

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Наименование: Оказание услуг по продлению неисключительных (лицензионных) прав использования антивирусного программного обеспечения.

Заказчик заявляет **продление** неисключительных (лицензионных) прав антивирусного программного обеспечения на уже приобретенный и используемый программный продукт Dr.Web® Desktop Security Suite КЗ и Dr.Web® Server Security Suite АВ, сроком на 1 год. Количество рабочих мест 214 (200 клиентских ПК и 14 файловых серверов) (продлеваемая лицензия Серийный номер: 23YX-V75C-****-**** на 214 (200 клиентских ПК и 14 файловых серверов) с датой окончания 2024-09-01. Участник размещения заказа не вправе предложить эквивалент, т.к. предложение другого антивирусного программного обеспечения не обеспечит совместимости с существующим у Заказчика программным обеспечением.

№ п/п	Наименование	Единица измерения	Количество
1	Dr.Web® Desktop Security Suite КЗ, продление на 12 месяцев в количестве 200 лиц.	шт.	1
2	Dr.Web® Server Security Suite АВ, продление на 12 месяцев в количестве 14 лиц	шт.	1

Техническая спецификация

Наименование: Система антивирусной защиты (далее - Система)

1 Общие требования

- 1.1 Участники запрос котировок на использование антивирусного программного продукта должны иметь статус официального партнера компании производителя, что является подтверждением их квалификации и прав на поставку антивирусных продуктов и/или лицензий. При заключении договора необходимо предоставить копии документов, подтверждающих статус официального партнера компании производителя.
- 1.2 Участник должен принять во внимание, что ссылка на наименование продукции носит описательный, а не обязательный характер. В случае если Участником предлагаются эквивалент требуемого Заказчиком ПО, то в составе своей конкурсной заявки он должен в обязательном порядке предоставить следующую информацию:
 - 1.2.1 в Техническом предложении – подробное техническое описание предлагаемого к поставке эквивалента, с указанием полного соответствия (или превосходящего) всем техническим характеристикам, указанным в данной спецификации, заверенное у производителя предлагаемого программного продукта

Отсутствие в составе конкурсной заявки подробного технического описания аналогов продукции и/или письма о согласовании может являться причиной отклонения конкурсной заявки Участника.

- 1.3 Все компоненты Системы должны принадлежать одной торговой марке с единой службой технической поддержки на русском языке. Техническая поддержка должна предоставляться непосредственно производителем поставляемых программных продуктов.
- 1.4 Поставляемые средства защиты должны представлять масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети заказчика.
- 1.5 Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке.
- 1.6 Все антивирусные средства, функционирующие под операционной системой типа Windows, включая средства управления, должны обладать контекстной справочной системой на русском языке.
- 1.7 Участник конкурса должен предоставить единый серийный номер для всех поставляемых по условиям конкурса продуктов.
- 1.8 Система лицензирования не должна иметь привязку к используемому на защищаемых объектах аппаратному обеспечению. Система должна позволять перенос лицензий с одних защищаемых объектов (в том числе рабочих станций и серверов) на иные без необходимости перепривязки или получения дополнительных лицензий
- 1.9 Антивирусные средства должны включать:
 - программные средства защиты рабочих станций;
 - программные средства защиты файловых серверов;
 - программные средства централизованного управления, мониторинга и обновления;
 - обновляемые базы данных сигнатур вредоносных программ всех типов и атак;
 - эксплуатационную документацию на русском языке.

2. Требования к программным средствам

2.1. Общие требования к системе антивирусной защиты

2.1.1. Программные средства Системы должны обеспечивать определение угроз следующих типов:

- 2.1.1.1. классических вирусов;
- 2.1.1.2. троянских программ;
- 2.1.1.3. руткитов;
- 2.1.1.4. сетевых червей;
- 2.1.1.5. рекламных программ;
- 2.1.1.6. программ автодозвона на платные сайты;
- 2.1.1.7. потенциально опасных приложений;
- 2.1.1.8. прочих вредоносных программ.

2.1.2. Антивирусная защита должна обеспечивать:

- 2.1.2.1. обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE и т.п.;
- 2.1.2.2. обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками;
- 2.1.2.3. обнаружение вирусов внутри контейнеров и архивных файлов формата ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (включая NRG, образы с нестандартным форматом сектора и не имеющие сигнатур), ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER с зашифрованными контейнерами и т.д. без ограничений на уровень вложенности проверяемых объектов;
- 2.1.2.4. обнаружение вирусов внутри контейнеров, не имеющих строгого формата (HTML, MIME);
- 2.1.2.5. обнаружение вирусов внутри контейнеров с нечетким значением размера объекта (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES и т.д.);
- 2.1.2.6. антивирусную проверку файлов и объектов, имеющих формат Smart Install Maker (SIM); DMG, HFS, XAR, Universal Binary (MacOS); SIS (Symbian 9); INNO SETUP (5.3.9 и выше); SETUP FACTORY (линейки 7,8); XENOCODE; TARMA INSTALL (линейка 3); XZ (UNIX); COMPRESS; SQUAHFS; CHILKAT ZIP; пакеты LHA (AWARD BIOS);
- 2.1.2.7. антивирусную проверку в самораспаковывающихся архивах: AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy;
- 2.1.2.8. проверку исполняемых файлов, упакованных следующими упаковщиками: PELOCK, ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT, а также почтовых файлов Mozilla Thunderbird- вне зависимости от их размера;
- 2.1.2.9. разбор неформатированных почтовых баз и обработка писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW), поддержка формата TNEF;
- 2.1.2.10. защиту от вредоносных программ, принадлежащих семействам вредоносных программ, информация о которых имеется в антивирусных базах, созданных после занесения соответствующей информации в антивирусные базы и еще не попавших на анализ в антивирусные лаборатории - как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле;
- 2.1.2.11. обнаружение вредоносных объектов в HTML- и PDF-документах, включая обфусцированные эксплойты в JavaScript, находящиеся в документах данных типов. Возможность извлечения и анализа «невидимых» IFRAME-элементов. Возможность извлечения для проверки скриптов любой сложности и снятие с них защиты;
- 2.1.2.12. обнаружение угроз по лицензионным данным (ASPROTECT, PEP и ENIGMA);
- 2.1.2.13. обнаружение угроз, направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля
- 2.1.2.14. обнаружение вредоносных объектов в DEX-файлах (Android).

2.1.3. Используемое антивирусное ядро:

- 2.1.3.1.** не должно допускать снижение скорости проверки при увеличении размера антивирусных баз;
- 2.1.3.2.** в связи с возможностью исчерпания ресурсов ОС (в том числе места на диске, памяти) в ходе обработки специальным образом сформированных архивов автоматически выбирать уровень анализа упакованных объектов, а также механизм уменьшения размера промежуточных файлов. При выборе уровня анализа должен учитываться уровень загрузки системы
- 2.1.3.3.** в целях ускорения проверки архивов и упакованных файлов должно обеспечивать опознание вредоносных программ без запуска распаковщика;
- 2.1.3.4.** должно обеспечивать защиту от так называемых «почтовых бомб»;
- 2.1.3.5.** должно обеспечивать работу с файлами размером как менее, так и больше 2 ГБ;
- 2.1.3.6.** должно поддерживать работу с дисками с LBA-адресацией;
- 2.1.3.7.** в целях исключения «утечки» оперативной памяти должно использовать механизм распределения динамической памяти уровня антивирусного ядра.

2.2. Требования к системе управления антивирусной защитой (далее - Сервер управления)

- 2.2.1.** Система управления должна быть построена по клиент-серверной архитектуре с возможностью построения иерархической системы серверов – с возможностью использования в системе антивирусного управления как главных, так подчиненных серверов.
- 2.2.2.** Система управления должна быть реализована на основе Web-интерфейса, поддерживающего Web-браузеры, используемые как в корпоративной сети, так и Web-браузеры, используемые на устройствах и компьютерах, имеющих доступ к сервисам управления антивирусной защитой извне корпоративной сети - в том числе Mozilla Firefox или Internet Explorer. Управление через данные браузеры должно быть доступно с любых ОС, имеющих возможность их установки и запуска.
- 2.2.3.** Система должна включать поддержку кластерного протокола, с помощью которого координируются действия над агентами защиты с разных антивирусных серверов
- 2.2.4.** Система управления должна быть доступной с любой операционной системы, поддерживающей браузеры Mozilla Firefox или Internet Explorer (в том числе с ОС Microsoft Windows и ОС типа UNIX (Linux, FreeBSD, Solaris)), без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения как на стороне сервера управления, так и на стороне администратора Системы. Контроль работы Системы должен быть также возможен консоли управления, функционирующей на мобильных устройствах iPhone
- 2.2.5.** В целях безопасности все ПО, входящее в состав антивирусного сервера (в том числе необходимое для доступа с помощью браузера) должно поставляться в виде единого дистрибутива и принадлежать одной торговой марке.
- 2.2.6.** Система управления должна включать систему управления лицензиями, позволяющую распределять между серверами в рамках иерархической сети необходимое количество лицензий
- 2.2.7.** Установка антивирусного сервера Системы должна быть возможна на:
 - 2.2.7.1.** Microsoft Windows Server 2008 R2;

- 2.2.7.2. Microsoft Windows 7;
- 2.2.7.3. Microsoft Windows 8;
- 2.2.7.4. Microsoft Windows 8.1;
- 2.2.7.5. Microsoft Windows 10 (21H2 или более ранняя версия);
- 2.2.7.6. Microsoft Windows Server 2012
- 2.2.7.7. Microsoft Windows Server 2012 R2;
- 2.2.7.8. Microsoft Windows Server 2016;
- 2.2.7.9. Microsoft Windows Server 2019;
- 2.2.7.10. Microsoft Windows Server 2022;
- 2.2.7.11. FreeBSD 11.3;
- 2.2.7.12. Debian GNU/Linux 9;
- 2.2.7.13. Debian GNU/Linux 10;
- 2.2.7.14. Red Hat Enterprise Linux 7;
- 2.2.7.15. Red Hat Enterprise Linux 8;
- 2.2.7.16. Ubuntu 18.04;
- 2.2.7.17. Ubuntu 20.04
- 2.2.7.18. CentOS 7;
- 2.2.7.19. CentOS 8;
- 2.2.7.20. Альт 8СП;
- 2.2.7.21. Альт Рабочая станция 9;
- 2.2.7.22. Альт Сервер 9;
- 2.2.7.23. ОС типового дистрибутива АИС ФССП России (Гослинукс IC6);
- 2.2.8. Система управления должна иметь возможность:
 - 2.2.8.1. просмотра и сравнения состава аппаратно-программного обеспечения на станциях антивирусной сети
 - 2.2.8.2. контроля неактивных станций антивирусной сети
 - 2.2.8.3. просмотра сессий пользователей антивирусной сети
 - 2.2.8.4. замены системного DNS
 - 2.2.8.5. использования как внутренней СУБД (поставляемой в составе дистрибутива антивирусного сервера), так и внешней (устанавливаемой отдельно до или после развертывания антивирусного сервера). При использовании внешней СУБД Система должна иметь возможность работы с ней как без установки дополнительного ПО (с СУБД MS SQL, Oracle), так и с помощью драйверов ODBC для операционных систем Windows и Linux (в том числе с СУБД PostgreSQL). Система должна иметь возможность замены типа используемой СУБД после установки серверной части – без необходимости переустановки серверной части Системы
 - 2.2.8.6. управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа, выполнения произвольных SQL-запросов

- 2.2.8.7. экспорта и импорта базы данных антивирусного сервера в XML-файл.
- 2.2.8.8. создания иерархической сети антивирусных серверов. В случае реализации иерархической сети Система должна иметь возможность:
 - 2.2.8.8.1. объединения информации от нескольких серверов на одном.
 - 2.2.8.8.2. распределения рабочих станций между серверами для получения обновлений в целях снижения общей нагрузки на сеть.
 - 2.2.8.8.3. обмена статистикой в рамках одной иерархической сети между антивирусными серверами различных версий
 - 2.2.8.8.4. контроля отсутствия связанных серверов в расписании антивирусного сервера.
- 2.2.8.9. построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне;
- 2.2.8.10. установки антивирусных агентов в сети, не использующей единого пароля доступа к рабочим станциям;
- 2.2.8.11. централизованной настройки параметров защиты, уникальных для различных групп, в том числе для рабочих станций, находящихся в режиме off-line.
- 2.2.8.12. централизованного сбора и просмотра статистической информации и создания отчетов о состоянии антивирусной защиты и их консолидации;
- 2.2.8.13. интеграции в системы управления и информационные системы с помощью встроенного в систему API
- 2.2.8.14. наличия множественных путей уведомления пользователей и администраторов путем отправки почтового сообщения, звукового оповещения, всплывающего окна, записи в журнал событий, SNMP-trap;
- 2.2.8.15. оповещения о возникновении эпидемий (множественных инфекций)
- 2.2.8.16. оповещения о наличии обновлений сервера
- 2.2.8.17. отправки информационных сообщений пользователям по сети в режиме реального времени через Web-интерфейс Системы;
- 2.2.8.18. обеспечения связи антивирусного сервера и клиентских частей через встроенный модуль в случае, когда они расположены в различных сетях, работающих по протоколам TCP/IP (в т.ч. IPv6), между которыми отсутствует маршрутизация пакетов
- 2.2.8.19. самостоятельного написания обработчиков событий на языке Lua, а также выполнения произвольных Lua-скриптов с помощью средств системы управления.
- 2.2.9. В случае интеграции с внешними подсистемами с помощью встроенного Web API, должна иметься возможность аудита действий, произведенных с помощью функций данного Web API
- 2.2.10. Вне зависимости от типа антивирусного агента и защищаемой системы, Система должна обеспечивать реализацию следующих функциональных возможностей
 - 2.2.10.1. экспорта, импорта и распространения конфигураций групп, станций антивирусной сети или компонентов антивирусной защиты на другие группы, станции и компоненты, в том числе в целях изменения политик, применения их к определенным группам

- 2.2.10.2. скачивания конфигурационных файлов с настройками подключения антивирусных агентов для ОС Android, Mac OS X и ОС семейства UNIX
- 2.2.10.3. восстановления рабочих станций, случайно удаленных из системы защиты;
- 2.2.10.4. централизованного обновления антивирусных баз на всех защищенных рабочих станциях, в том числе мобильных и находящихся в режиме off-line. Доставки обновлений на рабочие места пользователей как по расписанию, так сразу после их получения;
- 2.2.10.5. обновления программных средств и антивирусных баз из разных источников, доставляемые как автоматически по каналам связи в пределах антивирусной сети, так и на отчуждаемых машинных носителях информации – путем ручной синхронизации информации между серверами и рабочими станциями
- 2.2.10.6. обновления программных средств и антивирусных баз с помощью мобильного сервера обновлений, представляющего собой Сервер управления, развернутый на flash-диске;
- 2.2.10.7. управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая откат обновлений
- 2.2.10.8. контроля результатов обновления антивирусного ПО на станциях антивирусной сети.
- 2.2.10.9. организации межсерверного обмена согласно расписанию
- 2.2.10.10. ограничения канала связи по группам
- 2.2.10.11. наличия возможности групповых обновлений
- 2.2.10.12. обновлений по защищенному каналу с использованием SSL-сертификатов
- 2.2.10.13. организации отложенного обновления
- 2.2.10.14. проверки обновлений на выбранных администратором компьютерах/группах перед распространением их на все клиентские компьютеры
- 2.2.10.15. автоматического перехода установленного ПО на более новые версии, в том числе с возможностью выбора обновляемых компонентов;
- 2.2.11. Программные средства управления для всех защищаемых ресурсов, реализованных на платформах ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:
 - 2.2.11.1. централизованной удаленной установки и деинсталляции программных средств, антивирусных баз и антивирусного ядра на защищаемые узлы сети – в том числе на станции, находящиеся в разных доменах.
 - 2.2.11.2. создания инсталляционных пакетов для конкретных защищаемых рабочих станций;
 - 2.2.11.3. выбора и настройки устанавливаемых компонентов до начала установки антивирусного пакета на клиентские части;
- 2.2.12. Система должна обладать специальной политикой для мобильных пользователей (ноутбуки), при применении которой, мобильные пользователи должны иметь возможность редактирования настроек антивирусного пакета и обновления через Интернет при отсутствии доступа к антивирусному серверу. Применение политики должно происходить через Web-интерфейс, без необходимости использования файлов конфигурации типа *.xml.
- 2.2.13. Система управления должна поддерживать возможность:

- 2.2.13.1. создания точки восстановления перед установкой антивирусного пакета на защищаемые рабочие станции и сервера;
- 2.2.13.2. восстановления удаленных станций.
- 2.2.14. Система должна поддерживать множественную возможность установки своих компонентов на защищаемые рабочие станции – в том числе с помощью:
 - 2.2.14.1. прямого их указания в системе управления в результате сканирования локальной сети, Microsoft Active Directory,
 - 2.2.14.2. политик Microsoft Active Directory
 - 2.2.14.3. установки с помощью дистрибутива, содержащего все компоненты защиты
 - 2.2.14.4. рассылки инсталляционных файлов из системы управления по электронной почте
 - 2.2.14.5. возможностей службы распределенной файловой системы (DFS).
- 2.2.15. Система должна поддерживать возможность настройки правил автоматического распределения станций по пользовательским группам, а также возможность изменения первичной группы при автоматическом подтверждении доступа станций к антивирусному серверу
- 2.2.16. Система управления должна обладать возможностью встроенного автоматического резервного копирования критически важных данных и конфигурации антивирусного сервера по заранее заданному расписанию, а также опцию восстановления сервера из резервной копии без использования файлов конфигурации типа *.xml.
- 2.2.17. Система должна иметь возможность минимизации трафика:
 - 2.2.17.1. за счет применения специальных алгоритмов сжатия;
 - 2.2.17.2. ограничения трафика по пропускной способности и по времени в определенных IP-подсетях.
- 2.2.18. Система должна иметь возможность интеграции с платформой Microsoft® Network Access Protection (NAP), обеспечивающей автоматическую систему реагирования на инциденты безопасности.
- 2.2.19. Система должна иметь возможность выбора уровня подробности протоколирования своих компонентов. система управления должна иметь возможность загрузки архивированных файлов журнала работы всех антивирусных серверов иерархической сети
- 2.2.20. В целях ограничения использования серверного пространства должна иметься возможность ротации файлов журнала антивирусного сервера по времени (час, день, неделя)
- 2.2.21. Система управления должна обеспечивать защиту от несанкционированного доступа. Авторизация должна обеспечиваться парой логин/пароль.
- 2.2.22. Администраторы Системы должны иметь возможность авторизации с помощью ActiveDirectory, LDAP, RADIUS, PAM. Система управления должна иметь возможность предварительного тестирования настроек авторизации внешних администраторов Active Directory, LDAP и RADIUS
- 2.2.23. Система должна иметь журнал аудита действий администраторов Системы, позволяющий просматривать журнал событий и изменений, осуществленных администраторами при помощи системы управления.
- 2.2.24. Система должна обеспечивать:

- 2.2.24.1. возможность экспорта выбранных файлов из карантина рабочей станции и/или файлового сервера на антивирусный сервер для дальнейшего анализа;
- 2.2.24.2. возможность задания групповых политик в зависимости от группы IP-адресов.
- 2.2.24.3. возможность просмотра новостей безопасности, в том числе информирующих об актуальных угрозах
- 2.2.25. В случае включения какого-либо компонента Системы в единую систему управления антивирусной защиты локальной сети:
 - 2.2.25.1. обновления компонента Системы должны происходить через сервер обновления системы управления антивирусной защиты;
 - 2.2.25.2. статистика работы компонентов Системы должна:
 - 2.2.25.2.1. собираться на сервере системы управления антивирусной защиты;
 - 2.2.25.2.2. быть доступной с любой операционной системы, поддерживающей браузеры Mozilla Firefox, Internet Explorer, Safari, Opera без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения за исключением устанавливаемого автоматически с антивирусного сервера модуля, необходимого для отображения статистики.
 - 2.2.25.2.3. Иметь возможность экспорта в формат PDF
 - 2.2.25.2.4. Иметь возможность отправки по электронной почте согласно расписанию работы антивирусного сервера
- 2.2.26. Система должна обеспечивать реализацию следующих функциональных возможностей по обновлению:
 - 2.2.26.1. получения ежедневных обновлений вирусных баз не менее 10 раз в сутки независимо от того, рабочий, либо выходной день, что должно подтверждаться созданным Системой отчетом (файлом протокола). Система также должна поддерживать возможность получения экстренных обновлений, связанных с выходом новых типов вредоносного ПО, а также возможность мгновенного распространения этих обновлений;
 - 2.2.26.2. возможность множественности путей обновления, в том числе по каналам связи и на съемных электронных носителях информации;
 - 2.2.26.3. возможность обновления через прокси-серверы, в том числе прокси-серверы MS ISA/TMG.
 - 2.2.26.4. проверка целостности и подлинности обновлений средствами электронной цифровой подписи.
 - 2.2.26.5. обновления компонентов и вирусных баз по защищенному каналу, с использованием протокола HTTPS.
- 2.2.27. В случае размещения антивирусных серверов во внутренней сети без доступа к сети Интернет получение обновлений должно быть возможно с помощью специальной утилиты автономной загрузки репозитория;
- 2.2.28. Система должна иметь возможность перезагрузки защищаемой станции через систему управления
- 2.2.29. Система должна иметь возможность шифрования трафика между серверами и защищаемыми рабочими станциями в целях предотвращения утечки конфиденциальной информации.

2.2.30. Система должна иметь поддержку режима работы для виртуальных сред, предполагающую использование отдельной виртуальной машины со специализированным антивирусным компонентом, предоставляющим возможность подключения агентам антивирусной защиты в других виртуальных машинах для осуществления сигнатурной проверки файловых объектов без необходимости использования имеющихся у них ресурсов.

2.3. Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows

2.3.1. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:

2.3.1.1. осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях.

2.3.2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов:

2.3.3. Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию ПО должна обеспечивать защиту рабочих станций под управлением операционных систем:

2.3.3.1. Microsoft Windows XP Professional;

2.3.3.2. Microsoft Windows 7;

2.3.3.3. Microsoft Windows 8.1;

2.3.3.4. Microsoft Windows 10;

2.3.3.5. Microsoft Windows 11.

2.3.4. Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.

2.3.5. Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур.

2.3.6. Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов.

2.3.7. В случае наличия системы централизованного управления права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля.

- 2.3.8.** Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках имеющихся у них прав.
- 2.3.9.** В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
- 2.3.10.** Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.
- 2.3.11.** Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях:
- 2.3.11.1.** поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
- 2.3.11.2.** непрерывное фоновое сканирование в целях нейтрализации активных угроз
- 2.3.11.3.** проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;
- 2.3.11.4.** проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
- 2.3.11.5.** блокировку опасных макросов VBA в реальном времени;
- 2.3.11.6.** защиту от вредоносных сценариев, загружаемых с Web-страниц;
- 2.3.11.7.** защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевое экрана;
- 2.3.11.8.** проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО;
- 2.3.11.9.** защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе отдельным типам сменных носителей информации, локальным файлам и каталогам, сайтам в сети Интернет;
- 2.3.11.10.** ограничения доступа к сети Интернет или к компьютеру в определенный момент времени по расписанию
- 2.3.11.11.** помещение найденных зараженных файлов в специальное место на жестком диске -«карантин»;
- 2.3.11.12.** просмотр местоположения станций и серверов на карте, если заданы географические координаты станции
- 2.3.11.13.** автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
- 2.3.11.14.** запуск задач по расписанию и/или сразу после загрузки операционной системы;

- 2.3.11.15.** возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке.
- 2.3.12.** Система защиты рабочих станций должна обеспечивать проверку протоколов:
- 2.3.13.** HTTP;
- 2.3.14.** IMAP, SMTP, POP3 независимо от используемого почтового клиента;
- 2.3.15.** NNTP (только проверка на вирусы), независимо от почтового клиента.
- 2.3.16.** Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством:
- 2.3.17.** антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
- 2.3.18.** проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.
- 2.3.19.** В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
- 2.3.20.** Система должна обеспечивать защиту от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) с помощью превентивной защиты, отслеживающей попытки внедрения вредоносных файлов
- 2.3.21.** В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения.
- 2.4. Требования к программным средствам антивирусной защиты рабочих станций и домашних компьютеров под управлением ОС семейства Microsoft Windows, не входящих в систему централизованного управления**
- 2.4.1.** Программные средства системы защиты (далее Системы) должны обеспечивать реализацию следующих функциональных возможностей:
- 2.4.1.1.** осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях;
- 2.4.1.2.** создание резервных копий папок, указанных пользователем, а также восстановление данных из хранилища - в том числе самим пользователем.
- 2.4.2.** Система используя актуальную на момент проведения тендера версию ПО должна обеспечивать защиту рабочих станций под управлением операционных систем:
- 2.4.2.1.** Microsoft Windows XP;
- 2.4.2.2.** Microsoft Windows 7;
- 2.4.2.3.** Microsoft Windows 8.1;
- 2.4.2.4.** Microsoft Windows 10;
- 2.4.2.5.** Microsoft Windows 11.

- 2.4.3.** В целях противодействия вредоносным программам, блокирующим запуск известного ПО - для установки системы защиты не должна требоваться установка стороннего инсталлятора - включая Microsoft Windows Installer, либо использование служб, дополнительных к ранее используемым.
- 2.4.4.** В связи с необходимостью автоматизации развертывания системы защиты установка должна быть возможна в том числе в режиме командной строки - указанием необходимых параметров установки. В том числе установки в фоновом режиме, необходимости перезагрузки и состава устанавливаемых компонент;
- 2.4.5.** В связи с возможными ограничениями канала доступа в сеть Интернет установка системы защиты должна быть возможной без доступа в сеть Интернет - дистрибутив должен содержать все компоненты системы защиты, а также базы данных признаков вредоносных программ и вредоносных ресурсов сети Интернет, доступ к которым может регулироваться системой защиты.
- 2.4.6.** Для работы системы защиты не должны использоваться внешние библиотеки, а также среда .Net Framework, целостность которых не находится под контролем системы самозащиты и компрометация которых может привести к ошибкам отображения информации системы защиты или иным проблемам, связанным с интерфейсом системы защиты
- 2.4.7.** С целью противодействия вредоносным программам, запущенным на компьютере, система установки должна быть интегрирована с антивирусом - обнаружение и удаление угроз должно быть доступно во время установки.
- 2.4.8.** Система установки должна поддерживать импорт настроек, содержания карантина и хранилища резервных копий папок, сохраненных после удаления ранее установленного антивируса - в случае наличия совместимости версий.
- 2.4.9.** Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.
- 2.4.10.** Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур.
- 2.4.11.** Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов.
- 2.4.12.** В случае наличия системы централизованного управления права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля.

- 2.4.13.** Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках имеющихся у них прав.
- 2.4.14.** Обновление системы защиты должно быть возможно (по выбору администратора системы защиты) с серверов компании поставщика системы защиты, размещенных в сети Интернет, локальной или сетевой папки, компьютеров локальной сети, на которых установлена аналогичная система защиты и создано зеркало обновлений;
- 2.4.15.** В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
- 2.4.16.** Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.
- 2.4.17.** По умолчанию система защиты должна работать в так называемом пользовательском (ограниченном) режиме. Пользователю системы, не являющемуся администратором защиты, не должны быть доступны настройки компонентов системы защиты, а также возможность отключения системы защиты. При работе в данном режиме в интерфейсе системы защиты не должны показываться пункт меню или иконка, нажатие на которые открывает окно или раздел интерфейса с настройками системы защиты. Администратор должен иметь возможность ограничить доступ к настройкам с помощью пароля;
- 2.4.18.** Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях:
- 2.4.18.1.** поиск и удаление вредоносных программ всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
- 2.4.18.2.** обнаружение вредоносных программ, не обнаруживаемых средствами антивирусного ядра, с помощью превентивной защиты, отслеживающей поведение запущенных процессов, а также вредоносных объектов, внедренных в запущенные процессы;
- 2.4.18.3.** проверки ссылок на видоизменение, скрипты и фреймы;
- 2.4.18.4.** проверки файлов по ссылкам до скачивания из сети Интернет на локальный компьютер;
- 2.4.18.5.** проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;
- 2.4.18.6.** выявления вредоносных объектов в HTML- и PDF-документах;
- 2.4.18.7.** выявления и анализа «невидимых» IFRAME-элементов на страницах сайтов и HTML-документах;
- 2.4.18.8.** проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
- 2.4.18.9.** блокировку опасных макросов VBA в реальном времени;

- 2.4.18.10. блокировку перехода по внешним ссылкам в социальных сетях;
- 2.4.18.11. защиту от вредоносных сценариев, загружаемых с Web-страниц;
- 2.4.18.12. защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевого экрана;
- 2.4.18.13. проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО;
- 2.4.18.14. защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе отдельным типам сменных носителей информации, локальным файлам и каталогам, сайтам в сети Интернет;
- 2.4.18.15. помещение найденных зараженных файлов, а также резервных копий объектов, к которым были применены действия, отличные от «Поместить в карантин», в специальное место на жестком диске -«карантин»;
- 2.4.18.16. просмотр местоположения станций и серверов на карте, если заданы географические координаты станции;
- 2.4.18.17. автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
- 2.4.18.18. запуск задач по расписанию и/или сразу после загрузки операционной системы;
- 2.4.18.19. возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке
- 2.4.18.20. защиту возникновения претензий от правообладателей контента путем использования специальной базы данных признаков ресурсов, доступ к которым ограничен по требованию правообладателей.
- 2.4.19. Администратор системы должен иметь возможность:
 - 2.4.19.1.настройки правил защиты от намеренных/непреднамеренных действий посредством блокировки доступа к локальным и сетевым ресурсам (локальным файлам и каталогам, сайтам в сети Интернет) для конкретных пользователей;
 - 2.4.19.2.копировать настройки между учетными записями пользователей;
 - 2.4.19.3.запрещать возможность отправки заданий на печать;
 - 2.4.19.4.запрещать возможность передачи данных по сети;
 - 2.4.19.5.запрещать возможность изменения системного времени и часового пояса;
 - 2.4.19.6.отключать ранее заданные ограничения для конкретной учетной записи;
 - 2.4.19.7.назначать месторасположения карантина при обнаружении зараженных файлов на съемных носителей;
 - 2.4.19.8.используя возможности менеджера карантина, осуществлять повторную проверку объектов, помещенных в карантин;
 - 2.4.19.9.иметь возможность очистки карантина для отдельного диска.
- 2.4.20. Система защиты рабочих станций должна обеспечивать проверку протоколов:
 - 2.4.20.1.НТТР независимо от используемого браузера или иного приложения, получающего трафик;
 - 2.4.20.2.IMAP, SMTP, POP3 независимо от используемого почтового клиента;

- 2.4.20.3.** NNTP (только проверка на вирусы), независимо от почтового клиента.
- 2.4.21.** Система защиты рабочих станций должна обеспечивать проверку почтовых сообщений, передаваемых по протоколу MAPI для Microsoft Outlook 2000 (Outlook 9)/2002 (Outlook 10 или Outlook XP)/2003 (Outlook 11)/2007/2010/2013.
- 2.4.22.** Система защиты рабочих станций должна автоматически обеспечивать проверку трафика передаваемого по поддерживаемым системой защиты протоколам:
- 2.4.22.1.** вне зависимости от порта, через который передается трафик - без необходимости указания списка проверяемых портов для конкретных протоколов;
- 2.4.22.2.** включая проверку трафика, передаваемого по зашифрованному соединению SSL.
- 2.4.23.** Система защиты рабочих станций должна обеспечивать фильтрацию трафика в мгновенных сообщениях Mail.Ru Agent, ICQ, Jabber, QIP, Pidgin и другие, включая антивирусную проверку пересылаемых вложений, а также автоматическое удаление из сообщений ссылок, ведущих на вредоносные и фишинговые сайты.
- 2.4.24.** Система защиты рабочих станций должна обеспечивать фильтрацию выдачи результатов поисковых систем Google, Yandex, Yahoo!, Bing, Rambler с показом только безопасных с точки зрения поисковых систем и системы защиты ресурсов.
- 2.4.25.** Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством:
- 2.4.25.1.** антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
- 2.4.25.2.** проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы;
- 2.4.25.3.** непрерывного фонового сканирования и нейтрализации активных угроз. В том числе в критических областях Windows, оперативной памяти, запущенных процессах, MBR/VBR дисков, BIOS;
- 2.4.25.4.** проверки ссылок и файлов с помощью репутационного сервиса облачной защиты - в том числе с помощью базы данных алгоритмов работы вредоносных программ.
- 2.4.26.** В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
- 2.4.27.** С целью защиты от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) Система должна:
- 2.4.27.1.** обеспечивать защиту критически важных частей системы (в том числе папок и ветвей реестра) от модификаций вредоносными программами, в том числе блокировать попытки:
- 2.4.27.1.1.** изменения вредоносными программами загрузочных областей диска;
- 2.4.27.1.2.** изменения нежелательным образом пользовательских файлов (в том числе действия троянцев-шифровальщиков) ;

- 2.4.27.1.3. изменения файла HOSTS;
- 2.4.27.1.4. добавления новых задач в логику работы операционной системы;
- 2.4.27.1.5. изменения правил запуска ранее установленных программ;
- 2.4.27.1.6. изменения параметров работы системных служб, в том числе процесса создания резервных копий файлов;
- 2.4.27.1.7. загрузки новых или неизвестных драйверов без ведома пользователя, установки новых виртуальных устройств, загрузки в браузер вредоносных плагинов, в том числе блокировщиков браузера;
- 2.4.27.1.8. автозапуска вредоносных программ;
- 2.4.27.1.9. получения низкоуровневого доступа к диску;
- 2.4.27.1.10. регистрации вредоносных программ в реестре для последующего запуска;
- 2.4.27.1.11. отключения безопасного режима Windows путем блокировки изменения реестра;
- 2.4.27.1.12. сокрытия присутствия троянской программы в контролируемой системе в виде руткита.
- 2.4.27.2. блокировать попытки установления каналов связи между вредоносным ПО, ранее установленным на компьютер и удаленными серверами злоумышленников;
- 2.4.27.3. с помощью превентивной защиты, отслеживающей работу всех процессов системы в поисках действий, характерных для процессов вредоносных программ и не позволяющей вредоносным объектам внедриться в процессы других программ или каким-либо способом разместить вредоносные файлы в защищаемой системе, выявлять и прекращать работу вредоносных, подозрительных или ненадежных сценариев и процессов;
- 2.4.27.4. обеспечивать защиту от эксплойтов (программ, эксплуатирующих как уже известные, так и еще неизвестные уязвимости) путем внедрения специального модуля защиты в контролируемые процессы;
- 2.4.27.5. ограничивать время работы конкретного сотрудника на защищаемом компьютере - с целью исключения доступа у компьютера в остальное время неопределенного круга лиц. Система ограничения доступа должна позволять:
 - 2.4.27.5.1. задавать время работы на компьютере для выходных и будних дней для каждого сотрудника, а также ограничения по доступу в сеть Интернет;
 - 2.4.27.5.2. задавать суммарное время работы на компьютере для конкретного сотрудника;
 - 2.4.27.5.3. автоматически блокировать доступ к защищаемому компьютеру в ночное время.
- 2.4.27.6. ограничивать доступ к определенным ресурсам сети Интернет - согласно белым и черным спискам ресурсов сети, предопределенным группам ресурсов;
- 2.4.27.7. ограничивать доступ к определенным файлам и папкам - с указанием типа доступа объектам (блокировать доступ или разрешать только чтение);
- 2.4.27.8. обеспечивать возможность использования на защищаемом компьютере только устройств, входящих список разрешенных. Администратор Системы должен иметь возможность:
 - 2.4.27.8.1. контроля доступа к таким типам устройств, как дисковые накопители, приводы DVD/CD-ROM, клавиатуры, компьютерные мыши, сетевые карты, игровые устройства, USB-устройства;

- 2.4.27.8.2.** импорта и экспорта правил использования устройств (в том числе с помощью функционала управления удаленными компьютерами антивирусной сети), а также формирования правил блокировки шин и классов устройств, создания списка разрешенных устройств для заблокированных шин и классов устройств;
- 2.4.27.8.3.** задать уровень доступа к устройству осуществляется в форме полного запрета доступа всем процессам операционной системы или в форме интерактивного режима, в котором пользователю выводится оповещение о попытке доступа к устройству. Для устройств с файловой системой администратор Системы должен иметь возможность задать тип доступа - разрешать полный доступ к устройству или доступ только на чтение.
- 2.4.27.9.** обеспечивать возможность полного запрета использования USB-устройств и CD/DVD-приводов;
- 2.4.27.10.** обеспечивать создание резервных копий папок, указанных пользователем, а также восстановление данных из хранилища как системой защиты, так и самим пользователем в любой момент времени.
- 2.4.28.** модуль превентивной защиты должен:
- 2.4.28.1.** поддерживать возможность создания профилей - групп настроек, применяемых пользователем или администратором защищаемой системы - как для системы превентивной защиты в целом, так и для конкретных приложений с целью исключения потенциальных конфликтов при их работе.
- 2.4.29.** система создания резервных копий папок должна поддерживать возможность:
- 2.4.29.1.** выбора защищаемых каталогов;
- 2.4.29.2.** выбора диска для хранения защищаемых копий;
- 2.4.29.3.** настройки расписаний копирования;
- 2.4.29.4.** создания защищенных копий по требованию.
- 2.4.30.** С целью ускорения проверки Система должна поддерживать возможность исключения из проверки различными компонентами системы защиты:
- 2.4.30.1.** данных, передаваемых по защищенным протоколам (в том числе HTTPS), а также трафика доверенных приложений (имеющих валидную цифровую подпись) ;
- 2.4.30.2.** файлов и папок;
- 2.4.30.3.** ресурсов сети Интернет;
- 2.4.30.4.** почтовых адресов;
- 2.4.30.5.** доверенных программ;
- 2.4.31.** С целью ускорения проверки Брандмауэр (файрвол) должен поддерживать базу доверенных приложений, а также позволять создавать правила работы для приложений.
- 2.4.32.** В случае отсутствия централизованного управления системой защиты Система защиты рабочей станции должна поддерживать возможность удаленного управления Системами защиты, установленными на компьютерах в пределах одной локальной сети.
- 2.4.33.** Подсистема показа статистики Системы защиты должна:
- 2.4.33.1.** отображать время возникновения (детектирования) угроз;

- 2.4.33.2.** списки запрещенных сайтов, доступ к которым был запрошен с защищаемого компьютера.
- 2.4.34.** Подсистема статистики должна иметь возможность отображения только необходимых для анализа сообщений - в том числе создания выборки сообщений отдельных компонентов системы защиты, сообщений с определенными кодами
- 2.4.35.** В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения.
- 2.5. Требования к программным средствам антивирусной защиты рабочих станций Linux**
- 2.5.1.** Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.
- 2.5.2.** Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.
- 2.5.3.** Система, используя актуальную на момент проведения тендера версию ПО должна обеспечивать защиту ресурсов рабочих станций функционирующих под управлением операционных систем:
- 2.5.3.1.** Astra Linux Common Edition (релиз «Орел»), версия 2.12
- 2.5.3.2.** Astra Linux Special Edition (релиз «Смоленск»), версия 1.5
- 2.5.3.3.** Astra Linux Special Edition (релиз «Смоленск»), версия 1.6
- 2.5.3.4.** Astra Linux Special Edition (очередное обновление 1.7);
- 2.5.3.5.** CentOS 7;
- 2.5.3.6.** CentOS 8;
- 2.5.3.7.** Debian GNU/Linux 9;
- 2.5.3.8.** Debian GNU/Linux 10;
- 2.5.3.9.** Red Hat Enterprise Linux 7;
- 2.5.3.10.** Red Hat Enterprise Linux 8;
- 2.5.3.11.** Ubuntu 18.04;
- 2.5.3.12.** Ubuntu 20.04
- 2.5.3.13.** Альт 8СП;
- 2.5.3.14.** Альт Рабочая станция 9;
- 2.5.3.15.** Альт Сервер 9;
- 2.5.3.16.** ОС типового дистрибутива АИС ФССП России (Гослинукс IC6);
- 2.5.3.17.** РЕД ОС 7.2 МУРОМ;
- 2.5.3.18.** РЕД ОС 7.3 МУРОМ.
- 2.5.4.** Установка модулей Системы в зависимости от типа используемой операционной системы должна происходить с помощью универсального пакета для UNIX систем, независимого от типа и версии используемой операционной системы, репозитория или пакета, рассчитанного на работу с используемым в ОС менеджером пакетов
- 2.5.5.** Установка и обновление Системы должны быть возможны как через средства командной строки, так и с помощью графического инсталлятора.

- 2.5.6. Система установки должна включать возможность автоматической установки модулей, необходимых для компонентов Системы.
- 2.5.7. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности работы. При этом, в случае необходимости внесения изменений, Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках имеющихся у них прав.
- 2.5.8. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением заданных файловых областей.
- 2.5.9. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
- 2.5.9.1. поиск и удаление вирусов всех известных типов в файлах;
- 2.5.9.2. антивирусного сканирования ресурсов сервера как по команде администратора, так и по расписанию, заключающегося в однократной полной или выборочной проверке на наличие угроз объектов;
- 2.5.9.3. помещения найденных зараженных и подозрительных файлов в карантин для дальнейшего анализа;
- 2.5.9.4. автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
- 2.5.9.5. запуска задач по расписанию и/или сразу после загрузки операционной системы;
- 2.5.9.6. настройки расписания сканирования с указанием параметров запуска.
- 2.5.10. Управление программой должно осуществляться как непосредственно через конфигурационные файлы, так и через графический интерфейс, реализованный для операционных систем типа Linux. Система управления должна поддерживать возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих антивирусной проверке, действий по отношению к вредоносным объектам различных типов.
- 2.5.11. Администратор системы должен иметь возможность:
- 2.5.11.1. Определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки;
- 2.5.11.2. определять типы проверяемых файлов, в том числе с использованием масок;
- 2.5.11.3. задавать различные действия по отношению к различным типам вредоносных объектов в случае их обнаружения;
- 2.5.11.4. управлять детализацией протоколов антивирусной проверки;
- 2.5.11.5. просматривать информацию об используемом ключевом файле и его владельце;
- 2.5.11.6. запускать периодическую проверку в приоритетном или в фоновом режиме;
- 2.6. Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows**
- 2.6.1. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
- 2.6.1.1. Осуществление антивирусной защиты на серверах, включая защиту от руткит-технологий.

- 2.6.2.** Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.
- 2.6.3.** Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию ПО, должна обеспечивать защиту серверов под управлением операционных систем:
- 2.6.3.1.** Microsoft Windows Server 2003;
 - 2.6.3.2.** Microsoft Windows Server 2008;
 - 2.6.3.3.** Microsoft Windows Server 2012;
 - 2.6.3.4.** Microsoft Windows Server 2016;
 - 2.6.3.5.** Microsoft Windows Server 2019;
 - 2.6.3.6.** Microsoft Windows Server 2022.
- 2.6.4.** Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.
- 2.6.5.** Антивирусное программное обеспечение должно по умолчанию иметь оптимальные настройки с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках имеющихся у них прав.
- 2.6.6.** Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением системы.
- 2.6.7.** В Системе должна быть реализована возможность выбора приоритета сканирования, а также остановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
- 2.6.8.** Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.
- 2.6.9.** Система должна обеспечивать:
- 2.6.9.1.** поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
 - 2.6.9.2.** проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
 - 2.6.9.3.** блокировку опасных макросов VBA в реальном времени;
 - 2.6.9.4.** защиту от вредоносных сценариев, загружаемых с веб-страниц;
 - 2.6.9.5.** помещение найденных зараженных файлов в специальное место на жестком диске — «карантин»;
 - 2.6.9.6.** автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
 - 2.6.9.7.** запуск задач по расписанию и/или сразу после загрузки операционной системы.

2.6.10. Система защиты серверов под управлением семейства ОС Microsoft Windows должна обеспечивать реализацию следующих функциональных возможностей:

2.6.10.1. проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов посредством:

2.6.10.1.1. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;

2.6.10.1.2. проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.

2.6.11. В Системе должна быть реализована самозащита для всех ее объектов, в том числе критических файлов, процессов, окон, ключей и прочего, от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.

2.7. Требования к программным средствам антивирусной защиты файловых серверов UNIX

2.7.1. Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.

2.7.2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных файлов всех типов.

2.7.3. Система, используя актуальную на момент проведения тендера версию ПО, должна обеспечивать защиту ресурсов серверов, использующих Samba версий 3.0.x - 3.6.x, и функционирующих под управлением операционных систем:

2.7.3.1. FreeBSD 11;

2.7.3.2. FreeBSD 12;

2.7.3.3. Astra Linux Common Edition (релиз «Орел»), версия 2.12

2.7.3.4. Astra Linux Special Edition (релиз «Смоленск»), версия 1.5

2.7.3.5. Astra Linux Special Edition (релиз «Смоленск»), версия 1.6

2.7.3.6. Astra Linux Special Edition (очередное обновление 1.7);

2.7.3.7. CentOS 7;

2.7.3.8. CentOS 8;

2.7.3.9. Debian GNU/Linux 9;

2.7.3.10. Debian GNU/Linux 10;

2.7.3.11. Red Hat Enterprise Linux 7;

2.7.3.12. Red Hat Enterprise Linux 8;

2.7.3.13. Ubuntu 18.04;

2.7.3.14. Ubuntu 20.04

2.7.3.15. Альт 8СП;

2.7.3.16. Альт Рабочая станция 9;

2.7.3.17. Альт Сервер 9;

2.7.3.18. ОС типового дистрибутива АИС ФССП России (Гослинукс IC6);

2.7.3.19. РЕД ОС 7.2 МУРОМ;

2.7.3.20. РЕД ОС 7.3 МУРОМ.

2.7.4. Интеграция Системы с Samba должна осуществляться с помощью модуля VFS (Virtual File System).

2.7.5. В случае использования версий Samba, отличных от вышеперечисленных, либо Samba для 64-битных платформ семейства Linux должна существовать возможность компиляции модулей интеграции из исходных кодов.

2.7.6. Установка модулей Системы в зависимости от типа используемой операционной системы должна происходить с помощью универсального пакета для UNIX систем, независимого от типа и версии используемой операционной системы, репозитория или пакета рассчитанного на работу с используемым в ОС менеджером пакетов

2.7.7. Установка и обновление Системы должны быть возможны как через средства командной строки, так и с помощью графического инсталлятора.

2.7.8. Система установки системы должна включать возможность автоматической установки модулей, необходимых для установки необходимых компонентов.

2.7.9. Компоненты системы должны иметь возможность управления использованием серверных ресурсов при выполнении сканирования файлового пространства.

2.7.10. В Системе должна быть реализована возможность задания приоритета антивирусного сканирования.

2.7.11. Система должна поддерживать возможность порождения нескольких одновременно действующих процессов проверки.

2.7.12. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы настройки. При этом, в случае необходимости внесения изменений, Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователем в рамках имеющихся у них прав.

2.7.13. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением заданных файловых областей.

2.7.14. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:

2.7.14.1. поиск и удаление вирусов всех известных типов в файлах;

2.7.14.2. антивирусного сканирования ресурсов сервера, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде администратора, так и по расписанию;

2.7.14.3. антивирусной проверке «на лету» файлов, загружаемых как на сервер, так и с него;

2.7.14.4. помещения найденных зараженных и подозрительных файлов в карантин для дальнейшего анализа;

2.7.14.5. автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;

2.7.14.6. запуска задач по расписанию и/или сразу после загрузки операционной системы;

2.7.14.7. настройки расписания сканирования с указанием параметров запуска.

2.7.15. Управление программой должно осуществляться как с помощью веб-интерфейса, так и непосредственно через конфигурационные файлы. Система управления должна поддерживать возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих антивирусной проверке, и действий по отношению к вредоносным объектам различных типов.

2.7.16. Администратор системы должен иметь возможность:

2.7.16.1. определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки;

2.7.16.2. определять типы проверяемых файлов, в том числе с использованием масок;

2.7.16.3. задавать различные действия по отношению к различным типам вредоносных объектов в случае их обнаружения.

2.7.16.4. управлять детализацией протоколов антивирусной проверки;

2.7.16.5. просматривать результаты антивирусной проверки;

2.7.16.6. просматривать информацию об используемом ключевом файле и его владельце;

2.7.16.7. запускать периодическую проверку в приоритетном или в фоновом режиме;

2.7.16.8. использовать альтернативные языковые файлы.

2.8. Требования по комплектности поставки

2.8.1. В состав Системы должны входить:

2.8.1.1. программные средства антивирусной защиты, необходимые для выполнения требований данного технического задания;

2.8.1.2. программные средства централизованного управления, мониторинга и обновления;

2.8.1.3. обновляемые базы данных сигнатур всевозможных вредоносных программ.

2.8.2. Комплект поставки должен содержать:

2.8.2.1. необходимый набор серийных номеров либо ключевых файлов;

2.8.2.2. дистрибутив Системы;

2.8.2.3. файлы эксплуатационной документации в формате pdf (Adobe Acrobat Reader), в том числе руководство пользователя (администратора). Поставляемая документация должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

2.9. Требования по технической поддержке Системы

2.9.1. Техническая поддержка должна предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет.

2.9.2. Техническая поддержка должна включать возможность написания специального ПО, предназначенного для устранения последствий воздействия вредоносного ПО на зараженную систему. В том числе утилит расшифровки файлов, если данная операция является возможной

2.9.3. Техническая поддержка должна обеспечивать возможность получения специалистами и пользователями Заказчика информационной помощи по установке Системы и ее компонентов, в том числе:

- 2.9.3.1. ответов на вопросы, а также получение инструкций относительно процесса установки и применения программного обеспечения;
- 2.9.3.2. ответов на вопросы о наличии проблем в работе программного обеспечения, а также помощи в определении того, является ли данная проблема результатом сбоя программного обеспечения, ошибок настройки или же она вызвана проблемами, связанными с внешними условиями существования или установкой программного обеспечения.
- 2.9.4. Web-сайт производителя Системы должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов производителя.

А. Мельников
М. Мельников

