS и XML; 8.23. защиту от подмены ядра операционной системы и процедур инициализации; 8.24. возможность настройки всех параметров СЗИ НСД из единой консоли администрирования; 8.25. возможность синхронизации времени ОС с аппаратной платой средства доверенной загрузки для регистрации событий безопасности; 8.26. возможность сетевого режима функционирования с удаленным управлением учетными записями пользователей, получением информации о состоянии работы защищаемых ПЭВМ, удаленным просмотром журналов на ПЭВМ, входящих в домен безопасности; 8.27. централизованное управление защищенными рабочими станциями при помощи специального модуля. С помощью этого модуля должна выполняться синхронизация учетных записей в рамках защищаемого контура, синхронизация политик безопасности, удаленное развертывание и удаление клиентских частей СЗИ НСД, выгрузка журналов клиентов во внешнюю СУБД (SQL); 8.28. возможность централизованного управления защищенными рабочими	

		станциями при помощи отдельного кроссплатформенного центра управления; 8.29. возможность управления встроенным межсетевым экраном, контроль управления портами, а также протоколами; 8.30. возможность оповещения при событиях НСД; 8.31. возможность автоматизированного тестирования памяти, целостности ПО, доступа, авторизации, функции гарантированной очистки оперативной памяти; 8.32. наличие собственного механизма дискреционного управления доступом. 9. Должен быть реализован модуль контроля подключения съемных машинных носителей информации (СКН). Модуль СКН должен обеспечивать: 9.1. контроль использования интерфейсов ввода/вывода средств вычислительной техники, подключения внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации; 9.2. возможность назначения прав доступа к конкретному накопителю; 9.3. возможность установить описание для сменного накопителя. 10. Реализация СЗИ НСД должна быть полностью программной, но с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, а также следующих идентификаторов: USB-ключи Aladdin eToken Pro/Java, 72K, смарт-карты Aladdin eToken Pro/SC, USB-ключи и смарт-карты Рутокен (Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0, Рутокен Lite, Рутокен ЭЦП PKI), электронные ключи Touch Memory (iButton) (DS-1990, DS-1992, DS-1993, DS-1994, DS-1995, DS-1996), USB-ключи и смарт-карты JaCarta (JaCarta SF/ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta LT, JaCarta ГОСТ, JaCarta PKI, JaCarta PRO, JaCarta PKI/Flash), USB-ключи и смарт-карты ESMART (ESMART Token, ESMART Token ГОСТ, ESMART 64k). 11. Поставка СЗИ НСД 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 СЗИ НСД (программное обеспечение). ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К СЗИ НСД DALLAS LOCK 8.0-К (С МОДУЛЕМ СКН) (СБОРКА 761) СЗИ НСД должна представлять собой программный комплекс средств защиты информации в операционных системах (ОС) семейства Windows с возможностью подключения аппаратных идентификаторов. СЗИ НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением операционных систем Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 в многопользовательском режиме их эксплуатации. СЗИ НСД должна поддерживать 32- и 64-битные версии операционных систем. СЗИ НСД должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию Windows To Go. СЗИ НСД должна быть сертифицирована на соответствие требованиям руководящих документов к 5-му классу защищенности от НСД для СВТ (РД СВТ, Гостехкомиссия России, 1992) и 4-му уровню доверия («Требования по безопасности информации, устанавливающие уровни доверия к СТЗИ и СОБИТ», ФСТЭК России, 2020), разрабатываться и производиться на основании лицензии федеральных органов, имеющих полномочия в указанной сфере. 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). СЗИ НСД может быть использована: — 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.

СЗИ НСД должна обеспечивать:

1.1. регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества терминальных сессий на одном компьютере. Возможность автоматического блокирования неактивных учетных записей пользователей;

1.2. идентификацию и проверку подлинности пользователей при входе в ОС. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность задать расписание работы пользователей;

1.3. возможность записи авторизационных данных в идентификатор. Возможность определить принадлежность аппаратного идентификатора конкретному пользователю. Возможность запрета повторного использования идентификатора. Возможность назначить одной учетной записи два аппаратных идентификатора с возможностью авторизации по любому из них;

1.4. возможность ограничения количества неуспешных попыток входа и блокирования устройства;

1.5. возможность автоматизированно сохранять авторизационные данные пользователя в системном кэше ОС при использовании (установке) СЗИ НСД;

1.6. поддержку входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows;

1.7. поддержку аутентификации пользователей с применением биометрии и токенов JaCarta PKI/BIO;

1.8. реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам;

1.9. возможность автоматического выбора аппаратного идентификатора в окне авторизации при входе в ОС;

1.10. возможность настройки принудительной двухфакторной аутентификации для учетной записи с правами администратора и/или пользователя;

1.11. возможность средствами СЗИ НСД выполнить настройку периода действия учетной записи;

1.12. возможность настройки предупреждения пользователя до входа в систему о том, что в информационной системе реализованы меры по обеспечению безопасности информации;

1.13. возможность при создании учетной записи выбрать тип учетной записи (внутренний, внешний, системный, приложение, гостевой, временный);

1.14. независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), реестру, сети, съемным носителям информации. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных;

1.15. контроль аппаратной конфигурации компьютера и следующих подключаемых устройств:

- Android-устройств;
- iOS-устройств;
- Bluetooth-устройств;
- DVD- и CD-ROM-дисководов;
- устройств HID, MTD, PCMCIA, IEEE 1394, Secure Digital;
- USB-контроллеров;
- беспроводных устройств (Wireless Communication Devices);
- биометрических устройств;
- дисководов магнитных дисков;
- звуковых, видео- и игровых устройств;
- инфракрасных устройств (IrDA);
- контроллеров магнитных дисков;
- ленточных накопителей;
- модемов;
- переносных устройств;

		– портов (COM и LPT); – сенсоров; – сетевых адаптеров; – сканеров и цифровых фотоаппаратов; – принтеров; – съемных носителей информации (CD-ROM, FDD, USB-Flash-накопителей); 1.16. контроль устройств, подключаемых к терминальному серверу с RDP-клиентов (контроль перенаправления устройств); 1.17. предотвращение утечки информации с использованием съемных носителей информации. СЗИ НСД должна позволять разграничивать доступ как к отдельным типам носителей, так и к конкретным экземплярам; 1.18. возможность запретить запуск (без команды пользователя) ПО, используемого для взаимодействия со съемными носителями информации; 1.19. возможность запретить установку драйверов съемных носителей информации; 1.20. преобразование информации: – при работе с виртуальными дисками (преобразование выполняется незаметно для пользователя); – при создании преобразованных файлов-контейнеров, используемых для хранения информации на внешних носителях или для передачи по различным каналам связи; 1.21. блокировку виртуальных дисков с преобразованной информацией при отключении аппаратного идентификатора; 1.22. сохранение теневых копий файлов, записываемых на съемные носители; 1.23. автоматическое ограничение доступа к теневой копии, сделанной СЗИ НСД при копировании документа, содержащего информацию ограниченного доступа, на сменный машинный носитель; 1.24. использование дискреционного принципа контроля доступа, обеспечивающего доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа); 1.25. возможность ограничивать средствами СЗИ НСД круг доступных сетевых ресурсов (с точностью до отдельных удаленных рабочих станций и отдельных папок общего доступа); 1.26. регистрацию и учет (аудит) действий пользователей независимыми от ОС средствами (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки и автоматической архивации по истечении установленного интервала времени; 1.27. расширенные возможности аудита печати: печать документов с возможностью добавления штампа (произвольного или по ГОСТ), возможность сохранения теневых копий распечатываемых документов, разграничение доступа пользователей к печати и нанесению штампов; 1.28. возможность добавления произвольного комментария к зарегистрированным событиям НСД; 1.29. возможность экспорта журналов событий в syslog, возможность настройки кодировки экспортируемых в syslog событий; 1.30. возможность организации замкнутой программной среды (ЗПС) и различные способы ее настройки; 1.31. блокировку доступа к файлам по расширению; 1.32. возможность разграничения доступа к буферу обмена; 1.33. возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов); 1.34. возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при выявлении изменений. Возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности;	

1.35. очистку остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Возможность определения метода зачистки. Контроль зачистки при полной зачистке логического диска. Очистку данных сеанса пользователя в оперативной памяти за счет запрета смены пользователя без перезагрузки;

1.36. возможность проверки цифровой подписи объектов файловой системы, находящихся под контролем целостности, при их обновлении;

1.37. выполнение регистрации действий по зачистке остаточной информации;

1.38. самодиагностика основных функциональных возможностей СЗИ НСД и сохранение информации в виде отчета;

1.39. возможность сохранения конфигурации для последующего восстановления СЗИ НСД;

1.40. автоматическое создание точки восстановления при установке СЗИ НСД;

1.41. возможность настройки всех параметров СЗИ НСД из единой консоли администрирования;

1.42. возможность создания отчета по назначенным правам, формирование паспорта программного обеспечения, установленного на ПЭВМ, формирование паспорта аппаратной части ПЭВМ;

1.43. ведение двух копий программных средств защиты информации и возможность возврата к настройкам по умолчанию;

1.44. возможность сигнализации администратору безопасности о следующих инцидентах безопасности (ситуациях сбоя функционирования и ситуациях несанкционированного доступа на клиентских рабочих станциях):

- нарушение контроля целостности объекта;
- попытка работы после блокировки при нарушении целостности;
- попытка входа на клиентскую рабочую станцию с неправильным паролем;
- блокировка пользователя после многократного ввода неправильного пароля;
- СЗИ НСД на клиенте не отвечает (возможная причина – несанкционированная деактивация системы защиты);
- клиент недоступен долгое время (с возможностью задания периода времени);
- попытки монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами;

1.45. централизованное управление защищенными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учетными записями пользователей, группами учетных записей пользователей, политиками, правами пользователей, преобразованными съемными носителями информации. Должна поддерживаться многоуровневая иерархия групп компьютеров и наследование установленных параметров. Также этим модулем должен осуществляться периодический сбор журналов со всех защищенных рабочих станций. Возможность блокировки компьютера, завершения сеанса работы пользователя по команде администратора.

Централизованное управление СЗИ НСД должно обеспечивать:

1.46. возможность настройки репликации серверов безопасности (модулей централизованного управления);

1.47. возможность по управлению доменными учетными записями (создание, удаление, блокировка, перемещение) и группами Active Directory с учетом приоритета механизмов СЗИ над механизмами Active Directory (во избежание злоупотребления доменных администраторов своими полномочиями);

1.48. централизованное управление контролем целостности объектов ФС, системного реестра;

1.49. централизованное управление аппаратными идентификаторами;

1.50. централизованное управление сессиями-исключениями;

1.51. централизованное управление сменными накопителями;

1.52. возможность регистрации сменных накопителей, подключенных к клиентским рабочим станциям;

1.53. возможность блокирования сеанса доступа через средства

		централизованного и удаленного администрирования СЗИ НСД после установленного времени бездействия; 1.54. возможность нотификации о наличии обновлений для СЗИ НСД на сервере компании-разработчика СЗИ НСД; 1.55. возможность настройки места хранения журналов сервера безопасности (выбор локальной папки); 1.56. возможность использования SQL базы данных для централизованного хранения событий аудита; 1.57. возможность построения иерархии управления при помощи специального модуля – менеджера, управляющего несколькими модулями централизованного управления; 1.58. возможность использования механизма удаленной установки и обновления СЗИ НСД средствами модуля централизованного управления самой СЗИ или средствами групповых политик Active Directory с отображением сообщения об окончании удаленной установки с указанием необходимости выполнения перезагрузки. Возможность удаления СЗИ через Active Directory без перезагрузки удаленных ПК. Проверка подписи файлов при обновлении СЗИ НСД; 1.59. возможность визуализации сети защищаемых компьютеров; 1.60. возможность подключения к модулям администрирования пользователя с ограниченными правами (права только на просмотр настроек; только на просмотр журналов аудита; полные права с возможностью делегирования); 1.61. возможность выполнять синхронизацию времени между сервером безопасности и клиентами; 1.62. возможность интеграции с SIEM-системами; 1.63. возможность интеграции с антивирусными системами. Должен быть реализован модуль контроля подключения съемных машинных носителей информации (СКН). Модуль СКН должен обеспечивать: 1.64. контроль использования интерфейсов ввода/вывода средств вычислительной техники, подключения внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации; 1.65. возможность назначения прав доступа к конкретному накопителю; 1.66. возможность установить описание для сменного накопителя. Реализация СЗИ НСД должна быть полностью программной с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, а также аппаратных идентификаторов: — USB-флэш-накопители; — электронные ключи Touch Memory (iButton); — HID Proximity-карты; — USB-ключи Aladdin eToken Pro/Java; — смарт-карты Aladdin eToken Pro/SC; — USB-ключи и смарт-карты Рутокен (Rutoken): Рутокен ЭЦП Flash, Рутокен ЭЦП 2.0 Flash, Рутокен ЭЦП 2.0 Touch, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0, Рутокен ЭЦП Bluetooth, Рутокен ЭЦП PKI, Рутокен Lite, Рутокен S, Рутокен Web, Рутокен Lite SD, Рутокен PINPad, Рутокен 2151; — USB-ключи и смарт-карты JaCarta: JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta PKI, Jacarta PKI/Flash, Jacarta PKI/ГОСТ, Jacarta PKI/ГОСТ/Flash, JaCarta PKI/BIO, JaCarta PRO, JaCarta LT, Jacarta-2 ГОСТ, Jacarta-2 PKI/ГОСТ, Jacarta-2 PKI/BIO/ГОСТ, Jacarta-2 PRO/ГОСТ, JaCarta-2 SE; — USB-ключи и смарт-карты ESMART; — NFC-метки и смарт-карты семейства MIFARE. Поставка СЗИ НСД должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения с указанием всех необходимых модулей и требуемого количества лицензий по каждому модулю. Поставка модуля контроля за изменением состава программного обеспечения и контроля целостности файлов программного обеспечения должна осуществляться совместно с модулем централизованного управления, лицензируются при этом подключения к модулю. Варианты формулировок: — неисключительное право на использование СЗИ (НСД, СКН) (программное обеспечение); — неисключительное право на использование сервера безопасности для СЗИ НСД (программное обеспечение); — неисключительное право на использование сервера лицензий для СЗИ НСД	

		(программное обеспечение); — неисключительное право на подключения к серверу конфигураций для СЗИ НСД; — неисключительное право на терминальное подключение СЗИ НСД (программное обеспечение).	
2	Сертифицированный комплект для установки Dallas Lock Linux	Сертифицированный комплект для установки средства защиты информации от несанкционированного доступа Dallas Lock Linux В комплект входит: Компакт-диск с ПО Dallas Lock Linux (соответствующей версии) и документацией в электронном виде; Формуляр; Копия сертификата ФСТЭК России; Краткое руководство.	1
3	Dallas Lock 8.0-К. Сертифицированный комплект для установки	Сертифицированный комплект для установки средства защиты информации от несанкционированного доступа Dallas Lock 8.0-К. В комплект входит: Компакт-диск с ПО Dallas Lock 8.0-К (соответствующей версии) и документацией в электронном виде; Формуляр; Копия сертификата ФСТЭК России; Краткое руководство.	1
4	Лицензия: Kaspersky Endpoint Security для бизнеса – Стандартный. 3 year Educational Special License	Общие требования Антивирусные средства должны включать: • Программные средства антивирусной защиты для рабочих станций Windows. • Программные средства антивирусной защиты для рабочих станций Linux. • Программные средства антивирусной защиты для рабочих станций Mac OS. • Программные средства антивирусной защиты для файловых серверов Windows. • Программные средства антивирусной защиты для файловых серверов Linux. • Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows. • Программные средства антивирусной защиты для мобильных устройств. • Программные средства централизованного управления, мониторинга и обновления. • Обновляемые базы данных сигнатур вредоносных программ и атак. • Эксплуатационную документацию на русском языке. Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке. Требования к программным средствам антивирусной защиты для рабочих станций Windows Средства антивирусной защиты для рабочих станций Windows должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу В и Г не ниже второго класса защиты. Программные средства антивирусной защиты для рабочих станций Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: • Microsoft Windows 7; • Microsoft Windows 8; • Microsoft Windows 8.1; • Microsoft Windows 10. Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей: • возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью • возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту. • возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего. • возможность читать информацию из записей аудита. • ограничение доступа к чтению записей аудита. • поиск, сортировка и упорядочение данных аудита. • возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности; • возможность уполномоченным пользователям (ролям) управлять режимом	11

		выполнения функций безопасности. • поддержка определенных ролей их ассоциации с конкретными администраторами безопасности или пользователями; • возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации. • возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных. • возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами; • возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой; • возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов, удаления кода из файлов и системных областей носителей информации; • возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы. • отображение сигнала тревоги об обнаружении зараженных файлов • возможность восстановления функциональных свойств зараженных объектов. • возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса; • Возможность контроля доступа к веб-ресурсам; • Возможность контроля за запуском ПО на защищаемой рабочей станции или сервере. Кроме того, программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК: • антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта; • антивирусное сканирование по расписанию; • антивирусное сканирование подключаемых устройств; • эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы; • нейтрализация действий активного заражения; • анализ поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; • анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • блокирование действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов; • возможность совершить откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; • возможность ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений. Динамически обновляемые настраиваемые списки приложений с определением уровня доверия; • возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени для получения вердикта по запускаемой программе или файлу; • антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE в том числе и защищенных паролем; • защита электронной почты от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP; • фильтр почтовых вложений с возможностью переименования или удаления заданных типов файлов; • проверка трафика, поступающего на компьютер пользователя по протоколам	

		HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики; • блокировка баннеров и всплывающих окон на загружаемых Web-страницах; • распознавание и блокировка фишинговых и небезопасных сайтов; • наличие встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные; • контроль сетевых соединений, устанавливаемых с помощью сетевых мостов, с возможностью блокировки одновременной установки нескольких сетевых соединений. • наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп). Компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме MD5 или SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения. Компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки; • осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory; • возможность записи в журнал событий о записи и/или удалении файлов на съемных дисках; • осуществление контроля работы пользователя с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.). Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory; • наличие механизмов защиты от атак типа BadUSB; • запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. • защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; • возможность установки только выбранных компонентов программного средства антивирусной защиты; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; • ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • возможность проверки целостности антивирусной программы; • возможность добавления исключений из антивирусной проверки по хеш сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи; • наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления; • наличие защищенного хранилища для отчетов о работе антивируса; • возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей. Требования к программным средствам антивирусной защиты для рабочих станций Linux Средства антивирусной защиты для рабочих станций Linux должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты –	

		приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу В и Г не ниже второго класса защиты. Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: Поддерживаемые 32-битные операционные системы: • Ubuntu 16.04 LTS; • Red Hat® Enterprise Linux® 6.7; • Red Hat Enterprise Linux 7.2; • CentOS-6.7; • Debian GNU / Linux 8.6; • Debian GNU / Linux 9.4; • Linux Mint 18.2; • Linux Mint 19; • Альт Линукс СПТ 7.0 (работа с графическим пользовательским интерфейсом не поддерживается); • Альт 8 СП Рабочая станция; • Альт 8 СП Сервер • Альт Линукс 8.2 Рабочая станция; • Альт Линукс 8.2 Рабочая станция К; • Альт Линукс 8.2 Сервер; • Альт Линукс 8.2 Образование; • Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6); • Лотос; • РЕД ОС. Поддерживаемые 64-битные операционные системы: • Ubuntu 16.04 LTS; • Ubuntu 18.04 LTS; • Red Hat Enterprise Linux 6.7; • Red Hat Enterprise Linux 7.2; • CentOS-6.7; • CentOS-7.2; • Debian GNU / Linux 8.6; • Debian GNU / Linux 9.4; • OracleLinux 7.3; • SUSE® Linux Enterprise Server 15; • openSUSE® 15; • Альт Линукс СПТ 7.0 (работа с графическим пользовательским интерфейсом не поддерживается); • Альт 8 СП Рабочая станция; • Альт 8 СП Сервер; • Альт Линукс 8.2 Рабочая станция; • Альт Линукс 8.2 Рабочая станция К; • Альт Линукс 8.2 Сервер; • Альт Линукс 8.2 Образование; • Amazon Linux AMI; • Linux Mint 18.2; • Linux Mint 19; • Micro Focus Open Enterprise Server 2018; • Astra Linux Special Edition 1.5 (обычный режим и режим замкнутой программной среды); • Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды); • Astra Linux Common Edition 2.12; • программный комплекс терминального доступа «Циркон 36КТ»; • программный комплекс терминального доступа «Циркон 36СТ»; • ОС РОСА «КОБАЛЬТ» (версия 7.3 для клиентских систем); • ОС РОСА «КОБАЛЬТ» (версия 7.3 для серверных систем); • ЕМИАС 1.0; • Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6); • Лотос; • РЕД ОС. Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей:	

		• Возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту. • Возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего. • Возможность читать информацию из записей аудита. • Ограничение доступа к чтению записей аудита. • Поиск, сортировка и упорядочение данных аудита. • Возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности; • Поддержка определенных ролей их ассоциации с конкретными администраторами безопасности и администраторами серверов или пользователями; • возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности; • Возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации. • Возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных. • Возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами. • Возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой; • Возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов, удаления кода из файлов и системных областей носителей информации; • Возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы. • отображение сигнала тревоги об обнаружении КВ • Возможность восстановления функциональных свойств зараженных объектов. • Возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса. Кроме того, программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК: • резидентный антивирусный мониторинг; • возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени для получения вердикта по запускаемой программе или файлу; • проверка ресурсов доступных по SMB / NFS; • эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; • антивирусное сканирование по команде пользователя или администратора и по расписанию; • антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.; • проверка сообщений электронной почты в текстовом формате (Plain text); • наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов); • защита файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования; • помещение подозрительных и поврежденных объектов на карантин; • проверка почтовых баз приложений Microsoft Outlook • возможность перехвата и проверки файловых операций на уровне SAMBA; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность экспортировать и сохранять отчеты в форматах HTML и CSV; • гибкое управление использованием ресурсов ПК для обеспечения комфортной	

		работы пользователей при выполнении сканирования файлового пространства; • сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность; • настройка возможности управления через пользовательский графический интерфейс без root прав; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • возможность добавления точек монтирования в глобальные исключения; • возможность отслеживать целостность указанных файлов в режиме мониторинга в реальном времени и в режиме проверки по требованию. Требования к программным средствам антивирусной защиты для рабочих станций Mac Средства антивирусной защиты для рабочих станций Mac должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты. Программные средства антивирусной защиты для рабочих станций Mac должны функционировать на компьютерах на базе процессора Intel, работающих под управлением операционных систем следующих версий: • macOS 10.13 High Sierra; • macOS 10.12 Sierra; • OS X 10.11 El Capitan; • OS X 10.10 Yosemite; • OS X 10.9 Mavericks. Программные средства антивирусной защиты для рабочих станций Mac должны обеспечивать реализацию следующих функциональных возможностей: • Возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту. • Возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего. • Возможность читать информацию из записей аудита. • Ограничение доступа к чтению записей аудита. • Поиск, сортировка и упорядочение данных аудита. • Возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности; • Возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности. • Поддержка определенных ролей их ассоциации с конкретными администраторами безопасности, администраторами серверов и пользователями. • Возможность выполнять проверки с целью обнаружения зараженных объектов. • Возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных. • Возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами. • Возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам. • Возможность выполнять проверки с целью обнаружения зараженных объектов путем запуска с необходимыми параметрами функционирования своего кода внешней программой. • Возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из зараженных объектов; • Возможность отображения сигнала тревоги на рабочей станции администратора безопасности; • Возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения. Кроме того, программные средства антивирусной защиты для рабочих станций Mac должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК: • Резидентный антивирусный мониторинг. • Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы. • Антивирусное сканирование по команде пользователя или администратора и по расписанию.	

		• Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось. • Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления. • Возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени для получения вердикта по запускаемой программе или файлу. • Защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные. • Блокировка вредоносных и фишинговых сайтов на основе вердиктов локальных репутационных облачных сервисов производителя антивирусных средств защиты. • Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, HTTPS. • Автоматическое обновление антивирусных баз по расписанию. • Защита информации, передаваемой через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик). • Возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы • Требования к программным средствам антивирусной защиты для файловых серверов Windows Средства антивирусной защиты для файловых серверов Windows должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты. Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: • Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1; • Microsoft Windows Server 2008 Standard / Enterprise x86 Edition SP2; • Microsoft Windows Server 2008 Standard / Enterprise x64 Edition SP2; • Microsoft Windows Small Business Server 2011 Essentials / Standard x64 Edition; • Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition; • Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition; • Microsoft Windows MultiPoint Server 2012 x64 Edition; • Microsoft Windows Server 2016. Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей: • возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью • возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту. • возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего. • возможность читать информацию из записей аудита. • ограничение доступа к чтению записей аудита. • поиск, сортировка и упорядочение данных аудита. • возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности; • возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности. • поддержка определенных ролей их ассоциации с конкретными администраторами безопасности или пользователями; • возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации. • возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных. • возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами; • возможность выполнять проверки с целью обнаружения зараженных объектов	

		по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой; • возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов, удаления кода из файлов и системных областей носителей информации; • возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы. • отображение сигнала тревоги об обнаружении зараженных файлов • возможность восстановления функциональных свойств зараженных объектов. • возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса; • Возможность контроля за запуском ПО на защищаемой рабочей станции или сервере. Кроме того, программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК: • антивирусное сканирование в режиме реального времени и по запросу; • антивирусное сканирование по команде пользователя или администратора и по расписанию; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени для получения вердикта по запускаемой программе или файлу; • наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ. • защита от сетевых атак с использованием правил сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные. • запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям; • антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем. • ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • настройки проверки критических областей сервера в качестве отдельной задачи; • регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме; • наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий); • защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; • наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, а также обеспечивать возможность исключения из правил для определенных пользователей из Active Directory; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; Требования к программным средствам антивирусной защиты для файловых серверов Linux Средства антивирусной защиты для файловых серверов Linux должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты –	

		приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты. Программные средства антивирусной защиты для файловых серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: Поддерживаемые 32-битные операционные системы: • Ubuntu 16.04 LTS; • Red Hat® Enterprise Linux® 6.7; • Red Hat Enterprise Linux 7.2; • CentOS-6.7; • Debian GNU / Linux 8.6; • Debian GNU / Linux 9.4; • Linux Mint 18.2; • Linux Mint 19; • Альт Линукс СПТ 7.0 (работа с графическим пользовательским интерфейсом не поддерживается); • Альт 8 СП Рабочая станция; • Альт 8 СП Сервер • Альт Линукс 8.2 Рабочая станция; • Альт Линукс 8.2 Рабочая станция К; • Альт Линукс 8.2 Сервер; • Альт Линукс 8.2 Образование; • Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6); • Лотос; • РЕД ОС. Поддерживаемые 64-битные операционные системы: • Ubuntu 16.04 LTS; • Ubuntu 18.04 LTS; • Red Hat Enterprise Linux 6.7; • Red Hat Enterprise Linux 7.2; • CentOS-6.7; • CentOS-7.2; • Debian GNU / Linux 8.6; • Debian GNU / Linux 9.4; • OracleLinux 7.3; • SUSE® Linux Enterprise Server 15; • openSUSE® 15; • Альт Линукс СПТ 7.0 (работа с графическим пользовательским интерфейсом не поддерживается); • Альт 8 СП Рабочая станция; • Альт 8 СП Сервер; • Альт Линукс 8.2 Рабочая станция; • Альт Линукс 8.2 Рабочая станция К; • Альт Линукс 8.2 Сервер; • Альт Линукс 8.2 Образование; • Amazon Linux AMI; • Linux Mint 18.2; • Linux Mint 19; • Micro Focus Open Enterprise Server 2018; • Astra Linux Special Edition 1.5 (обычный режим и режим замкнутой программной среды); • Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды); • Astra Linux Common Edition 2.12; • программный комплекс терминального доступа «Циркон 36КТ»; • программный комплекс терминального доступа «Циркон 36СТ»; • ОС РОСА «КОБАЛЬТ» (версия 7.3 для клиентских систем); • ОС РОСА «КОБАЛЬТ» (версия 7.3 для серверных систем); • ЕМИАС 1.0; • Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6); • Лотос; • РЕД ОС. Программные средства антивирусной защиты для файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей:	

		• Возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту. • Возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего. • Возможность читать информацию из записей аудита. • Ограничение доступа к чтению записей аудита. • Поиск, сортировка и упорядочение данных аудита. • Возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности; • Поддержка определенных ролей их ассоциации с конкретными администраторами безопасности и администраторами серверов или пользователями; • возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности; • Возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации. • Возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных. • Возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами. • Возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой; • Возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов, удаления кода из файлов и системных областей носителей информации; • Возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы. • отображение сигнала тревоги об обнаружении КВ • Возможность восстановления функциональных свойств зараженных объектов. • Возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса. Кроме того, программные средства антивирусной защиты для файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК: • резидентный антивирусный мониторинг; • возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени для получения вердикта по запускаемой программе или файлу; • проверка ресурсов доступных по SMB / NFS; • эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; • антивирусное сканирование по команде пользователя или администратора и по расписанию; • антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.; • проверка сообщений электронной почты в текстовом формате (Plain text); • наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов); • защита файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования; • помещение подозрительных и поврежденных объектов на карантин; • проверка почтовых баз приложений Microsoft Outlook • возможность перехвата и проверки файловых операций на уровне SAMBA; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность экспортировать и сохранять отчеты в форматах HTML и CSV; • гибкое управление использованием ресурсов ПК для обеспечения комфортной	

		работы пользователей при выполнении сканирования файлового пространства; • сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность; • настройка возможности управления через пользовательский графический интерфейс без root прав; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • возможность добавления точек монтирования в глобальные исключения; • возможность отслеживать целостность указанных файлов в режиме мониторинга в реальном времени и в режиме проверки по требованию. Требования к программным средствам антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows Средства антивирусной защиты серверов масштаба предприятия и терминальных серверов Windows должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты. Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: • Small Business Server 2008 • Windows MultiPoint Server 2011 • Windows Storage Server 2012, 2012 R2, 2016 • Windows Server 2008, 2008R2 • Windows Server 2012, 2012 R2 • Windows Server 2016 • Windows Hyper-V Server Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны функционировать на следующих типах терминальных серверов: • Microsoft Remote Desktop Services на базе Windows 2008 Server; • Microsoft Remote Desktop Services на базе Windows 2008 R2 Server; • Microsoft Remote Desktop Services на базе Windows 2012 Server; • Microsoft Remote Desktop Services на базе Windows 2012 Server R2; • Microsoft Remote Desktop Services на базе Windows Server 2016; • Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15; • Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15. Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны обеспечивать реализацию следующих функциональных возможностей: • возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту; • возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего; • возможность читать информацию из записей аудита; • ограничение доступа к чтению записей аудита; • поиск, сортировка и упорядочение данных аудита; • возможность уполномоченным пользователям (ролям) управлять данными (административными данными), используемыми функциями безопасности; • возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности; • поддержка определенных ролей их ассоциации с конкретными администраторами безопасности и пользователями; • возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных; • возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами; • возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой; • возможность удаления (если технически возможно) файлов, в которых обнаружен вредоносный код, а также файлов, подозрительных на наличие вредоносного кода, перемещение и изолирование объектов воздействия; • возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на	

		которых обнаружены зараженные файлы; • возможность отображение сигнала тревоги об обнаружении на рабочей станции администратора, в том числе до подтверждения его получения или до завершения сеанса; • возможность восстановления функциональных свойств зараженных объектов; • возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения; • возможность выполнять проверки с целью обнаружения атаки эксплойтов в памяти процессов, в контейнерах Windows Server 2016; • возможность при обнаружении признаков атаки эксплойтов на защищаемый процесс завершать процесс, сообщать о факте дискредитации уязвимости в процессе. Кроме того, программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК: • антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: Серверов терминалов и принт-серверов; Серверов приложений и контроллеров доменов; Файловых серверов; • антивирусное сканирование по команде пользователя или администратора и по расписанию; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу; • антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем; • защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков; • непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting). Проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными. Анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • Возможность проверки контейнеров Microsoft Windows. • Механизмы защиты от эксплуатирования уязвимостей в памяти процессов с помощью техник снижения рисков; • ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи; • настройки проверки критических областей сервера в качестве отдельной задачи; • регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме; • Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий); • возможность интеграции с SIEM системами; • возможность указания количества рабочих процессов антивируса в ручную; • наличие удаленной и локальной консоли управления; • управления параметрами антивируса из командной строки; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; Требования к программным средствам антивирусной защиты мобильных устройств Средства антивирусной защиты мобильных устройств должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу В не ниже четвертого класса защиты. Программные средства для антивирусной защиты мобильных устройств должны функционировать под управлением следующих мобильных ОС: Android 4.2, 4.3, 4.4, 5.0, 5.1, 6.0, 7.0, 7.1, 8.0, 9.0. Программные средства антивирусной защиты мобильных устройств должны	

		обеспечивать реализацию следующих функциональных возможностей: • поддержка определенных ролей для программного изделия и их ассоциации с конкретными администраторами безопасности и пользователями ИС; • уполномоченным пользователям (ролям) управлять режимом и параметрами настройки выполнения функций безопасности программного изделия; • получения и установки обновлений без применения средств автоматизации; • Аудит безопасности: а) генерация записи аудита для событий, подвергаемых аудиту; б) чтение информации из записей аудита; в) ассоциация событий аудита с идентификаторами субъектов; г) ограничение доступа к чтению записей аудита; д) поиск, сортировка, упорядочение данных аудита; • выполнение проверки с целью обнаружения компьютерного вируса в файловых областях носителей информации; • выполнение проверки с целью обнаружения зараженных компьютерным вирусом объектов по команде администратора безопасности, пользователя информационной системы в режиме динамического обнаружения в процессе выполнения операций доступа к объектам; • выполнение проверки с целью обнаружения зараженных компьютерным вирусом объектов сигнатурными и эвристическими методами; удаление (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из зараженных объектов. Кроме того, средства антивирусной защиты мобильных устройств должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК: • Решение должно централизованно управлять с помощью единой консоли управления. • Постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с помощью репутационных облачных сервисов производителя антивирусных средств защиты. • Проверка устанавливаемых приложений. • Проверка файловой системы устройства по требованию и по расписанию. • Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты. Поддержка белых списков разрешенных сайтов. • Наличие хранилища для изолирования зараженных объектов. • Обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию • Блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений. Поддержка белых списков разрешенных приложений. • Блокировка системных приложений. • Возможность получения политик безопасности через Google Cloud Messaging. • Базовая поддержка Android for Work. • Наличие возможности создания специальной оболочки для мобильных программ с целью контроля действий программы, возможностью удаления данных и настроек программы, добавления дополнительного пароля для старта приложения, в том числе с помощью учетных данных Active Directory. • Возможность заблокировать WI-FI и Bluetooth модули, а также использование камеры мобильного устройства. • Указание параметров подключения к WI-FI сетям. • Наличие возможности указания обязательных к установке приложений. • Блокирование нежелательных SMS сообщений. • Возможность блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset). • Постоянная проверка телефона на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий. • Возможность получения текущего номера SIM-карты телефона посредством СМС, возможность автоматической блокировки устройства при смене SIM-карты или при включении телефона без SIM-карты. • Поддержка технологий Samsung KNOX1 и KNOX2. Требования к программным средствам централизованного управления, мониторинга и обновления Средства централизованного управления, мониторинга и обновления должны быть	

		сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу А не ниже второго класса защиты. Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: • Microsoft Windows 7 • Microsoft Windows 8 • Microsoft Windows 8.1 • Microsoft Windows 10 • Windows Server 2008, 2008R2 • Windows Server 2012, 2012 R2 • Windows Server 2016 Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: • Microsoft SQL Server® 2008 Express 32-разрядная; • Microsoft SQL 2008 R2 Express 64-разрядная; • Microsoft SQL 2012 Express 64-разрядная; • Microsoft SQL 2014 Express 64-разрядная; • Microsoft SQL Server 2008 (все редакции) 32-разрядная / 64-разрядная; • Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная; • Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная; • Microsoft SQL Server 2012 (все редакции) 64-разрядная; • Microsoft SQL Server 2014 (все редакции) 64-разрядная; • Microsoft SQL Server 2016 (все редакции) 64-разрядная; • Microsoft Azure SQL Database; • MySQL 5.5 32-разрядная / 64-разрядная (не поддерживаются версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5); • MySQL Enterprise 5.5 32-разрядная / 64-разрядная; • MySQL 5.6 32-разрядная / 64-разрядная; • MySQL Enterprise 5.6 32-разрядная / 64-разрядная; • MySQL 5.7 32-разрядная / 64-разрядная; • MySQL Enterprise 5.7 32-разрядная / 64-разрядная. Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей: • Возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту. • Возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего. • Возможность читать информацию из записей аудита. • Ограничение доступа к чтению записей аудита. • Поиск, сортировка данных аудита. • возможность создания учетных записей и аутентификации пользователей; • возможность администраторам безопасности управлять режимом выполнения функций безопасности • возможность отображения сигнала тревоги на автоматизированное рабочее место (АРМ) администратора безопасности, указывающего на обнаружение вредоносных компьютерных программ (вирусов) на пользовательских автоматизированных рабочих местах; • возможность идентифицировать автоматизированные рабочие места, порождающее событие аудита, вредоносные компьютерные программы (вирусы), которые были обнаружены, и действие, предпринятое средством антивирусной защиты; • возможность продолжать отображение сигнала тревоги на автоматизированном рабочем месте администратора безопасности, пока не будет получено подтверждение его получения или пока не будет завершен сеанс администратора безопасности; • Возможность получения и установки обновлений антивирусных баз в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения. • Возможность централизованной установки компонентов антивирусной защиты на серверы и рабочие станции вычислительной сети. • возможность обработки зараженных объектов на АРМ и серверах вычислительной сети; • возможность выполнения автоматизированного запуска системы защиты на АРМ и серверах вычислительной сети с заданными условиями поиска и режимами реагирования по расписанию; выполнение удаленного администрирования процессов	

		обнаружения КВ, обновления баз данных и компонентов системы защиты; • возможность создания учетных записей и аутентификации пользователей. Кроме того, программные средства централизованного управления, мониторинга и обновления должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК: • Установка системы управления антивирусной защиты из единого дистрибутива. • Выбор установки в зависимости от количества защищаемых узлов. • Возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации. • Возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети. • Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD. • Централизованные установка, обновление и удаление программных средств антивирусной защиты. Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе. • Централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления. • Сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям. • Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки. • Возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от УЗ, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности. Должна быть реализована возможность поддержки иерархии таких триггеров. • Автоматизированный поиск уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей. • Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка обновлений на рабочие места пользователей сразу после их получения. • Распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере. • Построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне. • Создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня. • Поддержка мультиарендности (multi-tenancy) для серверов управления. • Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации. • Доступ к локальным репутационным облачным серверам производителя антивирусного ПО через сервер управления. • Автоматическое распространение лицензии на клиентские компьютеры. • Инвентаризация установленного ПО и оборудования на компьютерах пользователей. • Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них. • Функция управления мобильными устройствами через сервер Exchange ActiveSync. • Функция управления мобильными устройствами через сервер iOS MDM. • Возможность отправки SMS-оповещений о заданных событиях. • Централизованная установка приложений на управляемые мобильные устройства. • Централизованная установка сертификатов на управляемые мобильные устройства. • Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления. • Возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу	

		централизованного управления для снижения сетевой нагрузки на систему управления. • Построение графических отчетов как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и т.д. • Наличие преднастроенных стандартных отчетов о работе системы. • Экспорт отчетов в файлы форматов PDF и XML. • Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение. • Создание внутренних учетных записей для аутентификации на сервере управления. • Создание резервной копии системы управления встроенными средствами системы управления. • Поддержка Windows Failover Clustering. • Поддержка интеграции с Windows сервисом Certificate Authority. • Наличие веб-консоли управления приложением. • Наличие портала самообслуживания пользователей. Портал самообслуживания должен обеспечивать возможность подключения пользователей с целью: Установки агента управления на мобильное устройство, просмотр мобильных устройств, отправка команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя. • Наличие системы контроля возникновения вирусных эпидемий. Требования к обновлению антивирусных баз Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей: • Регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток. • Множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации. • Проверку целостности и подлинности обновлений средствами электронной цифровой подписи. Требования к эксплуатационной документации Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе: • Руководство пользователя (администратора). Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты. Требования к технической поддержке Техническая поддержка антивирусного программного обеспечения должна: • Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по телефону, электронной почте и через Интернет. • Web-сайт производителя АПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов. Срок действия лицензии – 3 (три) года.	

Заказчик:
Директор ГБОУ школа № 661 Приморского района Санкт-Петербурга

_____ / Е.А.Данилова/

(подписано ЭЦП)

Исполнитель:
Директор ООО «Цифровые технологии»

_____/ Ю.А.Терентьева. /

(подписано ЭЦП)