АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ЮЖНЫЙ РЕГИОНАЛЬНЫЙ ЦЕНТР ПОДДЕРЖКИ ЭКСПОРТА»

295024, Россия, Республика Крым, г. Симферополь,
ул. Севастопольская, д. 8, офис 16
ИНН/КПП 9102223852 / 910201001 ОГРН 1179102001440
Тел.: + 7 (978) 990-79-24 E-mail: exportrk2018@yandex.ru Сайт: exporteram.ru

Настоящее техническое задание разработано с целью определения, поставки и настройки Автономной некоммерческой организации «Южный региональный Центр поддержки экспорта» (далее – Заказчик) состава и содержания услуг по обеспечению безопасности информации в информационных системах Заказчика.

Максимально допустимая сумма договора - 600 000, 00 руб.

Сбор коммерческих предложений до 24.11.2023.

1. Используемые сокращения

ИС – информационная система.
ИСПДн – информационная система персональных данных.
ОС – операционная система
СЗИ – средство защиты информации
МЭ – межсетевой экран
САЗ – средство антивирусной защиты
СДЗ – средство доверенной загрузки
СОВ – система обнаружения вторжений
СЗИ от НСД – средство защиты информации от несанкционированного доступа.
ПО – программное обеспечение.
ФСБ России – Федеральная служба безопасности Российской Федерации.
ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

2. Исходные данные об объекте информатизации Заказчика

Объект информатизации находится по адресу 295013, КРЫМ РЕСПУБЛИКА, Г. СИМФЕРОПОЛЬ, УЛ. СЕВАСТОПОЛЬСКАЯ, Д. 8, ОФИС 16 (Заказчик выполнения работ): Автономная некоммерческая организация «Южный региональный Центр поддержки экспорта».

3. Правовые основания для оказания услуг

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

− Постановление Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 года;

− Постановление Правительства Российской Федерации № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 года;

− Постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

− Постановление Правительства РФ от 16.11.2015г. №1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»;

− Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

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

− Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности и хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

− ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положение»;

− ГОСТ РО 0043-003-2012 «Аттестация объектов информатизации. Общие положения».

4. Состав, описание и содержание услуг, требования к документированию

В рамках закупки Исполнитель обязан оказать услуги по поставке средств защиты информации в соответствии с количеством и характеристиками, указанными в таблице.

Таблица

№ п/п	Наименование	Характеристики	Кол-во
1	Программно-аппаратный комплекс межсетевого экранирования	**Требования к Системе** **Требования к поставке** Система должна поставляться в виде программно-аппаратного комплекса и обеспечивать контроль не менее чем 10 единовременно подключенных пользователей на пропускной способности канала не менее 100 Мб/с. Требования к аппаратной составляющей комплекса: • Год выпуска поставляемого оборудования – не ранее 2020 года. • Поставляемое оборудование должно быть собрано в промышленных условиях, удовлетворяющих стандарту ISO9001, иметь сертификаты соответствия требованиям системы сертификации ЕАС. • Исполнитель должен обеспечить срок гарантийного обслуживания не менее 3 (трех) лет. • Поставка должна производиться в запечатанной упаковке, обеспечивающей сохранность содержимого и невозможность использования третьими лицами без ее повреждения. • В Системе должны быть установлены и настроены все обновления доступные на момент приобретения оборудования, все драйвера чипсета и устройств, входящих в комплектацию оборудования, а также необходимые утилиты, обеспечивающие полноценное функционирование Системы. **Аппаратная платформа** **размеры, ВхШхГ** не более 230 х 170 х47 мм **Типоразмер корпуса** Настольный (значение не меняется) **Количество портов** 1000Base-T, RJ-45 не менее 5 шт. **CPU (процессор)** Количество процессоров: 1 Количество ядер: 4 Количество потоков: 4 Базовая тактовая частота процессора: 2,0 ГГц	1

№ п/п	Наименование	Характеристики	Кол-во
		Максимальная тактовая частота с технологией Turbo Boost: 2.42 GHz Кэш-память: 2 MB Cache Частота системной шины: 9.6 GT/s QPI Кол-во соединений QPI: 2 Расчетная мощность: 10 Вт **Дисковое пространство** 1x500 Гбайт **Оперативная память** 8 Гбайт **Входное напряжения БП** 140-220 В **Ток** до 4 А **Энергопотребление** не более 36 Вт **Вес** не более 1.2 кг **Требования к программной составляющей комплекса:** 1. Наличие следующих основных функций: 1.1. контроль доступа пользователей в сеть Интернет и фильтрации трафика сети Интернет; 1.2. анализ трафика сети Интернет по категориям сайтов, URL-адресам и контенту данных; 1.3. мониторинг действий, совершаемых пользователями при работе с сетью Интернет, а также формирование отчетности; 1.4. предоставление возможности обновлять списки с помощью офлайн обновлений; 1.5. защита объектов сетевой инфраструктуры заказчика от DoS атак; 1.6. контроль технологических протоколов АСУ ТП: Modbus, DNP3, MMS; 1.7. возможность встраивания в сетевую инфраструктуру заказчика по протоколу WCCP; 1.8. защита объектов сетевой инфраструктуры с помощью системы обнаружения вторжений (СОВ); 1.9. контроль передаваемого трафика через МСЭ с помощью определения приложений L7. 2. Особенности реализации функций 2.1. Функционал настройки средств фильтрации входящего и исходящего трафика должен	

№ п/п	Наименование	Характеристики	Кол-во
		позволять указывать в качестве фильтра маску или регулярное выражение. 2.2. Должна быть обеспечена возможность применения правил МСЭ к фрагментированным, нефрагментированным и любым другим пакетам. 2.3. Необходимо наличие события об успешной загрузке системы в журнале событий. 2.4. Должно быть обеспечено журналирование изменения времени в консоли администрирования. 2.5. Необходимо наличие оповещений по SNMP при срабатывании запрещающих правил межсетевого экрана. 2.6. Должна обеспечиваться блокировка всего трафика при инцидентах, таких как нарушение функционирования системы. В случае если исполняемый файл из состава МСЭ изменен, весь трафик должен быть заблокирован. 2.7. Функционал решения должен иметь возможность запрашивать ввод пароля на разблокировку в случае несанкционированного доступа к изменениям правил МСЭ, изменениям правил оповещения, сетевым интерфейсам, добавлению учетной записи нового администратора, экспорту логов системы. 2.8. Должна быть обеспечена возможность удаленного подключения технической поддержки в случае полного падения системы (решения). 2.9. Фильтрация входящего и исходящего Интернет-трафика должна осуществляться с одновременным обеспечением проверки на наличие вредоносного программного обеспечения. 2.10. Средства, реализующие функционал мониторинга работоспособности и формирования отчетности, должны предоставлять функционал автоматизированного получения данных о действиях пользователей, совершаемых в сети Интернет, от средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет.	

№ п/п	Наименование	Характеристики	Кол-во
		2.11. Средства контроля доступа в сеть Интернет и фильтрации трафика сети Интернет, должны предоставлять следующую функциональность: 2.11.1. работать в качестве непрозрачного и прозрачного сервера-Интернет и обеспечивать кэширование HTTP, HTTPS; 2.11.2. поддерживать аутентификацию пользователей, интегрироваться с доменами, построенными на базе Microsoft Active Directory и поддерживать технологию Single Sign-On; 2.11.3. поддерживать аутентификацию пользователей с внешними серверами Radius, Kerberos, NTLM, Active Directory, локальной базой учетных записей; 2.11.4. поддерживать идентификацию пользователей с помощью протокола Radius accounting; 2.11.5. поддерживать идентификацию пользователей по IP/MAC-адресам, идентификаторам VLAN; 2.11.6. поддерживать аутентификацию пользователей, работающих на терминальных серверах Microsoft Windows, и на рабочих станциях, работающих под управлением ОС Microsoft Windows, с использованием агентов авторизации. 2.11.7. обеспечивать разделение прав при доступе к сети Интернет на основе доменных и локальных групп и поддерживать управление разрешениями; 2.11.8. обеспечивать категорирование ресурсов сети Интернет и обеспечивать фильтрацию доступа пользователей на основе данных категорий; 2.11.9. предоставлять возможность переопределения категории сайтов; 2.11.10. обеспечивать фильтрацию доступа пользователей к ресурсам сети Интернет на основе контентной фильтрации; 2.11.11. поддерживать и автоматически обновлять базу данных ресурсов сети Интернет и присвоенных им категорий; 2.11.12. поддерживать и автоматически обновлять список сайтов на основе единой автоматизированной информационной системы	

№ п/п	Наименование	Характеристики	Кол-во
		«Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено»; 2.11.13. обеспечивать фильтрацию передаваемого контента и блокировку определенных типов файлов, в том числе в SSL-трафике, включая трафик, зашифрованный с помощью протокола TLSv1.3; 2.11.14. предоставлять функционал гибкой настройки правил фильтрации на основе различных параметров, в частности, групп доступа пользователей, категорий ресурсов, отдельных ресурсов (в том числе ресурсов, не отнесенных ни к одной из категорий) и типов передаваемого контента; 2.11.15. предоставлять интегрированные механизмы оповещения и уведомления администраторов и пользователей о событиях; 2.11.16. предоставлять клиента для авторизации на АРМ пользователей; 2.11.17. предоставлять возможность применения фильтрации на основе информации о реферере; 2.11.18. предоставлять возможность применения правил в указанные временные интервалы. 3. Требования к доступности и производительности 3.1. Программное обеспечение должно иметь возможность быть реализованным в соответствии с методом обеспечения высокой доступности, гарантируя минимальное время простоя, и полного решения возложенных задач при выходе из строя одного из компонентов. 3.2. Программное обеспечение должно обеспечивать резервное копирование конфигураций компонентов и журналов регистрации событий с функцией исторического хранения данных с глубиной хранения не менее 12 месяцев.	

№ п/п	Наименование	Характеристики	Кол-во
		3.3. Программное обеспечение должно обеспечивать доступ в сеть Интернет не менее чем для 10 пользователей, подключенных к Интернет, при этом не оказывая влияния на скоростные показатели доступа пользователей в сеть Интернет и не препятствуя функционированию компонентов корпоративной информационной вычислительной сети Заказчика. 3.4. Программное обеспечение должно иметь возможность масштабирования. Увеличение числа обслуживаемых пользователей и объема обрабатываемого трафика сети Интернет должно осуществляться путем подключения дополнительных программно-аппаратных компонентов. 3.5. При наличии дополнительных узлов программное обеспечение должно позволять в любое время выводить часть узлов фильтрации из эксплуатации для обслуживания с автоматическим перераспределением нагрузки на оставшиеся узлы прозрачно для пользователей. 3.6. Должен обеспечиваться функционал настройки программно-аппаратных средств, входящих в состав, без остановки всей Системы. 3.7. Программное обеспечение должно обеспечивать функцию планового отключения для выполнения профилактических мероприятий, изменений или наращивания аппаратного обеспечения, установки обновлений на программное обеспечение. 3.8. Программное обеспечение должно предоставлять инструменты диагностирования состояния собственных компонентов. 3.9. В Программном обеспечении должна быть предусмотрена ролевая модель разграничения доступа. Роли должны иметь ограничения по доступу к Программному обеспечению на уровне интерфейсов, функционала, отчетов и производственных объектов. 4. Требования к функционалу средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет. 4.1. Обеспечение и контроль доступа пользователей в сеть Интернет с фильтрацией	

№ п/п	Наименование	Характеристики	Кол-во
		входящего и исходящего Интернет-трафика по протоколам HTTP/HTTPS. 4.2. Проверка подлинности пользователей при доступе в сеть Интернет с использованием службы каталогов Microsoft Active Directory. 4.3. Контроль доступа пользователей в сеть Интернет с функционалом установки различных политик доступа для различных групп пользователей на основе членства в группах безопасности службы каталогов Microsoft Active Directory. 4.4. Управление доступом к сайтам сети Интернет на основе «чёрных» и «белых» списков, составленных с использованием категоризации сайтов. Функционал настройки фильтрации входящего и исходящего трафика должен позволять указывать в качестве фильтра маску или регулярное выражение. Списки категорий сайтов должны предоставляться производителем средств контроля доступа в сеть Интернет. Для Администраторов программного обеспечения должна быть реализована функция внесения корректировок в данные списки, а также создания собственных категорий. Списки должны формироваться путём внесения не только одиночных сайтов, но и их списков (в формате текстовых файлов с разделителями). 4.5. Управление доступом в сеть Интернет программ и сетевых служб путём разрешения и назначения портов. 4.6. Отключение функционала контроля доступа в сеть Интернет и фильтрации трафика сети Интернет для конкретных пользователей/IP-адресов. 4.7. Управление доступом пользователей к различным типам информации в сети Интернет (видео, аудио, изображения и т.д.). 4.8. Предоставление интерфейса гибкой настройки правил фильтрации на основе различных параметров, в частности, групп доступа пользователей, категорий ресурсов (в том числе и ресурсов, не отнесенных ни к одной из категорий) и типов передаваемого контента. 4.9. Настраиваемые оповещения администраторов Системы о событиях в работе средств контроля	

№ п/п	Наименование	Характеристики	Кол-во
		доступа в сеть Интернет и фильтрации трафика сети Интернет. 4.10. Уведомление в окне браузера пользователя сети Интернет о блокировании доступа к запрашиваемому пользователем web-ресурсу в случае нарушения корпоративных требований информационной безопасности, а также на основании наличия потенциально опасного кода (с функцией правки кода и текста уведомления). 5. Требования к функционалу средств контентного анализа: 5.1. Получение информации от средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет. 5.2. Обеспечение следующих видов фильтрации (анализа) передаваемого контента: 5.2.1. анализ передаваемых объектов по типу передаваемых объектов, в том числе определение и корректная обработка распространенных форматов файлов, применяемых в офисном ПО (Microsoft Office, PDF, TXT и т.д.); 5.2.2. поиск и анализ регулярных выражений (ключевых слов); 5.2.3. лингвистический (морфологический) анализ. 5.3. Автоматическое или ручное обновление компонентов с сайта производителя. 5.4. Управление доступом к средствам контентного анализа с использованием ролевой модели. 6. Требования к функционалу средств мониторинга и отчетности 6.1. Протоколирование действий пользователей и администраторов Системы. 6.2. Возможность, в режиме on-line, отслеживания текущей сессии пользователя, определения сервера, через который установлена сессия, подключения к серверу и разбора пользовательской сессии. 6.3. Определение геолокации на основе IP-адреса домена. 6.4. Формирование отчетности с функционалом: 6.4.1. объявления пользовательских (новых) полей	

№ п/п	Наименование	Характеристики	Кол-во
		6.4.2. формирования запросов с использованием перекрестных запросов. 6.5. Формирование отчетности с предоставлением функционала: 6.5.1. задания фильтров по всем (любым) полям, поддерживаемым средствами мониторинга функционирования и формирования отчетности; 6.5.2. формирования запросов к базе данных; 6.5.3. задания формата отчетов. 6.6. Отправку отчетов по расписанию и по запросу администраторов Системы. 6.7. Отключение мониторинга функционирования и формирования отчетности для конкретных пользователей/IP-адресов. 6.8. Автоматическое или ручное обновление компонентов с сайта производителя. 6.9. Управление доступом к средствам мониторинга и отчетности с использованием ролевой модели. 6.10. Отправка статистической информации по протоколу NetFlow версий 5, 9, 10. 6.11. Связь с существующим окружением и интеграция 6.12. Разграничение полномочий доступа для работы с Системой и доступа пользователей в сеть Интернет должно быть реализовано на ролевой основе с использованием групп существующих доменов Active Directory. 6.13. Система должна взаимодействовать со следующими смежными системами: 6.13.1. Система Active Directory, в части аутентификация пользователей в Active Directory, определение принадлежности пользователей к группам Active Directory. 6.13.2. Системами авторизации пользователей Kerberos, NTLM, Single-sign-on в части автоматической авторизации пользователей. 6.13.3. Система идентификации пользователей Radius accounting, определение IP-адресов пользователей. 6.13.4. Система синхронизации времени, в части взаимодействия с системой синхронизации	

№ п/п	Наименование	Характеристики	Кол-во
		времени должна поддерживать определение точного времени. 6.13.5. Система доменных имен (DNS), в части взаимодействия с системой DNS должно поддерживать определение IP-адресов узлов сети по имени узла. 6.13.6. Система мониторинга SNMP, в части взаимодействия с системой мониторинга SNMP должно поддерживать оповещение и работу в режиме запросов состояния системы по протоколам SNMP v2 и SNMP v3. 6.13.7. Корпоративная почтовая система (E-mail), в части взаимодействия с корпоративной почтовой системой должно поддерживать отправку по e-mail оповещений администраторам о событиях в работе средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет. 6.13.8. Система сбора и корреляции событий информационной безопасности, в части взаимодействия с системами сбора и корреляции событий информационной безопасности должно предоставлять механизм экспорта журнальных сообщений в режиме реального времени. Формат и детализация данных сообщений должны настраиваться. 6.13.9. Системы дополнительного контентного анализа, в части взаимодействия с системами дополнительного контентного анализа должно предоставлять модуль интеграции по протоколу I-CAP с указанными системами в части условий доступа на основании результатов анализа контента. 7. Требования к пользовательскому интерфейсу 7.1. Программный интерфейс компонентов Системы, включая средства управления, а также формы оповещений и уведомлений администраторов Системы и пользователей сети Интернет должен полностью поддерживать русский язык, используя кодировку текста UTF-8. 7.2. Наличие web-интерфейса для доступа к компонентам узла фильтрации Интернет-трафика, включая средства управления, полностью поддерживающего русский язык, используя кодировку текста UTF-8.	

№ п/п	Наименование	Характеристики	Кол-во
		8. Требования к наличию отчетов 8.1. Система должна обеспечивать формирование отчетности в табличном и графическом виде о совершаемых пользователями действиях в сети Интернет за различные периоды времени. 9. Дополнительные требования 9.1. Автоматическое или ручное обновление программных компонентов с сайта производителя. 9.2. Управление доступом к средствам контроля доступа в сеть Интернет и фильтрации трафика сети Интернет с использованием ролевой модели. 9.3. Протоколирование действий администраторов Системы. 9.4. Обеспечение отказоустойчивости программно-аппаратных компонентов Системы. 9.5. Предоставление возможности автоматического развертывания серверов фильтрации трафика с использованием API. 10. Требования к происхождению 10.1. Поставляемое решение внесено в Единый реестр российских программ для электронных вычислительных машин и баз данных. 11. Требования к сертификации: 11.1. Система должна иметь действующий сертификат соответствия ФСТЭК России на соответствие следующим требованиям: 11.1.1. «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты» ИТ.МЭ.А4.ПЗ (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты» ИТ.МЭ.Б4.ПЗ (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Д» четвертого класса защиты» ИТ.МЭ.Д4.ПЗ (ФСТЭК России, 2016); 11.1.2. «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2012); 11.1.3. «Требования по безопасности информации, устанавливающие уровни доверия	

№ п/п	Наименование	Характеристики	Кол-во
		к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020). Четвертый уровень доверия.	
2	Средство антивирусной защиты информации	Общие требования Антивирусные средства должны включать: • программные средства антивирусной защиты для рабочих станций Windows; • программные средства антивирусной защиты для рабочих станций и серверов Linux; • программные средства антивирусной защиты для файловых серверов Windows; • программные средства антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows • 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 и английском языке. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском 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 должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий: • Windows 7 Home / Professional / Enterprise (32 / 64-разрядная); • Windows 8 Professional / Enterprise (32 / 64-разрядная); • Windows 8.1 Professional / Enterprise (32 / 64-разрядная);	10

№ п/п	Наименование	Характеристики	Кол-во
		• Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядная) TH1, TH2, RS1, RS2, RS3, RS4, RS5, 19H1, 19H2, 20H1, 20H2 (с ограничениями). Программные средства антивирусной защиты (далее САВЗ) для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей: • поддержку определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности, администраторами серверов или пользователями; • возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ; • возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ; • получение и установку обновлений в автоматизированном режиме, в том числе с сетевого ресурса; • получение и установку обновлений без применения средств автоматизации; • генерацию записи аудита для событий, подвергаемых аудиту; • чтение информации из записей аудита; • ассоциацию событий аудита с идентификаторами субъектов; • ограничение доступа к чтению записей аудита; • поиск, сортировку, упорядочение данных аудита; • выполнение проверок 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; • выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных; • выполнение проверок с целью обнаружения зараженных объектов по команде; • выполнение проверок с целью обнаружения зараженных объектов в режиме динамического обнаружения в процессе выполнения операций доступа к объектам; • выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;	

№ п/п	Наименование	Характеристики	Кол-во
		• удаление (если удаление технически возможно) вредоносного кода из оперативной памяти, удаления файлов, в которых обнаружен вредоносный код, а также файлов, с подозрением на наличие вредоносного кода; • возможность перемещения и изолирования зараженных объектов, удаления вредоносного кода из файлов и системных областей носителей информации; • возможность блокирования АРМ, на котором обнаружены зараженные файлы; • возможность восстановления функциональных свойств зараженных объектов; • отображение сигнала тревоги об обнаружении вредоносных объектов; • возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью • возможность контроля доступа к веб-ресурсам • возможность контроля за запуском ПО на защищаемом АРМ. Кроме того, программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК: • антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта; • антивирусное сканирование по расписанию; • антивирусное сканирование подключаемых устройств; • эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы; • нейтрализации действий активного заражения; • анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; • анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;	

№ п/п	Наименование	Характеристики	Кол-во
		• откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; • ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия; • облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу; • антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; • защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP; • фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов; • проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики; • блокировку баннеров и всплывающих окон на загружаемых Web-страницах; • распознавания и блокировку фишинговых и небезопасных сайтов; • встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа; • возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства; • контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;	

№ п/п	Наименование	Характеристики	Кол-во
		• создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки; • контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory; • возможность управления MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств; • записи в журнал событий о записи и/или удалении файлов на съемных дисках; • контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory; • защиты от атак типа BadUSB; • запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. • защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля; • установки только выбранных компонентов программного средства антивирусной защиты;	

№ п/п	Наименование	Характеристики	Кол-во
		• централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • запуск задач по расписанию и/или сразу после запуска приложения; • гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; • ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • возможность проверки целостности антивирусной программы; • возможность добавления исключений из антивирусной проверки по контрольной сумме 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 упрощенной версии графического интерфейса, с минимальным набором возможностей; • возможность интеграции с Windows Defender Security Center; • наличие поддержки Antimalware Scan Interface (AMSI); • наличие поддержки Windows Subsystem for Linux (WSL); • возможность защитить паролем восстановление объектов из резервного хранилища. • полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем; • восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем; • поддержка двухфакторной аутентификации при полнодисковом шифровании; • шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии,	

№ п/п	Наименование	Характеристики	Кол-во
		позволяющей расшифровывать файлы за пределами организации с помощью пароля; • шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации; • возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий). Требования к программным средствам антивирусной защиты для 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 должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий: • Windows Small Business Server 2011 Essentials / Standard (64-разрядная); • Windows MultiPoint Server 2011 (64-разрядная); • Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная); • Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядная); • Windows Server 2012 Foundation / Essentials / Standard (64-разрядная); • Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная); • Windows Server 2016 (64-разрядная) (с ограничениями); • Windows Server 2019 (64-разрядная) (с ограничениями). Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей: • поддержку определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и администраторами серверов; • возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;	

№ п/п	Наименование	Характеристики	Кол-во
		• возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ; • получение и установку обновлений в автоматизированном режиме, в том числе с сетевого ресурса; • получение и установку обновлений без применения средств автоматизации; • генерацию записи аудита для событий, подвергаемых аудиту; • чтение информации из записей аудита; • ассоциацию событий аудита с идентификаторами субъектов; • ограничение доступа к чтению записей аудита; • поиск, сортировку, упорядочение данных аудита; • выполнение проверок 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; • выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных; • выполнение проверок с целью обнаружения зараженных объектов по команде; • выполнение проверок с целью обнаружения зараженных объектов в режиме динамического обнаружения в процессе выполнения операций доступа к объектам; • выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами; • удаление (если удаление технически возможно) вредоносного кода из оперативной памяти, удаления файлов, в которых обнаружен вредоносный код, а также файлов, с подозрением на наличие вредоносного кода; • возможность перемещения и изолирования зараженных объектов, удаления вредоносного кода из файлов и системных областей носителей информации; • возможность блокирования АРМ, на котором обнаружены зараженные файлы; • возможность восстановления функциональных свойств зараженных объектов; • отображение сигнала тревоги об обнаружении вредоносных объектов;	

№ п/п	Наименование	Характеристики	Кол-во
		• возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью • возможность контроля за запуском ПО на защищаемом 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 из контекстного меню объекта; • антивирусное сканирование по расписанию; • антивирусное сканирование подключаемых устройств; • эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы; • нейтрализации действий активного заражения; • анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; • анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов; • откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; • ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия; • облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;	

№ п/п	Наименование	Характеристики	Кол-во
		• антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; • встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • 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, 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; • запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. • защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; • установки только выбранных компонентов программного средства антивирусной защиты; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • запуск задач по расписанию и/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 контрольной сумме файл,	

№ п/п	Наименование	Характеристики	Кол-во
		маске имени/директории или по наличию у файла доверенной цифровой подписи; • наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления; • наличие защищенного хранилища для отчетов о работе антивируса; • возможность включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей; • возможность интеграции с Windows Defender Security Center; • наличие поддержки Antimalware Scan Interface (AMSI); • наличие поддержки Windows Subsystem for Linux (WSL); • возможность защитить паролем восстановление объектов из резервного хранилища. Требования к программным средствам антивирусной защиты для рабочих станций и серверов 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 Б, В и Г не ниже второго класса защиты. Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 32-битных операционных систем следующих версий: • Ubuntu 16.04 LTS и выше; • Red Hat Enterprise Linux 6.7 и выше; • CentOS 6.7 и выше; • Debian GNU / Linux 9.4 и выше; • Debian GNU / Linux 10.1 и выше; • Linux Mint 18.2 и выше; • Linux Mint 19 и выше; • Альт 8 СП Рабочая Станция; • Альт 8 СП Сервер; • Альт Рабочая Станция 8; • Альт Рабочая Станция К 8; • Альт Сервер 8; • Альт Образование 8; • Альт Сервер 9; • Альт Рабочая Станция 9; • Альт Образование 9; • Гослинукс 6.6;	

№ п/п	Наименование	Характеристики	Кол-во
		• Операционная система Лотос (редакция для серверов и рабочих станций); • Mageia 4. Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий: • Ubuntu 16.04 LTS и выше; • Ubuntu 18.04 LTS и выше; • Red Hat Enterprise Linux 6.7 и выше; • Red Hat Enterprise Linux 7.2 и выше; • Red Hat Enterprise Linux 8.0 и выше; • CentOS 6.7 и выше; • CentOS 7.2 и выше; • CentOS 8.0 и выше; • Debian GNU / Linux 9.4 и выше; • Debian GNU / Linux 10.1 и выше; • Oracle Linux 6,7 и выше; • Oracle Linux 7,3 и выше; • Oracle Linux 8 и выше; • SUSE Linux Enterprise Server 15 и выше; • openSUSE Leap 15 и выше; • Альт 8 СП Рабочая Станция; • Альт 8 СП Сервер; • Альт Рабочая Станция 8; • Альт Рабочая Станция К 8; • Альт Сервер 8; • Альт Образование 8; • Альт Рабочая Станция 9; • Альт Сервер 9; • Альт Образование 9; • Amazon Linux AMI; • Linux Mint 18.2 и выше; • Linux Mint 19 и выше; • Astra Linux Astra Linux Common Edition; • Astra Linux Special Edition (исполнение РУСБ.10015-01); • Гослинукс 6.6; • Гослинукс 7.2; • AlterOS 7.5; • Pardus OS 19.1; • RED OS 7.1; • RED OS 7.2. Программные средства антивирусной защиты для рабочих станций и серверов Linux должны обеспечивать реализацию следующих функциональных возможностей: • возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций • безопасности САВЗ;	

№ п/п	Наименование	Характеристики	Кол-во
		• возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций • безопасности САВЗ; • получение и установку обновлений в автоматизированном режиме, в том числе с сетевого ресурса; • получение и установку обновлений без применения средств автоматизации; • генерацию записи аудита для событий, подвергаемых аудиту; • чтение информации из записей аудита; • ассоциацию событий аудита с идентификаторами субъектов; • ограничение доступа к чтению записей аудита; • поиск, сортировку, упорядочение данных аудита; • выполнение проверок 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; • выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных; • выполнение проверок с целью обнаружения зараженных объектов по команде; • выполнение проверок с целью обнаружения зараженных объектов в режиме динамического обнаружения в процессе выполнения операций доступа к объектам; • выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами; • удаление (если удаление технически возможно) вредоносного кода из оперативной памяти, удаления файлов, в которых обнаружен вредоносный код, а также файлов, с подозрением на наличие вредоносного кода; • возможность перемещения и изолирования зараженных объектов, удаления вредоносного кода из файлов и системных областей носителей информации; • возможность блокирования АРМ и серверов, на которых обнаружены зараженные файлы; • возможность восстановления функциональных свойств зараженных объектов; • отображение сигнала тревоги об обнаружении вредоносных объектов.	

№ п/п	Наименование	Характеристики	Кол-во
		Кроме того, программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК: • резидентного антивирусного мониторинга; • облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу; • проверку ресурсов доступных по SMB / NFS; • эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; • антивирусное сканирование по команде пользователя или администратора и по расписанию; • антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.; • проверку сообщений электронной почты в текстовом формате (Plain text); • наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов); • защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования; • возможность включения опции блокирования файлов во время проверки; • помещение подозрительных и поврежденных объектов на карантин; • проверку почтовых баз приложений Microsoft Outlook на наличие вредоносных объектов; • возможность перехвата и проверки файловых операций на уровне SAMBA; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность экспортировать и сохранять отчеты в форматах HTML и CSV; • гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;	

№ п/п	Наименование	Характеристики	Кол-во
		• сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность; • возможность управления через пользовательский графический интерфейс без root прав; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления. • управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения; • проверки съемных дисков; • отслеживания во входящем сетевом трафике активности, характерной для сетевых атак • проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым • получения данных о действиях программ на компьютере пользователя; • проверки памяти ядра. Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, 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 файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: 32-разрядных операционных систем Microsoft Windows • Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Server 2008 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше. 64-разрядных операционных систем Microsoft Windows	

№ п/п	Наименование	Характеристики	Кол-во
		• Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Microsoft Small Business Server 2008 Standard / Premium; • Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше; • Microsoft Small Business Server 2011 Essentials / Standard; • Microsoft Windows MultiPoint™ Server 2011 Standard / Premium; • Windows Server 2012 Foundation / Essentials / Standard / Datacenter; • Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter; • Microsoft Windows MultiPoint Server 2012 Standard / Premium; • Windows Storage Server 2012; • Windows Hyper-V Server 2012; • Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; • Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter; • Windows Storage Server 2012 R2; • Windows Hyper-V Server 2012 R2; • Windows Server 2016 Essentials / Standard / Datacenter; • Windows Server 2016 MultiPoint; • Windows Server 2016 Core Standard / Datacenter; • Microsoft Windows MultiPoint Server 2016; • Windows Storage Server 2016; • Windows Hyper-V Server 2016; • Windows Server 2019 Essentials / Standard / Datacenter; • Windows Server 2019 Core; • Windows Storage Server 2019; • Windows Hyper-V Server 2019. • 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:	

№ п/п	Наименование	Характеристики	Кол-во
		• 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 управлять данными (административными данными), используемыми функциями безопасности; • возможность уполномоченным пользователям управлять режимом выполнения функций безопасности; • 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	

№ п/п	Наименование	Характеристики	Кол-во
		режиме с сетевого ресурса, автоматически через сетевые подключения; • возможность выполнять проверки с целью обнаружения атаки эксплойтов в памяти процессов, в контейнерах Windows Server 2016 и Windows Server 2019; • возможность при обнаружении признаков атаки эксплойтов на защищаемый процесс завершать процесс, сообщать о факте дискредитации уязвимости в процессе; • возможность проведения проверки целостности компонентов программного изделия. 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, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов; • антивирусное сканирование по команде пользователя или администратора и по расписанию; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу; • антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB; • защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков; • непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными. • анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • возможность проверки контейнеров Microsoft Windows;	

№ п/п	Наименование	Характеристики	Кол-во
		• защиты от эксплуатирования уязвимостей в памяти процессов; • должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться; • возможность добавлять процессы в список защищаемых; • ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи; • настройки проверки критических областей сервера в качестве отдельной задачи; • регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач; • возможность продолжать антивирусное сканирование в фоновом режиме; • наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий); • ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом; • возможность интеграции с SIEM системами; • возможность указания количества рабочих процессов антивируса вручную; • возможность отключить графический интерфейс; • наличие удаленной и локальной консоли управления; • управления параметрами антивируса из командной строки; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил. • защита от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;	

№ п/п	Наименование	Характеристики	Кол-во
		• защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления; • наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп); • компонент создания специальных правил должен контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме; • компонент создания специальных правил должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должен иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы; • осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory; • осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем; • информирование администратора о подключении внешних устройств; • наличие механизмов автоматической генерации правил для контроля устройств и приложений. Требования к программным средствам 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	

№ п/п	Наименование	Характеристики	Кол-во
		управлением операционных систем следующих версий: • Microsoft Windows 10 20H2 32-разрядная / 64-разрядная; • Microsoft Windows 10 20H1 32-разрядная / 64-разрядная; • Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная / 64-разрядная; • Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная / 64-разрядная; • Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная / 64-разрядная; • Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная; • Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная; • Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная; • Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная; • Microsoft Windows 10 Pro 19H1 32-разрядная / 64-разрядная; • Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная / 64-разрядная; • Microsoft Windows 10 Enterprise 19H1 32-разрядная / 64-разрядная; • Microsoft Windows 10 Education 19H1 32-разрядная / 64-разрядная; • Microsoft Windows 10 Home 19H2 32-разрядная / 64-разрядная; • Microsoft Windows 10 Pro 19H2 32-разрядная / 64-разрядная; • Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная / 64-разрядная; • Microsoft Windows 10 Enterprise 19H2 32-разрядная / 64-разрядная; • Microsoft Windows 10 Education 19H2 32-разрядная / 64-разрядная; • Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная; • Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная; • Microsoft Windows 8 Pro 32-разрядная / 64-разрядная; • Microsoft Windows 8 Enterprise 32-разрядная / 64-разрядная; • Microsoft Windows 7 Professional Service Pack 1 32-разрядная / 64-разрядная;	

№ п/п	Наименование	Характеристики	Кол-во
		• Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32-разрядная / 64-разрядная; • Windows Server® 2019 Standard 64-разрядная; • Windows Server 2019 Core 64-разрядная; • Windows Server 2019 Datacenter 64-разрядная; • Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-разрядная; • Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-разрядная; • Windows Server 2016 (вариант установки Server Core RS3 (v1709) (LTSB/CBB) 64-разрядная; • Windows Server 2016 Standard (LTSB) 64-разрядная; • Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная; • Windows Server 2016 Datacenter (LTSB) 64-разрядная; • Windows Server 2012 R2 Standard 64-разрядная; • Windows Server 2012 R2 Server Core 64-разрядная; • Windows Server 2012 R2 Foundation 64-разрядная; • Windows Server 2012 R2 Essentials 64-разрядная; • Windows Server 2012 R2 Datacenter 64-разрядная; • Windows Server 2012 Standard 64-разрядная; • Windows Server 2012 Server Core 64-разрядная; • Windows Server 2012 Foundation 64-разрядная; • Windows Server 2012 Essentials 64-разрядная; • Windows Server 2012 Datacenter 64-разрядная; • Windows Server 2008 R2 with Standard Service Pack 1 64-разрядная; • Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная; • Windows Storage Server 2016 64-разрядная; • Windows Storage Server 2012 R2 64-разрядная; • Windows Storage Server 2012 64-разрядная. Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах: • VMware™ vSphere™ 6.7; • VMware vSphere 7.1; • VMware Workstation 15 Pro; • VMware Workstation 16 Pro; • Microsoft Hyper-V® Server 2012 64-разрядная;	

№ п/п	Наименование	Характеристики	Кол-во
		• Microsoft Hyper-V Server 2012 R2 64-разрядная; • Microsoft Hyper-V Server 2016 64-разрядная; • Microsoft Hyper-V Server 2019 64-разрядная; • Citrix® XenServer® 7.1 LTSR; • Citrix XenServer 8.x. Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: • Microsoft SQL Server® 2012 Express 64-разрядная; • Microsoft SQL Server 2014 Express 64-разрядная; • Microsoft SQL Server 2016 Express 64-разрядная; • Microsoft SQL Server 2017 Express 64-разрядная; • Microsoft SQL Server 2019 Express 64-разрядная; • Microsoft SQL Server 2014 (все редакции) 64-разрядная; • Microsoft SQL Server 2016 (все редакции) 64-разрядная; • Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная; • Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная; • Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная; • Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная; • MySQL Standard Edition 5.7 32-разрядная / 64-разрядная; • MySQL Enterprise Edition 5.7 32-разрядная / 64-разрядная; • Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon™ RDS и Microsoft • Azure™; • MariaDB Server 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: • генерация записи аудита для событий, подвергаемых аудиту; • чтение информации из записей аудита; • ассоциация событий аудита с идентификаторами субъекта; • ограничение доступа к чтению записей аудита;	

№ п/п	Наименование	Характеристики	Кол-во
		• поиск, сортировка данных аудита; • обработка зараженных объектов на АРМ и серверах вычислительной сети; • выполнение автоматизированного запуска САВЗ на АРМ и серверах вычислительной сети с заданными условиями поиска вредоносных объектов и режимами реагирования по расписанию; • выполнение удаленного администрирования процессов обнаружения вредоносных объектов, обновления базы данных признаков вредоносных компьютерных программ (БД ПКВ) и компонентов САВЗ; • поддержка определенных ролей для САВЗ и их ассоциация с конкретными администраторами • безопасности; • возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ; • возможность создания учетных записей и идентификации/аутентификации пользователей; • отображение сигнала тревоги на автоматизированном рабочем месте администратора безопасности, указывающего на обнаружение вредоносных объектов на пользовательских автоматизированных рабочих местах. • выполнение получения и установки обновлений БД ПКВ без применения средств автоматизации и в автоматизированном режиме, в том числе с сетевого ресурса; • выполнение централизованной установки компонентов САВЗ; • поиск известных уязвимостей на управляемых АРМ и серверах Windows. Кроме того, программные средства централизованного управления, мониторинга и обновления должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК: • выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов; • возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации; • возможность настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;	

№ п/п	Наименование	Характеристики	Кол-во
		• автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по IPv4-адресу, типу ОС, нахождению в OU AD; • централизованные установка, обновление и удаление программных средств антивирусной защиты; • централизованная настройка, администрирование; • просмотр отчетов и статистической информации по работе средств защиты; • централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления; • сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям; • наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки; • возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности; • возможность иерархии триггеров, по которым происходит перераспределение; • тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; • доставка обновлений на рабочие места пользователей сразу после их получения; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; • создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;	

№ п/п	Наименование	Характеристики	Кол-во
		• поддержка мультиарендности (multi-tenancy) для серверов управления; • обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации; • доступ к облачным серверам производителя антивирусного ПО через сервер управления; • автоматическое распространение лицензии на клиентские компьютеры; • инвентаризация установленного ПО и оборудования на компьютерах пользователей; • наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них; • функция управления мобильными устройствами через сервер Exchange ActiveSync; • функция управления мобильными устройствами через сервер iOS MDM; • возможность отправки SMS-оповещений о заданных событиях; • централизованная установка сертификатов на управляемые мобильные устройства; • возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления; • возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления; • построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ; • наличие преднастроенных стандартных отчетов о работе системы; • экспорт отчетов в файлы форматов PDF и XML; • централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение; • создание внутренних учетных записей для аутентификации на сервере управления; • создание резервной копии системы управления встроенными средствами системы управления; • поддержка Windows Failover Clustering;	

№ п/п	Наименование	Характеристики	Кол-во
		• поддержка интеграции с Windows сервисом Certificate Authority; • наличие веб-консоли управления приложением; • наличие системы контроля возникновения вирусных эпидемий; • возможность установки в облачной инфраструктуре Microsoft Azure и Google Cloud; • возможность интеграции по OpenAPI; • возможность управления антивирусной защитой с использованием WEB консоли. • автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; • возможность подключения по RDP или штатными средствами из консоли управления, пользователю должен выводиться запрос на разрешение дистанционного подключения; • наличие инструментов работы с образами ОС: создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры; • должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ; • возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС; • возможность импортировать образ операционной системы из дистрибутивов (WIM) • наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии; • автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF. Требования к обновлению антивирусных баз Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:	

№ п/п	Наименование	Характеристики	Кол-во
		• создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток; • множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации; • проверку целостности и подлинности обновлений средствами электронной цифровой подписи. Требования к эксплуатационной документации Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе: • «Руководство пользователя (администратора)» Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты. Требования к технической поддержке Техническая поддержка антивирусного программного обеспечения должна: • Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по электронной почте и через Интернет. • Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.	
3	Средство защиты информации от несанкционированного доступа	СЗИ НСД должна представлять собой программный комплекс средств защиты информации в операционных системах семейства Linux с возможностью подключения аппаратных идентификаторов для усиления механизма аутентификации. СЗИ НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением следующих операционных систем семейства Linux в многопользовательском режиме их эксплуатации:	2

№ п/п	Наименование	Характеристики	Кол-во
		• Альт Рабочая Станция 8.2 x64 (версия ядра СЗИ НСД 4.9); • Альт Рабочая Станция 9.0 x64 (версия ядра СЗИ НСД 4.19); • Astra Linux Common Edition (Орёл) 2.12 x64 (версия ядра СЗИ НСД 4.19); • Debian 8 (версия ядра СЗИ НСД 3.16); • Debian 9 (версия ядра СЗИ НСД 4.19); • CentOS 7 x64 (версия ядра СЗИ НСД 3.16); • Red Hat Enterprise Linux 7 x64 (версия ядра СЗИ НСД 3.16); • Fedora 30 x64 (версия ядра СЗИ НСД 4.19); • Ubuntu 16.04 x64 (версия ядра СЗИ НСД 4.19); • Ubuntu 18.04 x64 (версия ядра СЗИ НСД 4.19); • РЕД ОС 7.1, 7.2 Муром (версия ядра СЗИ НСД 4.19); • ROSA Enterprise Linux Desktop/Server x64 (версия ядра СЗИ НСД 3.16); • ЛотОС 2.1 x64 (версия ядра СЗИ НСД 3.16). СЗИ НСД должна поддерживать 64-битные версии операционных систем. СЗИ НСД должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах, также поддерживать виртуальные среды. 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, 2018) 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;	

№ п/п	Наименование	Характеристики	Кол-во
		• 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. регистрацию пользователей. Возможность задать пароль пользователя. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества сессий пользователей на одном компьютере; 2. возможность принудительной блокировки пользователей и автоматической блокировки в случае нарушения политик безопасности; 3. идентификацию и проверку подлинности пользователей при входе в операционную систему. Возможность двухфакторной аутентификации по паролю и аппаратному идентификатору; 4. возможность сохранения авторизационных данных пользователя на аппаратном идентификаторе; 5. реализацию настроек сложности паролей (длины парольной строчки, контроля наличия цифр и специальных символов) и срока их действия; 6. возможность настройки разграничения прав доступа к объектам файловой системы, съемным накопителям, разграничения прав на доступ к устройствам печати; 7. возможность контроля целостности аппаратной конфигурации компьютера; 8. 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; 9. возможность периодического архивирования журналов событий; 10. возможность экспорта журналов безопасности в форматы PDF и ODS; 11. возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов); 12. 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,	

№ п/п	Наименование	Характеристики	Кол-во
		функционирующую в операционных системах семейства Windows; 13. 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; 14. контроль целостности объектов СЗИ; 15. очистку остаточной информации (освобождаемого дискового пространства, освобождаемых областей оперативной памяти, зачистку определенных файлов и папок по команде пользователя или АИБ); 16. возможность проверки корректности функционирования СЗИ НСД, самотестирования; 17. защиту от подмены ядра операционной системы и процедур инициализации; 18. возможность настройки всех параметров СЗИ НСД из единой консоли администрирования; 19. возможность синхронизации времени ОС с аппаратной платой средства доверенной загрузки для регистрации событий безопасности; 20. 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; 21. 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); 22. возможность централизованного управления защищенными рабочими станциями при помощи отдельного кроссплатформенного центра управления; 23. возможность управления встроенным межсетевым экраном, контроль управления портами, а также протоколами; 24. возможность оповещения при событиях НСД; 25. возможность автоматизированного тестирования памяти, целостности ПО, доступа, авторизации, функции гарантированной очистки оперативной памяти.	

№ п/п	Наименование	Характеристики	Кол-во
		26. наличие собственного механизма дискреционного управления доступом. Должен быть реализован модуль контроля подключения съемных машинных носителей информации (СКН). Модуль СКН должен обеспечивать: 1. контроль использования интерфейсов ввода/вывода средств вычислительной техники, подключения внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации; 2. возможность назначения прав доступа к конкретному накопителю; 3. возможность установить описание для сменного накопителя; 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, USB-ключи Рутокен (Рутокен ЭЦП, Рутокен Lite), электронные ключи Touch Memory (iButton), USB-ключи JaCarta (JaCarta SF/ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta LT). 1. 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).	
4	Средство анализа защищенности	Средство анализа защищенности должно обеспечивать одновременное сканирование не менее 16 IP адресов Требования к механизмам сетевого аудита САЗ 1) САЗ должно обеспечивать инвентаризацию ресурсов сети, определение состояния TCP и UDP портов в диапазоне от 1 до 65535, идентификацию операционных систем и сетевых приложений, трассировку маршрутов следования данных для построения топологии сети. 2) САЗ должно обнаруживать уязвимости кода и конфигурации программного обеспечения. Для выявления (поиска) уязвимостей САЗ должно использовать встроенную базу данных уязвимостей кода и уязвимостей конфигурации программного обеспечения. База данных уязвимостей САЗ должна содержать унифицированные описания	1

№ п/п	Наименование	Характеристики	Кол-во
		уязвимостей, аналогичные содержащимся в следующих общедоступных источниках: банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru), база данных «Common Vulnerabilities and Exposures (https://cve.mitre.org). САЗ должно осуществлять тестирование на проникновение путем эксплуатации уязвимостей, выявленных и содержащихся в базе данных уязвимостей. 3) САЗ должно осуществлять поиск уязвимостей автоматизировано или по расписанию, задаваемому оператором. 4) САЗ должно осуществлять обновление базы данных уязвимостей через сервис обновлений САЗ. 5) САЗ должно осуществлять подбор паролей по словарю для следующих сетевых сервисов: ftp, http, imap, mssql, mysql, oracle, pop3, postgres, rdp, redis, smb, smtp, snmp, ssh, telnet, vnc. 6) САЗ должно осуществлять аудит безопасности беспроводных сетей и имитацию атак на них. 7) САЗ должно осуществлять перехват, анализ и фильтрацию сетевых пакетов локальной и внешней сетей информационной системы и извлечение из сетевого трафика парольной информации (для протоколов ftp, pop3, http, https, telnet), а также, проверку возможности атак подмены MAC-адресов. 8) САЗ должно обеспечивать контроль за установкой обновлений ОС Microsoft Windows: 7, 8.1, 10, Server 2012, Server 2012-R2, Server 2016 9) САЗ должно обеспечивать контроль за настройками комплекса средств защиты ОС специального назначения «Astra Linux Special Edition». 10) САЗ должно обеспечивать формирование отчетов по результатам проверок в форматах: HTML, PDF, DOC, CSV. 2 Требования к механизмам локального аудита САЗ 1) САЗ должно осуществлять поиск остаточной информации на различных носителях информации и гарантированное уничтожение информации путем записи случайной последовательности символов поверх стираемой информации, а также записи случайной последовательности символов в освободившееся пространство накопителей на жестких магнитных дисках, накопителей на основе флэш-памяти и съемных носителей информации. 2) САЗ должно осуществлять локальный подбор паролей по словарю для учетных записей пользователей ОС Microsoft Windows:7, 8.1, 10.	

№ п/п	Наименование	Характеристики	Кол-во
		3) САЗ должно обеспечивать контрольное суммирование заданных файлов, папок, подпапок, съемных носителей и накопителей на жестких магнитных дисках.	
5	Шкаф настенный телекоммуникационный	Ширина (мм): не менее 600 Высота (мм): не менее 745 Глубина (мм): не менее 450 Материал передней двери: стекло	1
6	Неуправляемый коммутатор	Интерфейсы: • 24 порта 10/100/1000Base-T Индикаторы: • Power • Link/Activity/Speed (на порт) DIP-переключатели: • Energy-Efficient Ethernet (EEE) • Управление потоком • Изоляция портов и защита от шторма Сетевые кабели: • Ethernet: 2-парный кабель категории 3/4/5/5e, неэкранированная витая пара • Fast Ethernet: 2-парный кабель категории 5/5e, неэкранированная витая пара • Gigabit Ethernet: 4-парный кабель категории 5/5e, неэкранированная витая пара Разъем питания: • Разъем для подключения питания (переменный ток) Тип корпуса: • Металл	1
7	Установка и настройка сети	Услуги по установке сетевого оборудования и настройке сети учреждения	1
8	Установка и настройка средств защиты информации	Услуги по установке и настройке средств защиты информации: -средство межсетевого экранирования -средство антивирусной защиты информации -средства защиты информации от несанкционированного доступа -средство анализа защищенности.	1

5. Требования к патентной чистоте

При оказании услуг должны соблюдаться положения законодательных актов Российской Федерации по соблюдению авторских прав и защите специальных знаков.

6. Требования к гарантийному обслуживанию и технической поддержке

Программные и программно-аппаратные средства, поставляемые в рамках этого технического задания, должны быть обеспечены гарантийной

поддержкой, обновлением ПО и баз определений (антивирусных, обнаружения вторжений, и пр.) на срок не менее 12 месяцев со дня заключения Контракта.

7. Сроки оказания услуг

Начало оказания услуг: с момента подписания Контракта. Срок оказания услуг: в течение 30 (тридцать) рабочих дней с момента подписания Контракта.

8. Требования по обеспечению режима конфиденциальности при оказании услуг

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

9. Требования к Исполнителю

Исполнитель не должен являться офшорной компанией, находится в списке недобросовестных поставщиков.

Исполнитель должен иметь лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации, перечень услуг: услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации программных (программно-технических) средств защиты информации; защищенных программных (программно-технических) средств обработки информации; программных (программно-технических) средств контроля эффективности защиты информации).

Исполнитель должен иметь лицензию ФСБ на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем.

Исполнитель гарантирует наличие необходимых профессиональных знаний и квалификации, оборудования и других возможностей для оказания указанных услуг субъектам малого и среднего предпринимательства.

Исполнитель гарантирует наличие подтверждающих документов на выполнение данных услуг.

В случае выявления Заказчиком недостатков, Исполнитель обязан устранить их своими силами, и за свой счёт.

Исполнитель предоставляет копии следующих документов:

- выписки из ЕГРЮЛ/ЕГРИП;
- свидетельство о регистрации;
- свидетельство о постановке на налоговый учет;
- приказ о назначении директора или иные документы, подтверждающие

право подписания должностным лицом договора;

- выписка из Устава;
- карточку предприятия с подписью ответственного лица;
- копии документов, подтверждающие наличие необходимых профессиональных знаний и квалификации для выполнения вышеуказанных услуг.

Коммерческое предложение со всеми необходимыми документами, указанными в настоящем Техническом задании должно быть направленно на официальную почту **exportrk2018@yandex.ru** Заказчика до **24.11.2023**.

10.Порядок приемки поставленного товара

Исполнитель осуществляет поставку заказанных средств защиты информации в течении срока действия договора.

Заказчик обязан осуществить приемку поставленных средств защиты информации в день поставки.

При приемке заказа подлежит проверке объем и качество поставленных средств защиты информации.

Поставляемые средства защиты информации должны быть укомплектованы формулярами, установочными дистрибутивами, а также копиями сертификатов соответствия ФСТЭК или ФСБ (для СКЗИ, и СЗИ для защиты СКЗИ).

В день передачи средств защиты информации, Исполнитель обязан передать Заказчику оригиналы счетов, акт приемки-передачи товаров, акты приёма-передачи прав на ПО, подписанный Исполнителем, в двух экземплярах, сертификаты (декларации о соответствии), обязательные для данного вида товара, и иные документы, подтверждающие качество товара, оформленные в соответствии с законодательством Российской Федерации.

В случае поставки товара ненадлежащего качества Исполнитель обязан безвозмездно устранить недостатки товара в течение 10 рабочих дней с момента заявления о них Заказчиком либо возместить расходы Заказчика на устранение недостатков товара.

В случае существенного нарушения требований к качеству товара Исполнитель обязан в течение 10 рабочих дней заменить некачественный товар товаром, соответствующим ТЗ.