Приложение 1 к техническому заданию на систему антивирусной защиты	Отдел: Департамент ИТ сопровождения и инфраструктуры, отдел ИБ Дата: 17.10.2024

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ к системе антивирусной защиты

Приложение 1 к техническому заданию на систему антивирусной защиты	Отдел: Департамент ИТ сопровождения и инфраструктуры, отдел ИБ Дата: 17.10.2024

I. Технические требования

1. Описание услуги

№	Услуга	Описание
1	Система антивирусной защиты	– Система антивирусной защиты служит для обеспечения защиты ИТ-инфраструктуры Заказчика от целевых и массовых компьютерных атак путем обнаружения и реагирования на угрозы информационной безопасности на серверах и рабочих станциях (далее — **защита конечных устройств**) корпоративной сети и защиты от угроз и спама информации, поступающей Заказчику по электронной почте (далее – **защита электронной почты**).

2. Антивирусная защита

№	Группы требований	Описание
1	Требования к архитектуре	– Система должна быть построена на основе программного и аппаратного обеспечения, размещаемого на объектах Заказчика. – Программные компоненты Системы должны быть реализованы на базе клиент-серверной сетевой архитектуры и включать следующие основные функциональные компоненты: o клиентские компоненты — компоненты Системы, размещаемые на конечных устройствах: серверах, рабочих станциях; предназначенные для сбора и обработки информации, а также реализации функций реагирования; o серверные компоненты — компоненты Системы, размещаемые на аппаратном и (или) программном обеспечении (в виртуальной инфраструктуре Заказчика), обеспечивающие централизованное управление клиентскими компонентами и поступающей от них информацией. – Система должна поддерживать схемы развертывания, включающие несколько клиентских компонентов, установленных в различных средах функционирования. – Клиентские компоненты Системы должны поддерживать развертывание на конечных устройствах под управлением следующих ОС:

		○ Microsoft Windows 7 x64/x86; ○ Microsoft Windows 8, 8.1 x64; ○ Microsoft Windows 10 x64; ○ Microsoft Windows Server: 2012, 2012R2, 2016, 2019; ○ CentOS: 7, 8; ○ RHEL: 7, 8; ○ Debian: 10,11; ○ Ubuntu: 18.04 LTS, 20.04 LTS; – Клиентские компоненты Системы должны поддерживать возможность функционирования (проводить анализ и выполнять реагирование) в автономном режиме работы.
2	Требования по интеграции с другими системами	Система должна обеспечивать возможность интеграции со следующими смежными системами: – внешними syslog-серверами — для отправки сведений о событиях ИБ; – Система позволяет интегрироваться со службой доменов Active Directory.
3	Общие функциональные требования	Требования к подсистеме: 1. Подсистема антивирусной защиты (далее – ПАЗ) должна обеспечивать защиту рабочих станций и серверной инфраструктуры Заказчика от запуска вредоносного кода. 2. ПАЗ должна обеспечивать защиту от вредоносного кода на уровне входного контроля устройств и переносных (отчуждаемых) носителей информации. 4. ПАЗ должна обеспечивать поддержку работы и обновления в фоновом режиме. 5. ПАЗ должна обеспечивать контроль целостности программных компонентов антивирусной защиты (далее – АВЗ). 6. ПАЗ должна обеспечивать контроль отключения компонентов АВЗ, а также обеспечивать постоянное обновление антивирусных сигнатур. 7. ПАЗ должна обеспечивать выполнение сканирования на наличие вредоносного кода по расписанию. 8. ПАЗ должна осуществлять контроль запуска самораспаковывающихся архивов и исполняемых файлов и их проверку на наличие вредоносного кода. 9. ПАЗ должна обеспечивать регистрацию результатов проверок на наличие вредоносного кода и срабатывания компонентов АВЗ, а также их отключения и сбоев. 10. ПАЗ должна обеспечивать поддержку отключения портов для средств вычислительной техники. 11. ПАЗ должна обеспечивать поддержку регистрации разрешенных съемных носителей. 13. Агенты защиты должны передавать данные на Сервер управления.

		14. БД должна подключаться к Серверу управления и хранить статистические данные о событиях Агентов защиты, настройки самого Сервера управления, параметры защищаемых устройств и Агентов защиты, устанавливаемых на защищаемые объекты. 15. Установленные Агенты защиты должны иметь возможность централизованного управления с Сервера управления. – Сервер управления должен иметь возможность централизованной установки, обновления и удаления Агентов защиты.
4	Требования к функциям управления	– Должна обеспечиваться возможность выбора мер реагирования, применяемых к конкретной группе конечных устройств. – Требования к функциям управления, обеспечиваемым серверными компонентами: – Должен предоставляться веб-интерфейс, обеспечивающий доступ к управлению Системой. – Должна поддерживаться группировка клиентских компонентов. – Должно поддерживаться управление группами компонентов в автоматизированном (на основе задач, запускаемых в ручном режиме) или автоматическом режиме (на основе автоматически запускаемых задач). – Должно обеспечиваться управление конфигурацией клиентских компонентов (в том числе управление политиками и правилами, действующими для групп клиентских компонентов). – Должно обеспечиваться управление авторизацией клиентских компонентов серверными компонентами.
5	Требования к функциям передачи данных	– Требования к функциям передачи данных, выполняемым клиентскими компонентами: o Клиентские компоненты должны обеспечивать отправку данных серверным компонентам в автоматическом режиме в соответствии с предустановленными политиками. o Клиентские компоненты должны обеспечивать отправку данных серверным компонентам при получении запроса на передачу данных. o Клиентские компоненты должны передавать сведения о собственном состоянии серверным компонентам в автоматическом режиме. – Требования к функциям передачи данных, выполняемым серверными компонентами: o Серверные компоненты должны обеспечивать возможность передачи регистрируемых Системой событий ИБ в Систему мониторинга событий информационной безопасности.

		○ Серверные компоненты должны обеспечивать прием информации сведений об угрозах из базы знаний разработчика системы.
6	Требования к функциям обновления	– Требования к обновлению клиентских компонентов: ○ Должна поддерживаться возможность автоматизированного (по команде из веб-интерфейса или графического-интерфейса) обновления клиентских компонентов; ○ Должна поддерживаться возможность автоматического (на основании планировщика задач) обновления клиентских компонентов. – Требования к обновлению серверных компонентов: ○ Должна обеспечиваться возможность автоматического получения файлов с обновлениями серверных компонентов Системы с сервера обновлений разработчика; ○ Должна поддерживаться возможность автоматического обновления базы знаний (пакетов экспертизы) с сервера обновлений разработчика; ○ Должна поддерживаться возможность автоматизированного обновления базы знаний (пакетов экспертизы) из локального источника.
9	Требования к функциям обеспечения собственной безопасности	– Требования к функциям обеспечения собственной безопасности (общие) – Должна обеспечиваться идентификация, аутентификация и авторизация пользователей Системы на основе учетных записей. Доступ к веб-интерфейсу или графическому интерфейсу, предназначенному для управления системой, должен предоставляться только после авторизации пользователя. – Должна обеспечиваться реализация ролевой модели управления доступом к функциям Системы. – Должна обеспечиваться возможность управления учетными записями пользователей Системы, предоставляемая уполномоченным пользователям: ○ созданием учетных записей, их статусом (действующая/заблокированная); ○ назначение ролей; ○ методами аутентификации (локальная база или LDAP -аутентификация). – Должна обеспечиваться возможность блокировки учетной записи пользователя в Системе. – Должно обеспечиваться журналирование действий пользователей. – При любом взаимодействии через API должна осуществляться проверка прав пользователя.

		– Взаимодействие между компонентами системы должно осуществляться по защищенному каналу – До начала использования клиентских компонентов должна осуществляться их авторизация, выполняемая уполномоченным пользователем через веб-интерфейс Системы. – Система должна обеспечивать возможность резервного копирования и архивации конфигурационных данных. – Отказоустойчивость ПАЗ обеспечивается посредством резервного копирования и восстановления из резервной копии (конфигураций и сведений о событиях безопасности) средствами ПАЗ. В случае сбоя должен обеспечиваться возврат к резервной копии, снятой с Сервера управления. – Временная недоступность Сервера управления не должна влиять на работу Агентов защиты.
10	Дополнительные требования. Перечисленные функции приведены как примеры снижения рисков соответствующих угроз – важно наличие соответствующих функций, снижающих данные угрозы возможно и другим способом до сравнимого уровня.	Защита конечных устройств должна дополнительно обеспечивать следующие функциональные возможности: – 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; – блокировки действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов; – отката 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; – проверки сетевого трафика, поступающего на конечное устройство по протоколам HTTPS (SSL 3.0, TLS 1.x), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки

		доверенных ресурсов и работой в режиме блокировки или статистики; – блокировки 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; – защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства; – контроля сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений; – наличие функции Анти-Бриджинг для запрета рабочей станции одновременно устанавливать сетевые соединения по разным каналам передачи информации (проводной и беспроводной) для предотвращения создание сетевых мостов; – желательно наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi; – запуска специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью получения и отправки отчета по обнаруженным уязвимостям в средство управления уязвимостями производителя решений класса EDR; – полнодискового шифрования с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем; – интеграции с Windows Defender;

3. Защита электронной почты

№	Группы требований	Описание
1	Общие требования	Защита электронной почты должна включать: – Программные средства антивирусной защиты и фильтрации спама с помощью отдельного сервера – Программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux; – Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange; – Эксплуатационную документацию на русском языке. – Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языках.
2	Защита с помощью отдельного сервера	– Система должна поддерживать установку на физический и виртуальный сервер, для работы в виртуальной среде, поддерживать установку на следующие гипервизоры: o VMware ESXi 7.0 Update 3. o VMware ESXi 8.0 Update 2. o Microsoft Hyper-V Server 2019. o Windows Server 2019 Standard с установленной ролью Hyper-V. – Программные средства антивирусной защиты и фильтрации спама должны обеспечивать реализацию следующих функциональных возможностей: o поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения; o проверка входящего потока почтовых сообщений на наличие спама, потенциального спама, массовых рассылок (в том числе маркетинговых рассылок), удаление выявленных сообщений, помещение копии сообщений в карантин; o наличие общего карантина сообщений; o управление карантином из веб-интерфейса; o детектирование вредоносных и фишинговых ссылок в теле письма; o наличие эвристических методов детектирования; o возможность использования репутационных облачных сервисов; o возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;

№	Группы требований	Описание
		○ наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз; ○ обнаруживать, блокировать и лечить зараженные почтовые сообщения и зараженные вложения, удалять сообщения и вложения, помещать копии сообщений в карантин; ○ обнаруживать и блокировать сообщения, содержащие макросы во вложении (например, файлы форматов Microsoft Office с макросами), удалять сообщения или вложения, помещать копии сообщений в карантин; ○ обнаруживать и блокировать сообщения, содержащие зашифрованные объекты, удалять сообщения или вложения, помещать копии сообщений в карантин; ○ обнаруживать и блокировать сообщения, содержащие архивы, распознавать типы файлов внутри архивов, блокировать отдельные файлы внутри архивов; ○ выполнять контентную фильтрацию сообщений по имени, размеру и типу вложений, заголовкам, теме и телу письма, определять формат и тип вложения, независимо от его расширения, удалять сообщения, содержащие вложения определенного формата или с определенным именем или сообщения, размер которых превышает допустимый, помещать копии сообщений в хранилище; ○ возможность включить или отключить добавление информационных заголовком в начало сообщения и в MIME-часть сообщения; ○ сохранять резервные копии сообщений в карантине по результатам их обработки модулями защиты; ○ сохранять сообщения из карантина в файл и пересылать сообщения получателям; ○ возможность развертывания кластерной архитектуры почтовых серверов с возможностью централизованного управления для масштабирования решения (как горизонтально, так и вертикально); ○ интеграции со службами каталогов Active Directory и Open LDAP.

№	Группы требований	Описание
		○ возможность проверки получателей сообщений согласно списку допустимых получателей, наполняемому вручную или при интеграции с LDAP; ○ возможность отправки ловушек по протоколу SNMP; ○ обрабатывать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей; ○ отправлять уведомления пользователям о результатах проверки их сообщений модулями программы; ○ поддерживать работу персонального карантина на основе LDAP-записей; ○ доступ к персональному карантину должен осуществляться на основе учетных записей LDAP; ○ отправлять уведомления пользователям о состоянии персонального карантина, уведомления должны содержать список последних сообщений в карантине; ○ возможность просмотра содержимого сообщения в веб-интерфейсе продукта; ○ настройки расписания отправки уведомлений; ○ возможность почтовой рассылки с информацией о последних полученных письмах, помещенных в персональное хранилище пользователя. ○ обновлять базы программы с серверов обновлений и пользовательских ресурсов (HTTP- и FTP-серверов) по расписанию и по требованию; ○ отправлять и получать сообщения по защищенному каналу TLS/SSL, осуществлять управление ключами шифрования; ○ осуществлять проверку подлинности отправителей сообщений с помощью технологий SPF, DKIM и DMARC; ○ подписывать исходящие сообщения электронной почты с помощью технологии DKIM; ○ добавлять предупреждения о небезопасном вложении к входящим сообщениям в теме письма; ○ просматривать журнал событий, аудита в веб интерфейсе программы и загружать его на жесткий диск; ○ фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail

№	Группы требований	Описание
		и/или IP-адрес) на основе собственных «черных» и «белых» списков; ○ проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL); ○ проверка с помощью сервиса SPAM URI Realtime Blocklists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма; ○ проверка графических вложений на совпадение с известными сигнатурами спам-сообщений; ○ выявление подозрительных, поврежденных и защищенных паролем файлов, а также файлов, в результате проверки которых произошла ошибка; ○ перенос в карантин зараженных, подозрительных и поврежденных объектов почтового трафика, определять защищенные паролем файлы, а также файлы, в результате проверки которых произошла ошибка; ○ использование регулярных выражений при создании правил фильтрации; ○ в правилах фильтрации сообщений электронной почты указывать пользователей и группы пользователей из Microsoft Active Directory и generic LDAP; ○ наличие встроенных ролей администратора и специалиста поддержки; ○ возможность уведомления отправителя, получателя и администратора сервера о почтовом сообщении, содержащем заражённые и подозрительные объекты; ○ управление работой программы должно осуществлять как стандартными средствами операционной системы с помощью командной строки, так и через специальный веб-интерфейс, работающий на браузерах: Mozilla Firefox версии 119 или выше, Google Chrome версии 96 или выше, Microsoft Edge версии 96 или выше; ○ должна поддерживаться возможность интеграции с системами типа «песочница» для оправки файлов, полученных системой защиты веб-трафика для анализа, а также для получения результатов сканирования;

№	Группы требований	Описание
		○ возможность формировать отчеты за выбранный период (сутки, неделя, месяц, год) в формате PDF; ○ обнаруживать сообщения с Юникод-спуфингом. В случае обнаружения Юникод-спуфинга считаеть сообщение спамом. ○ возможность управления маршрутизацией почтового трафика через веб-интерфейс; ○ осуществлять быструю настройку MTA с помощью мастера быстрой настройки; ○ настраивать режимы TLS-шифрования сообщений для ситуаций, когда система принимает сообщения от другого сервера (действует как Сервер) или пересылает сообщения на другой сервер (действует как Клиент), а также настраивать параметры TLS для отдельных доменов.
3	Защита для почтовых серверов, установленных на Linux	– Программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий: ○ CentOS 6.9. ○ CentOS 7.4. ○ Red Hat Enterprise Linux 7.4. ○ Ubuntu Server 14.04.5 LTS. ○ Ubuntu Server 16.04.4 LTS. ○ Debian GNU / Linux 9.3. ○ FreeBSD 11.1. – Программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux должны функционировать совместно с почтовыми системами следующих версий: ○ Exim-4.86 до 4.92. ○ Postfix-2.6 и выше. ○ Sendmail-8.14 и выше. ○ Qmail-1.03 и выше. – Программные средства антивирусной защиты и фильтрации спама должны обеспечивать реализацию следующих функциональных возможностей: ○ поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и

№	Группы требований	Описание
		исходящих почтовых сообщений, включая вложения; ○ проверка входящего потока почтовых сообщений на наличие спама, потенциального спама, массовых рассылок (в том числе маркетинговых рассылок), удаление выявленных сообщений, помещение копии сообщений в карантин; ○ наличие общего карантина сообщений; ○ управление карантином из веб-интерфейса; ○ детектирование вредоносных и фишинговых ссылок в теле письма; ○ наличие эвристических методов детектирования; ○ возможность использования репутационных облачных сервисов; ○ возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации; ○ наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз; ○ обнаруживать, блокировать и лечить зараженные почтовые сообщения и зараженные вложения, удалять сообщения и вложения, помещать копии сообщений в карантин; ○ обнаруживать и блокировать сообщения, содержащие макросы во вложении (например, файлы форматов Microsoft Office с макросами), удалять сообщения или вложения, помещать копии сообщений в карантин; ○ обнаруживать и блокировать сообщения, содержащие зашифрованные объекты, удалять сообщения или вложения, помещать копии сообщений в карантин; ○ обнаруживать и блокировать сообщения, содержащие архивы, распознавать типы файлов внутри архивов, блокировать отдельные файлы внутри архивов; ○ выполнять контентную фильтрацию сообщений по имени, размеру и типу вложений, определять формат и тип вложения, независимо от его расширения, удалять сообщения, содержащие вложения определенного формата или с определенным именем или сообщения, размер

№	Группы требований	Описание
		которых превышает допустимый, помещать копии сообщений в хранилище; ○ сохранять резервные копии сообщений в карантине по результатам их обработки модулями защиты; ○ сохранять сообщения из карантина в файл и пересылать сообщения получателям; ○ интеграции со службами каталогов Active Directory и Open LDAP; ○ возможность отправки ловушек по протоколу SNMP; ○ обрабатывать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей; ○ отправлять уведомления пользователям о результатах проверки их сообщений модулями программы; ○ поддерживать работу персонального карантина на основе LDAP-записей; ○ доступ к персональному карантину должен осуществляться на основе учетных записей LDAP; ○ отправлять уведомления пользователям о состоянии персонального карантина, уведомления должны содержать список последних сообщений в карантине; ○ настройки расписания отправки уведомлений; ○ обновлять базы программы с серверов обновлений производителя и пользовательских ресурсов (HTTP- и FTP-серверов) по расписанию и по требованию; ○ отправлять и получать сообщения по защищенному каналу TLS/SSL, осуществлять управление ключами шифрования; ○ осуществлять проверку подлинности отправителей сообщений с помощью технологий SPF, DKIM и DMARC; ○ добавлять предупреждения о небезопасном вложении к входящим сообщениям в теме письма; ○ просматривать журнал событий, аудита в веб интерфейсе программы; ○ фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;

№	Группы требований	Описание
		○ проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL); ○ проверка с помощью сервиса SPAM URI Realtime Blocklists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма; ○ проверка графических вложений на совпадение с известными сигнатурами спам-сообщений; ○ выявление подозрительных, поврежденных и защищенных паролем файлов, а также файлов, в результате проверки которых произошла ошибка; ○ перенос в карантин зараженных, подозрительных и поврежденных объектов почтового трафика, определять защищенные паролем файлы, а также файлы, в результате проверки которых произошла ошибка; ○ использование регулярных выражений при создании правил фильтрации; ○ в правилах фильтрации сообщений электронной почты указывать пользователей и группы пользователей из Microsoft Active Directory и generic LDAP; ○ наличие встроенных ролей администратора и специалиста поддержки; ○ возможность уведомления отправителя, получателя и администратора сервера о почтовом сообщении, содержащем заражённые и подозрительные объекты; ○ управление работой программы должно осуществлять как стандартными средствами операционной системы с помощью командной строки, так и через специальный веб-интерфейс, работающий на браузерах: Internet Explorer, Mozilla Firefox, Google Chrome; ○ должна поддерживаться возможность интеграции с системами типа «песочница» для оправки файлов, полученных системой защиты веб-трафика для анализа, а также для получения результатов сканирования ○ возможность формировать отчеты за выбранный период (сутки, неделя, месяц, год) в формате PDF;

№	Группы требований	Описание
		○ обнаруживать сообщения с Юникод-спуфингом. В случае обнаружения Юникод-спуфинга считает сообщение спамом.
4	Защита для серверов Microsoft Exchange	– Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: ○ Microsoft Windows Server 2019 Standard или Datacenter (Desktop Experience) или Core. ○ Microsoft Windows Server 2019 Standard или Datacenter или Core. ○ Microsoft Windows Server 2016 Standard или Datacenter или Core. – Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать с программным обеспечением Microsoft Exchange Server следующих версий: ○ Microsoft Exchange Server 2019, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт. ○ Microsoft Exchange Server 2016, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт. ○ Microsoft Exchange Server 2013 SP1, развернутый как минимум в одной из следующих ролей: Почтовый ящик, Пограничный транспорт или Сервер клиентского доступа (CAS). – Консоль управления программными средствами антивирусной защиты для серверов Microsoft Exchange должна быть реализована с использованием Microsoft Management Console и должна функционировать на компьютерах, работающих под управлением операционных систем следующих версий: ○ Microsoft Windows 10 (x64); ○ Microsoft Windows 11 (x64); ○ Microsoft Windows Server 2019 Standard или Datacenter; ○ Microsoft Windows Server 2019 Core; ○ Microsoft Windows Server 2016 Standard или Datacenter; ○ Microsoft Windows Server 2022 Standard или Datacenter;

№	Группы требований	Описание
		– Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны обеспечивать реализацию следующих функциональных возможностей: o совместимость с DAG в Microsoft Exchange; o поиск и удаление по требованию всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения; o поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в хранящихся на сервере Microsoft Exchange (в том числе в общих папках) сообщениях, включая вложения; o наличие эвристических методов детектирования; o проверка почтовых хранилищ и общих папок на сервере, в фоновом режиме для гарантированной обработки всех объектов с использованием самой актуальной версии антивирусных баз без заметного увеличения нагрузки на сервер; o возможность лечить зараженные архивы; o возможность выявления и удаления не только однозначно вредоносных, но и потенциально опасных приложений, таких как: рекламные программы, программы-сборщики информации, программы автоматического дозвона на платные сайты и другие утилиты, которые могут использоваться злоумышленниками в своих целях; o возможность детектирования вредоносных и фишинговых ссылок в теле письма; o сохранение копий изменяемых сообщений в резервном хранилище, что позволяет восстановить важную информацию в случае некорректного лечения объекта; o набор параметров поиска для удобства нахождения объекта в резервном хранилище; o дополнительный уровень проверки с помощью репутационных облачных сервисов; o возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;

№	Группы требований	Описание
		○ наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз; ○ возможность проверять текст в сообщениях и в темах сообщений электронной почты на наличие запрещенных слов. ○ проверка различных параметров письма, таких как адреса отправителей и получателей, размер письма, а также поля заголовка сообщения; ○ защита от спуфинга (подделка адреса отправителя с целью сокрытия истинного автора сообщения электронной почты). ○ фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков; ○ проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL); ○ проверка IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF); ○ проверка с помощью сервиса SPAM URI Realtime Block lists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма; ○ использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и файлов вложений); ○ возможность использовать роли пользователей/администраторов для разграничения доступа к настройкам безопасности; ○ аудит изменения параметров программы по событиям в журнале событий Windows; ○ мониторинг состояния программы, получение статистики работы программы и управление белыми и черными списками адресов Анти-Спама с помощью команд в среде Windows PowerShell; ○ использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и имён файлов); ○ возможность фильтрации файлов Microsoft Office, содержащих макросы;

№	Группы требований	Описание
		○ возможность проверки и удаления сообщений, являющихся спамом или содержащих фишинговые и вредоносные ссылки; ○ проверка графических вложений на совпадение с известными сигнатурами спам-сообщений; ○ создание отчетов по работе системы защиты; ○ возможность автоматической рассылки отчетов администраторам по расписанию; ○ возможность обновления антивирусных баз как с сайтов производителя, так и с внутренних сетевых ресурсов организации; ○ возможность фоновой проверки почтовых ящиков и общих папок с использованием Exchange Web Services; ○ детальные отчеты в формате HTML; ○ наличие возможности отправки отчётов и уведомлений на указанные адреса электронной почты; ○ мониторинг работы программы с помощью System Center - Operations Manager; ○ интеграция с Active Directory; ○ централизованный просмотра состояния защиты; ○ возможность распределять роли администраторов системы.

4. Требования к эксплуатационной документации

Функциональные характеристики (потребительские свойства) и качественные характеристики товара
– Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна быть на русском языке, в том числе: ○ руководство пользователя (администратора) – Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства защиты.

5. Требования к внедрению

5.1. Антивирусной защиты

5.1.1. Требования к содержанию работ

5.1.1.1. Предварительный анализ инфраструктуры:

- анализ существующих антивирусных решений;
- создание и согласование требований к построению антивирусной защиты:

- текущие политики и применяемые функциональности;
- исключения из политик для отдельных ресурсов и приложений;
- описание процессов (добавление, изменение, удаление доверенных объектов);

5.1.1.2. Дизайн и написание технической документации:

- дизайн инфраструктуры решения;
- рабочие инструкции для администраторов и пользователей по эксплуатации системы;
- инструкции по аварийному восстановлению системы (APR), в том числе и в случае необходимости полного восстановления системы в инфраструктуре заказчика.
- планирование тестов по итогам внедрения;

5.1.1.3. Подготовка к развёртыванию:

- подготовка образов и выделение необходимых ресурсов;
- конфигурирование сетевых доступов;
- создание виртуальных машин;
- развёртывание и настройка центров управления;
- базовая конфигурация и активация лицензий;
- конфигурация доступа SSH и интеграция с LDAP;
- настройка процесса аутентификации и авторизации пользователей;
- конфигурация и экспорт текущих настроек решения;
- конфигурирование и тестирование компонентов защиты в соответствии с требованиями производителя;
- разработка, настройка и тюнинг правил и политик мониторинга
- тестирование решения на тестовых устройствах (сервера и рабочие станции – всего до 50 единиц);

5.1.1.4. Пилотный запуск:

- пилотная группа пользователей (до 50) и пилотная партия серверов (до 50), состав которой согласован с заказчиком на этапе планирования
- период анализа (минимум 10 рабочих дней) оповещений и полученных данных и устранения неполадок при развертывании
- передача знаний администраторам;
- оптимизация и тонкая настройка политик (исключения для приложений и файлов, обнаружение скриптов, анализ архивов и старых приложений и т.д.);

5.1.1.5. Ввод в промышленную эксплуатацию:

- подготовка методики приёмки;
- подготовка плана расширения системы на всех пользователей и сервера.
- расширения системы на группу пользователей (до 50 компьютеров) и партии серверов, состав которой согласован с заказчиком на этапе планирования (до 50 серверов)

5.1.1.6. Гарантийный период (15 рабочих дней):

- диагностика и устранение неисправностей компонентов и серверов решения;
- консультации в устранении новых проблем с пользователями, связанными с новым решением;
- консультации и помощь в решении инцидентов безопасности, связанных с эксплуатацией системы;
- консультации, разработка, оптимизация, в том числе – конфигурации, правил, настройки управления, содействие в добавлении нового функционала;
- обновление решения в рамках основного релиза (минорные обновления).
- передача знаний администраторам;

5.1.2. Минимальные проектные артефакты (могут быть в составе разных проектных документов)

- Планирование и проектные работы:
  - Частные требования к внедрению
  - График выполнения работ.
  - Списки необходимых ресурсов и трудозатрат.
  - Пояснительная записка
  - Описание настроек системы
  - Программа и методика испытаний
  - Описание правил и политик мониторинга системы, включая расписание обновлений антивирусных баз и других компонентов, периодичность проведения аудитов безопасности.
- Схемы и диаграммы:
  - Дизайн инфраструктуры решения со схемой IT-инфраструктуры.
  - Диаграмма взаимодействия компонентов системы.

- Инструкции и руководства:
  - Руководства по эксплуатации системы для пользователя и администратора.
  - Инструкции по восстановлению системы после сбоя (APR)
- Отчетность:
  - Протокол испытаний и результаты тестирования (документирование результатов тестирования продукта на соответствие требованиям безопасности и производительности).
  - Результаты тестирования (анализ эффективности работы системы в ключевых сценариях, отчет о выявленных проблемах и рекомендации по их решению)
  - Отчет о выполненных работах (краткий обзор проведенных мероприятий по внедрению и настройке системы, включая обучение администраторов заказчика и передаче знаний, оценка достижения поставленных целей и достигнутого уровня безопасности, выполненных работах)
  - Рекомендации по дальнейшему использованию системы (например, по оптимизации работы, проведению регулярных аудитов и обновлений).

5.1.3. Дополнительные работы (опционально) в пилотных группах до 50 конечных устройств

5.1.3.1. Внедрение функциональности шифрования устройств

Внедрения шифрования на базе встроенного функционала для защиты данных

- Подготовка:
  - Оценка текущего состояния системы и выявление потребностей в шифровании.
  - Определение политик и требований к шифрованию.
- Установка и настройка:
  - Установка и настройка модулей шифрования
  - Настройка политик шифрования для различных типов данных и устройств.
- Тестирование:
  - Проведение тестов на реальных данных для проверки работоспособности шифрования.
  - Оценка влияния на производительность системы.
- Ввод в эксплуатацию:

- Запуск шифрования в продуктивной среде.
- Обучение персонала и предоставление документации по использованию шифрования.

5.1.3.2. Внедрение функциональности контроля приложений

Внедрение контроля приложений на базе встроенного функционала системы для обеспечения безопасности и управления использованием приложений в компании

- Подготовка:
  - Оценка текущего состояния системы и выявление потребностей в контроле приложений.
  - Определение политик и требований к контролю приложений.
- Установка и настройка:
  - Установка и настройка модулей контроля приложений
  - Настройка политик контроля для различных типов приложений и групп пользователей.
- Тестирование:
  - Проведение тестов на реальных данных для проверки работоспособности контроля приложений.
  - Оценка влияния на производительность системы.
- Ввод в эксплуатацию:
  - Запуск контроля приложений в продуктивной среде.
  - Обучение персонала и предоставление документации по использованию контроля приложений.

5.1.3.3. Внедрение функциональности контроля веб-трафика

Внедрения контроля веб-трафика на базе встроенного функционала для обеспечения безопасности веб-трафика и управления доступом к веб-ресурсам в компании рабочих станций при подключении к интернету (например, вне офиса без корпоративного прокси-сервера)

- Подготовка:
  - Оценка текущего состояния системы и выявление потребностей в контроле веб-трафика.
  - Определение политик и требований к контролю веб-трафика.
- Установка и настройка:
  - Установка и настройка модулей системы.

- Настройка политик контроля для различных категорий веб-сайтов и групп пользователей.

- Тестирование:
  - Проведение тестов на реальных данных для проверки работоспособности функционала.
  - Оценка влияния на производительность системы.
- Ввод в эксплуатацию:
  - Запуск функционала в продуктивной среде.
  - Обучение персонала и предоставление документации по использованию.

5.2. Защита электронной почты

5.2.1. Требования к минимальному содержанию работ по внедрению

5.2.1.1. Планирование и подготовка

- Согласование проектной команды
- Согласовать цели внедрения и требования заказчика (бизнеса и IT).
- Проверка соответствия оборудования требованиям решения.

5.2.1.2. Установка и настройка

- **Подготовка и развертывание виртуальной машины**
  - Создать образ для развертывания виртуальной машины.
  - Развернуть виртуальную машину.
  - Изменить параметры виртуальной машины согласно рекомендациям производителя.
- **Первоначальная настройка системы защиты**
  - Подключиться к виртуальной машине и запустить мастер начальной настройки.
  - Установить и настроить систему.
- **Подготовка к работе**
  - Подключиться к веб-интерфейсу программы.
  - Проверить состояние защиты почтового сервера.
  - Провести все рекомендованные производителем настройки, включая интеграцию с внешними сервисами и провайдерами безопасности.
  - Выполнить процедуру приемки.

5.2.1.3. Тестирование и ввод в эксплуатацию

- **Функциональное тестирование**
  - Провести тестирование всех функциональных возможностей решения.
  - Проверить работу антивируса, спам-фильтра, фишинг-защиты и других компонентов.
- **Нагрузочное тестирование**

- Провести тестирование системы под нагрузкой для оценки производительности.
- Оптимизировать настройки для достижения оптимальных показателей.

- **Апробация и корректировка**
  - Провести пилотное внедрение на ограниченном сегменте инфраструктуры.
  - Собрать обратную связь от пользователей и внести необходимые корректировки.
- **Ввод в эксплуатацию**
  - Ввести систему в продуктивную эксплуатацию.
  - Обучить ключевых пользователей и администраторов работе с системой.

5.2.1.4. Гарантийный период, поддержка и развитие (15 рабочих дней)

- **Организация поддержки пользователей**
  - Создать базу знаний и FAQ для пользователей.
  - Назначить ответственных за техническую поддержку.
- **Регулярное обслуживание и обновление**
  - Настроить регулярное обновление антивирусных баз и других компонентов.
  - Проводить периодическую проверку и оптимизацию системы.
- **Резервное копирование и аварийное восстановление**
  - Настроить регулярное резервное копирование данных и конфигураций системы.
  - Разработать, протестировать и задокументировать план аварийного восстановления.

5.2.2. Минимальные проектные артефакты (могут быть в составе разных проектных документов)

- Планирование и проектные работы:
  - Частные требования к внедрению
  - График выполнения работ.
  - Списки необходимых ресурсов и трудозатрат.
  - Пояснительная записка
  - Описание настроек системы
  - Программа и методика испытаний
  - Описание правил и политик мониторинга системы, включая расписание обновлений антивирусных баз и других компонентов, периодичность проведения аудитов безопасности.
- Схемы и диаграммы:
  - Дизайн инфраструктуры решения со схемой IT-инфраструктуры.
  - Диаграмма взаимодействия компонентов системы.

- Инструкции и руководства:
  - Руководства по эксплуатации системы для пользователя и администратора.
  - Инструкции по восстановлению системы после сбоя (APR)
- Отчетность:
  - Протокол испытаний и результаты тестирования (документирование результатов тестирования продукта на соответствие требованиям безопасности и производительности).
  - Результаты тестирования (анализ эффективности работы системы в ключевых сценариях, отчет о выявленных проблемах и рекомендации по их решению)
  - Отчет о выполненных работах (краткий обзор проведенных мероприятий по внедрению и настройке системы, включая обучение администраторов заказчика и передаче знаний, оценка достижения поставленных целей и достигнутого уровня безопасности, выполненных работах)
  - Рекомендации по дальнейшему использованию системы (например, по оптимизации работы, проведению регулярных аудитов и обновлений).

6. Требования к технической поддержке производителя и его партнеров

.
– Поддержка должна предоставляться на русском языке специалистами, прошедшими необходимую подготовку (или сертификацию) в соответствии с требованиями производителя поставляемого программного продукта и его партнеров на всей территории Российской Федерации по электронной почте и через Интернет. – Web-сайт производителя должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке, пополняемую базу знаний, а также форум пользователей программных продуктов.