«Universal Mobile Systems»
Mas'uliyati cheklangan jamiyati

Общество с ограниченной
ответственностью
«Universal Mobile Systems»

O'zbekiston, 100000
Toshkent shahri, Amir
Temur shoh ko'chasi, 24.
Tel: (+99897) 403 83 35
Faks: (+99871) 235 81 60,
e-mail: info@mobi.uz
www.mobi.uz

УТВЕРЖДАЮ
Заместитель генерального директора по
технике и ИТ
ООО «UNIVERSAL MOBILE SYSTEMS»

_____ А.Р. Абдурахманов

«_____»_____ 2025 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на приобретение услуг по предоставлению неисключительного права (лицензии, подписка, 36 месяцев) на использование программного обеспечения средств антивирусной защиты информации для нужд ООО «UMS»
(Общество с ограниченной ответственностью «Universal Mobile Systems»)

Ташкент – 2025г.

Оглавление

1 Общие сведения 3
2. Основание для реализации проекта 3
3. Перечень работ, услуг и их объемы (количество), требуемые от Исполнителя 3
4. Место выполнения работ и оказания услуг 4
5. Назначение ПО и требования к нему 4
6. Требование к участнику 19
7. Требования к безопасности выполнения работ и оказания услуг 19
8. Требования по передаче технических и иных документов по результатам выполненных работ и оказанных услуг 19
9. Требования к обучению персонала Заказчика 20
10. Требования к сроку оказания услуг и объему гарантий 20
11. Условия сервисной поддержки 20
12. Иные требования к работам, услугам и условиям их оказания 21
13. Используемые термины и сокращения 23
14. Перечень приложений 23

1 Общие сведения

В настоящем Техническом задании описаны требования к модернизации существующего антивирусного ПО на ИТ-инфраструктуре ООО «UMS» (далее - ИС, ПО), достаточные для однозначного и точного описания требований Заказчика к внедряемому ПО с целью объявления закупочной процедуры на приобретение программного обеспечения и обучения.

1.1 Наименование оказываемых услуг

1.1.1. Приобретение на условиях простой (неисключительной) лицензии прав пользования программного обеспечения средств антивирусной защиты информации, для антивирусной защиты компьютеров ООО «UMS» (далее – ПО) с правом доступа к технической поддержке (далее - ТП), уровень поддержки - расширенная, на 36 (тридцать шесть) календарных месяцев для нужд ООО «UMS» (далее – Заказчик).

1.1.2. Предоставляемые неисключительные права (лицензии) на использование ПО включает в себя право на воспроизведение, ограниченное правом инсталляции, копирования и запуска, предоставляемое с единственной целью передачи этого права конечным пользователям.

1.1.3. Срок действия неисключительных прав (период использования, на который передаются неисключительные права) – 36 месяцев.

1.1.4. Неисключительные права передаются для использования на территории Республики Узбекистан.

Основной целью оказания услуг является обеспечение средств надежной, современной, непрерывно обновляемой Антивирусной защиты рабочих станций сотрудников компании, а также серверных мощностей на ИТ-инфраструктуре, обеспечение требований к средствам обеспечения информационной безопасности, централизованное обеспечение пользователей заказчика правами пользования ПО антивирусной защиты, выполнение производственных задач по сохранению процесса непрерывного функционирования, стабильной работы инфокоммуникативной инфраструктуры, сокращение издержек, связанных с отказами оборудования и информационных систем Заказчика.

Достижение вышеуказанных целей проекта предполагает, что внедрение ПО на инфраструктуре ООО «UMS», повысит ИТ-безопасность Компании.

2. Основание для реализации проекта

Запланированный на 2025г. план развития ИТ (Утвержденный Бизнес план и Бюджет ООО «UMS» на 2025 год).

3. Перечень работ, услуг и их объемы (количество), требуемые от Исполнителя

В рамках проекта Исполнителем должны быть выполнены следующие работы и услуги:

- передача неисключительного права на использование антивирусного программного обеспечения;
- технические консультации Заказчика;
- обучение персонала Заказчика.

Все работы на инфраструктуре Заказчика могут проводиться удаленно, с использованием VPN подключения.

Предоставление прав пользования ПО антивирусные защиты осуществляется в объемах, указанных в п.5.5.3. данного Технического задания, путем цифровой дистрибуции на

электронный адрес, а именно передача Заказчику ключей посредством электронной почты либо путем предоставления доступа для скачивания установочных файлов и лицензионных ключей с ресурса (сайта) в сети «Интернет

3.1. Инсталляционные работы

Данный этап проводится силами специалистов Заказчика, Исполнитель оказывает технические консультации, на этапе ввода ПО в эксплуатацию, и включает в себя следующие работы:

- активация лицензий на ПО;
- настройка резервирования ПО;
- интеграция ПО с Active Directory для аутентификации пользователей (в случае необходимости);
- настройка конфигураций и политик доступа к ПО;
- постановка установленного ПО на мониторинг. Настройка отправки сообщений о возникновении аварийных ситуаций по протоколу SNMP, в систему мониторинга Заказчика (Zabbix).

3.2. Обучение персонала Заказчика.

В рамках проекта, Исполнитель обеспечивает обучение сотрудников Заказчика в соответствии с п.9.

4. Место выполнения работ и оказания услуг

Исполнитель должен обеспечить поставку ПО по следующему адресу: Республика Узбекистан, г. Ташкент, 100000, проспект Амира Темура, 24, Центральный офис ООО «UMS».

5. Назначение ПО и требования к нему

Назначение ПО заключается в обнаружении, блокировке и удалении вирусов, и вредоносных программ, а также для защиты корпоративных пользователей и серверного оборудования от других киберугроз.

5.1. Требования в целом

ПО и все ее элементы должны быть развернуты в контуре Заказчика, на виртуальных ресурсах Заказчика.

До реализации проекта Исполнитель должен предоставить информацию по:

- требованиям к аппаратной части для развертывания ПО предлагаемого решения;
- требования к платформе виртуализации;
- системные требования для полноценного функционирования программного комплекса (операционная система, системное ПО, ПО СУБД и т.п.);
- требования к сетевой инфраструктуре Заказчика.

После согласования всех требований, Исполнитель готовит предварительную архитектуру предлагаемого решения и варианты его интеграции в инфраструктуру Заказчика.

5.2. Функциональные требования

К ПО предъявляются следующие функциональные требования:

5.2.1. Требования к программным средствам антивирусной защиты для рабочих станций Windows

Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий:

- Windows 8 Professional / Enterprise (32 / 64-разрядная);
- Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
- Windows 10 Professional / Enterprise;
- Windows 11 Professional / Enterprise.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

- антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристический анализ, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализация действий активного заражения;
- анализ поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
- анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
- ограничение 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;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- защита электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
- фильтр почтовых вложений с возможностью переименования или удаления заданных типов файлов;
- проверка сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
- блокировка баннеров и всплывающих окон на загружаемых Web-страницах;
- распознавание и блокировка фишинговых и небезопасных сайтов;
- встроенный сетевой экран, позволяющий создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- защита от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;

- защита от сетевых угроз, которые используют уязвимости в ARP-протоколе для подмены MAC-адреса устройства;
- контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
- создание специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп);
- контроль работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
- управление MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
- запись в журнал событий о записи и/или удалении файлов на съемных дисках;
- назначение приоритета для правил доступа к устройствам с файловой системой;
- контроль работы пользователя с сетью Интернет;
- защита от атак типа BadUSB;
- защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
- запуск задач по расписанию и/или сразу после запуска приложения;
- гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- проверка целостности антивирусной программы;
- добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
- импорт и экспорт списков правил и исключений в XML-формат;
- наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
- наличие защищенного хранилища для отчетов о работе антивируса;
- включение и выключение графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
- интеграция с Windows Defender Security Center;
- наличие поддержки Antimalware Scan Interface (AMSI);
- наличие поддержки Windows Subsystem for Linux (WSL);
- защита паролем восстановления объектов из резервного хранилища;
- наличие инструмента мониторинга сети по протоколам TCP и UDP;
- возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
- установка ограничения длительности выполнения задачи проверки;
- постановка задачи на проверку в очередь, если проверка уже выполняется;
- 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;

- обновление без перезагрузки системы;
- настройка прав доступа (чтение / запись) для портативных устройств (MTP);
- настройка доступ пользователей к мобильным устройствам в приложении Android Debug Bridge (ADB);
- настроить доступ пользователей к мобильным устройствам в приложении iTunes;
- настройка прав печати для пользователей;
- наличие поддержки протокола WPA3 для контроля подключения к сетям WiFi;
- запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем;
- восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем;
- поддержка двухфакторной аутентификации при полнодисковом шифровании;
- шифрование данных на съемных носителях;
- возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий)
- возможность создавать служебную учетную запись агента аутентификации при шифровании диска;
- возможность настроить исключения и ограничить доступ ко всем Bluetooth-устройствам кроме устройств ввода;
- возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО;
- возможность запретить внешнее управление службами приложения.

5.2.2. Требования к программным средствам антивирусной защиты для серверов Windows

Программные средства антивирусной защиты должны функционировать на серверах, работающих под управлением операционной системы Windows следующих версий:

- Windows Server 2008 R2 Standard / Enterprise / Datacenter Service Pack 1 и выше;
- Windows Server 2012 Standard / Datacenter;
- Windows Server 2012 R2 Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022 Standard / Datacenter / Datacenter.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

- антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристический анализ, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
- функционал нейтрализации действий активного заражения;
- анализ поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;

- анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- встроенный сетевой экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- защита от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
- защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
- возможность установки только выбранных компонентов программного средства антивирусной защиты;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- проверки целостности антивирусной программы;
- добавление исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
- наличие защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
- наличие защищенного хранилища для отчетов о работе антивируса;
- функционал включение и выключение графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
- интеграция с Windows Defender Security Center;
- наличие поддержки Antimalware Scan Interface (AMSI);
- наличие поддержки Windows Subsystem for Linux (WSL);
- функционал защиты паролем восстановление объектов из резервного хранилища.
- функционал импорта и экспорта списков правил и исключений в XML-формат;
- ограничение сетевого трафика в том случае, если подключение к интернету является лимитным;
- создание специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или

локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;

- формирование шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);
- запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
- поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов.
- возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
- возможность установки ограничения длительности выполнения задачи;
- возможность ставить задачи проверки в очередь, если проверка уже выполняется;
- обновление без перезагрузки системы;
- настройка прав доступа (чтение / запись) для портативных устройств (MTP), выбирать пользователей или группу пользователей, которые имеют доступ к устройствам, а также задавать расписание доступа к устройствам;
- наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi;
- возможность обновления приложения без перезагрузки операционной системы;
- возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО;
- возможность запретить внешнее управление службами приложения;
- возможность использования предустановленных исключений из проверки и доверенных приложений, предназначенных для быстрой настройки доверенной зоны для работы приложения на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager.

5.2.3. Требования к программным средствам антивирусной защиты для серверов Linux

Программные средства антивирусной защиты для серверов Linux должны функционировать на устройствах, работающих под управлением 64-битных операционных систем следующих версий:

- CentOS 7.2 и выше
- CentOS Stream 8 и выше
- Oracle Linux 7.3 и выше.
- Red Hat Enterprise Linux 7.2 и выше.
- SUSE Linux Enterprise Server 12.5 и выше.
- Ubuntu 20.04 LTS и выше

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

- резидентного антивирусного мониторинга;
- облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

- проверку ресурсов доступных по SMB / NFS;
- возможность проверки памяти ядра;
- эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
- проверку сообщений электронной почты в текстовом формате (Plain text);
- наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
- защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
- включения опции блокирования файлов во время проверки;
- помещение подозрительных и поврежденных объектов на карантин;
- перехвата и проверки файловых операций на уровне SAMBA;
- управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- экспортировать и сохранять отчеты в форматах HTML и CSV;
- гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
- сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
- управления через пользовательский графический интерфейс без root прав;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;
- управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;
- проверки съемных дисков;
- отслеживания во входящем сетевом трафике активности, характерной для сетевых атак;
- проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым
- получения данных о действиях программ на компьютере пользователя;
- получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация);
- создание файлов трассировки при запуске программы;
- получение информации обо всех исполняемых файлах программ, установленных на компьютерах;
- проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;

- сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий;
- исключения процессов из проверки памяти процессов в общих параметрах программы;
- оптимизировать проверку журналов работы программ с помощью параметра SkipPlainTextFiles;
- исключения трафика из проверки программой;
- использовать формат JSON для запросов и вывода информации, а также для экспорта и импорта параметров программы и параметров задач;
- установки и работы на устройствах с операционными системами для архитектуры Arm;
- работать в режиме информирования пользователя в случае обнаружения угроз или при обнаружении попытки доступа к устройству;
- возможность управлять запуском приложений на защищаемых устройствах с помощью правил контроля в режимах списка запрещенных или разрешенных приложений;
- автоматический перезапуск приложения при обновлении;
- возможность задать ограничение на использование ресурсов процессора;
- возможность в автоматическом режиме выключить компоненты защиты и задачи проверки при запуске приложения после установки;
- уведомления пользователя о работе компонентов и задач в графическом пользовательском интерфейсе;
- возможность читать память процессов, не останавливая их (ядра Linux начиная с версии 3.4);
- возможность управлять доступом пользователей к веб-ресурсам;
- функция мониторинга стабильности собственной работы приложения.

5.2.4. Требования к программным средствам антивирусной защиты файловых серверов, терминальных серверов Windows

Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: 32/64-разрядных операционных систем Microsoft Windows

- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Hyper-V Server;
- Windows Server 2022;

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

- антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;

- защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
- непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
- анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- проверки контейнеров Microsoft Windows;
- защиты от эксплуатирования уязвимостей в памяти процессов;
- должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
- добавлять процессы в список защищаемых;
- ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
- настройки проверки критических областей сервера в качестве отдельной задачи;
- регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;
- продолжать антивирусное сканирование в фоновом режиме;
- наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
- ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
- интеграции с SIEM системами;
- указания количества рабочих процессов антивируса вручную;
- отключить графический интерфейс;
- наличие удаленной и локальной консоли управления;
- управления параметрами антивируса из командной строки;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
- управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
- защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;
- включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов.
- контроль устройств, в том числе сетевых карт и модемов;
- веб-контроль;
- защита от почтовых угроз (плагин для Outlook);

- защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления;
- создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп);
- создания специальных правил должно контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме;
- создания специальных правил должно работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должно иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
- осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
- осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем;
- информирование администратора о подключении внешних устройств;
- наличие механизмов автоматической генерации правил для контроля устройств и приложений.

5.2.5. Требования к программным средствам антивирусной защиты и фильтрации спама 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 2022 Standard или Datacenter;
- Microsoft Windows Server 2019 Standard или Datacenter;
- Microsoft Windows Server 2016 Standard или Datacenter.

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 и серверах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2022 Standard или Datacenter;
- Microsoft Windows Server 2019 Standard или Datacenter;

- Microsoft Windows Server 2016 Standard или Datacenter;
- Операционные системы Microsoft Windows Server в режиме Core.
- Microsoft Windows 11 (x64);
- Microsoft Windows 10 (x64).

Для установки любого компонента программы (Сервера безопасности или Консоли управления) требуется пакет обновлений Microsoft Windows KB2999226.

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны обеспечивать реализацию следующих функциональных возможностей:

- совместимость с DAG в Microsoft Exchange;
- поиск и удаление по требованию всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
- 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;
- наличие эвристических методов детектирования;
- 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;
- возможность лечить зараженные архивы;
- 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;
- возможность детектирования вредоносных и фишинговых ссылок в теле письма;
- сохранение копий изменяемых сообщений в резервном хранилище, что позволяет восстановить важную информацию в случае некорректного лечения объекта;
- набор параметров поиска для удобства нахождения объекта в резервном хранилище;
- дополнительный уровень проверки с помощью 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;
- 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;
- 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 ПО.

5.3. Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

- создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток;
- множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;
- проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

5.4. Требования к эксплуатационной документации

Эксплуатационная документация ПО антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

- «Руководство пользователя (администратора)»

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

5.5. Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

- Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его по электронной почте и через Интернет.
- Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.

5.5.1. Требования к структуре и функционированию ПО

Предлагаемое ПО должно соответствовать следующим требованиям к структуре и функционированию:

- Функционировать круглосуточно в автоматическом режиме (с перерывами на регламентное техническое обслуживание).

Программное обеспечение должно обеспечивать функционирование в следующих режимах:

- штатный режим эксплуатации;
- режим обновление, создание резервной копии, архивирование;
- режим модернизации (внедрение нового функционала, интеграция со смежными системами, активация дополнительных лицензий);
- регламентное техническое обслуживание, восстановление после сбоев в работе технических, программных средств, а также при возникновении нештатных ситуаций.

Конкретный состав и содержание функций, исполняемых в каждом режиме, определяются на этапах технического и рабочего проектирования.

5.5.2. Требования к ПО в части лицензирования

Исполнитель должен предоставить Заказчику информацию по политике лицензирования ПО, в том числе тип сервисной поддержки (подписка, непрерывность сервиса, наличие штрафных санкций при несвоевременном продлении поддержки, и т.д.);

- ПО должно быть поставлено Заказчику по модели подписки;
- ПО должно иметь возможность масштабирования путем активации дополнительных лицензий и добавления дополнительных вычислительных мощностей.

5.5.3. Показатели назначения

ПО должно быть рассчитано не менее, чем на 2000 устройств (рабочих станций + серверных устройств).

5.5.4. Требования к надежности

Все компоненты решения должны быть зарезервированы в режиме Active-Active или Active-Standby.

ПО должно сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

- при сбоях в аппаратной или программной части, приводящих к перезагрузке операционной системы, восстановление ПО должно происходить после перезагрузки серверных ресурсов;
- при ошибках, связанных с программным обеспечением рабочей станции администратора ПО, восстановление работоспособности возлагается на операционную систему;

- ПО, после проведения работ по настоящему Техническому заданию, должна быть устойчива по отношению к программно-аппаратным ошибкам, с возможностью восстановления ее работоспособности и целостности информационного содержимого.

5.5.5. Требования к безопасности

ПО должно соответствовать общим требованиям безопасности программных средств.

Принципы построения решения должны отвечать современным мировым стандартам по степени защищенности и сохранности информации и включать:

- протоколирование и аудит, регистрация всех событий и действий пользователей;
- ограничение доступа пользователя к объектам ИС на основе идентификации пользователя в том числе по его роли;
- гибкое управление правами доступа, предоставление возможности Администратору вести учетные записи пользователей.

При работе с ПО, безопасность должна быть обеспечена за счет аутентификации, идентификации и ролевых прав пользователей.

При работе ПО на уровне бэкенда должно реализовываться журналирование каждого сеанса пользователя с указанием времени входа в систему.

Автоматическое ведение журнала аудита должно также предоставлять возможность мониторинга наиболее критичных (уникальных) данных, хранящихся в БД и регистрации всех происходящих событий и изменений любых данных в системе в соответствии с настройкой системы.

Журнал аудита должен создаваться автоматически и вестись постоянно. Каждая операция в журнале аудита должна идентифицироваться по пользователю, дате и времени.

5.5.6. Требования к защите информации от несанкционированного доступа

ПО должно соответствовать всем установленным требованиям в действующей нормативной документации Заказчика по защите информации от несанкционированного доступа.

ПО должно реализовывать механизм безопасности и защиты информации на основе следующих основных принципов:

- ограничение доступа к системе на основе идентификации пользователя;
- ограничение доступа к объектам системы в зависимости от разграничения прав доступа для сотрудников Контакт-центра (оператор, супервайзер, руководитель) и администраторов системы;
- ведение журнала аудита для выявления неавторизованных изменений в системе.

5.5.7. Требования по сохранности информации при авариях

При авариях ПО должно обладать возможностью полного восстановления данных за счет резервных копий конфигураций. Резервное копирование настроек и конфигураций ПО – зона ответственности Заказчика.

Информационная безопасность должна соответствовать требованиям, установленным в действующих редакциях стандартов: O‘z DSt ISO/IEC 13335-1, O‘z DSt 1SO/IEC 15408-1, O‘z DSt ISO/IEC 15408-2, O‘z DSt ISO/IEC 15408-3, O‘z DSt ISO/IEC 27001, O‘z DSt ISO/IEC 27002, O‘z DSt 2814.

Информация, отображаемая в ПО, не должна терять свое качество (актуальность, полноту, достоверность), разрушаться, повреждаться, искажаться и теряться при возникновении любых аварийных ситуаций: отказа технических средств, потери питания в электросети и т.п.

5.5.8. Требования к эргономике и технической эстетике

ПО должно обеспечивать удобные для пользователей интерфейсы, отвечающие следующим требованиям:

- интерфейс удобный и интуитивно понятный для пользователя, который хорошо знает свою предметную область и не является специалистом в области информационных технологий;
- графический дизайн пользовательских интерфейсов, цветовые, шрифтовые и композиционные решения для отображения текстов, изображений, таблиц, гиперссылок, управляющих и навигационных элементов (меню, кнопок, форм и т.п.), поля для заполнения должны иметь примечания о данных, которые требуется ввести;
- качественное взаимодействие пользователя (человека) с системой;
- детали пользовательского интерфейса системы должен быть адаптивным под разрешения большинства экранов.

5.6. Требования к видам обеспечения

5.6.1. Квалифицированные требования

- наличие необходимого количества квалифицированного персонала;
- Исполнитель должен иметь успешно реализованные аналогичные проекты.

5.6.2. Требования к математическому обеспечению

Требования не предъявляются.

5.6.3. Требования к информационному обеспечению

ПО должно поддерживать создание резервной копии конфигурации встроенными средствами.

5.6.4. Требования к лингвистическому обеспечению

Все функции ПО должны обеспечивать русскоязычный интерфейс пользователя.

5.6.5. Требования к программному обеспечению

Прикладное программное обеспечение должно отвечать следующим требованиям:

- высокая степень готовности для решения поставленных задач;
- совместимость программных продуктов в части используемых технических средств, системного ПО и общесистемной инфраструктуры Заказчика в пределах требований к техническому обеспечению.

Доступ к информации должен осуществляться своевременно, представляться в виде таблиц, отчетов, форм, соответствующих главных и контекстных меню. Данные должны передаваться по сети без ущерба для функционирования сетевой инфраструктуры Заказчика.

ПО должно поставляться с комплектами лицензий, согласно политики лицензирования производителя Системы, и иметь наиболее позднюю по времени выпуска версию производителя.

ПО Системы должно обладать следующими характеристиками:

- обеспечивать устойчивость к ошибочным ситуациям, в том числе при неверных и противоречивых данных;
- сбои в работе программ, отказы части вычислительных средств, ошибки персонала должны диагностироваться, сопровождаться сообщениями, и не должны вызывать нарушений в работе системы;
- обеспечивать автоматический перезапуск при восстановлении электрического питания после его отключения без выдачи ложных сигналов и управляющих воздействий;
- иметь возможность оперативного конфигурирования в процессе функционирования ПО.

5.6.6. Требования к техническому обеспечению

ПО должно разворачиваться на виртуальных серверах под управлением VMware Заказчика.

5.6.7. Требования к организационному обеспечению

Организационное обеспечение ИС должно быть достаточным для эффективного выполнения персоналом возложенных на него обязанностей при осуществлении автоматизированных и связанных с ними неавтоматизированных функций системы.

К работе с ИС должны допускаться работники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации, техники безопасности и прошедшие обучение работе с ИС.

Необходимы обязательные инструктажи пользователей, перед началом работы с Системой.

Дополнительных требований к организационному обеспечению не предусматривается.

5.6.8. Требования к методическому обеспечению

Требования не предъявляются.

6. Требование к участнику

К квалификации Исполнителя предъявляются следующие требования:

1) Исполнитель должен предоставить авторизационное письмо (MAF) от производителя ПО подтверждающее правомочность Исполнителя на передачу ПО (лицензий) проведение технических консультаций и гарантийную поддержку.

2) Лицензионный Сертификат, в котором указан номер неисключительных прав (лицензий) на пользование ПО.

3) Для оказания услуг требуется квалифицированный персонал, в количестве не менее 2 человек, прошедших обучение, и имеющих соответствующие сертификаты.

4) Исполнитель должен соответствовать следующим критериям:

- наличие необходимых технических, финансовых, материальных, кадровых и других ресурсов для исполнения договора;
- правомочность на заключение договора;
- отсутствие задолженности по уплате налогов и других обязательных платежей;
- отсутствие введенных в отношении них процедур банкротства, отсутствие записи о них в Едином реестре недобросовестных исполнителей.

7. Требования к безопасности выполнения работ и оказания услуг

Требований к безопасности выполнения работ не предъявляется.

8. Требования по передаче технических и иных документов по результатам выполненных работ и оказанных услуг

На основе требований, изложенных в настоящем документе, Исполнитель должен подготовить технико-коммерческое предложение, описывающее предлагаемое им решение. С целью экономической оценки эффективности проекта, корректного и полного расчета стоимости владения Участник должен предоставить следующие документы:

- стоимость покупки лицензий/подписки;
- эксплуатационную документацию на русском языке

Технико-коммерческое предложение должно включать:

- описание ПО (лицензий) и услуг;
- описание технической поддержки;
- программу и условия обучения персонала Заказчика.

9. Требования к обучению персонала Заказчика

В рамках проекта, Исполнитель обеспечивает следующие учебные программы от правообладателя:

a) Обучение двух специалистов Заказчика, сертифицированными специалистами производителя по программе системное администрирование ПО и компонентов, входящих в ее состав. Факт прохождения обучения должен быть подтвержден соответствующим сертификатом. Программу обучения предварительно согласовать с Заказчиком.

b) Обучение двух специалистов Заказчика, специфическим настройкам клиентского ПО. Программу обучения предварительно согласовать с Заказчиком.

10. Требования к сроку оказания услуг и объему гарантий

10.1 Срок предоставления неисключительных прав (лицензий) на использование ПО предоставляется в течении 10 (десять) рабочих дней со дня получения Исполнителем от Заказчика авансового платежа.

10.2 Срок предоставления технических консультаций по инсталляции и эксплуатации: 36 (тридцать шесть) календарных месяца, с даты подписания Акта приема-передачи предоставления неисключительных прав (лицензий) на использование ПО

10.3 Гарантийные обязательства, принимаемые Исполнителем, включают следующее:

10.3.1 Исполнитель должен гарантировать, что качество выполненной работы будет соответствовать техническому заданию и требованиям указанным Заказчиком, при условии соблюдения правил эксплуатации программного комплекса, установленных производителем в документации и отсутствия несанкционированного вмешательства в работу инсталлированного программного обеспечения.

10.3.2. Исполнитель должен обеспечить Заказчика всей информацией и документацией, необходимой для оказания услуг по сервисной поддержке.

10.3.3 Гарантийная, сервисная поддержка должна составлять **36 (тридцать шесть) месяцев**, с даты подписания Акта. В состав поддержки входят: гарантийная и техническая поддержка от правообладателя/ Вендора (включая апгрейды на новые версии ПО), техническая поддержка от Поставщика, направленная на поддержание работоспособности, конфигурацию ПО, либо, в случае возникновения отказов, восстановление работоспособности ПО.

11. Условия сервисной поддержки

Перечень услуг по сервисной поддержке, оказываемой Исполнителем, включает следующее:

11.3. Консультирование по вопросам работоспособности ПО – бесплатное, неограниченное, на протяжении всего срока действующей сервисной поддержки.

11.4. Исполнитель должен предоставить возможность открытия заявок следующими способами:

- по телефону на территории Узбекистана;
- по электронной почте.

11.5. Специалисты технической поддержки обрабатывают заявки от Заказчика в рабочие

дни с 09:00 до 18:00 (UTC+5) в соответствии с законодательством Республики Узбекистан

11.6. Исполнитель должен обеспечить время реагирования и осуществлять сервисную поддержку с классификацией инцидентов, не менее, чем по четырём приоритетам, в соответствии с нижеследующей таблицей:

Приоритет	Описание	Время реакции
Критический	Проблемы, приводящие к полной неработоспособности системы или критически влияющие на бизнес-процессы Клиента.	**до 2 рабочих часов**
Высокий	Значительное влияние на работу системы или бизнес Клиента.	**до 4 рабочих часов**
Средний	Проблемы, возникающие в специфических условиях эксплуатации, не оказывающие значительного влияния на бизнес Клиента.	**до 8 рабочих часов**
Низкий	Вопросы информационного характера или незначительные сбои, не влияющие на эксплуатацию системы.	**до 2 рабочих дней**

Обозначения:
РЧ – рабочие часы
РД – рабочий день
КД – календарный день

- **Режим обслуживания** – расписание работы технической поддержки Исполнителя, в течение которого они выполняют запрошенное Заказчиком техническое обслуживание.
- **Время реакции** – максимальный период времени с момента уведомления о возникшей проблеме Заказчиком, технической поддержки Исполнителя, в течение которого инженеры Исполнителя должны приступить к процедуре выявления неисправности.
- **Время восстановления** – промежуток времени с момента уведомления о возникшей проблеме Заказчиком технической поддержки Исполнителя, до момента восстановления полноценного функционирования Системы, или поиска обходного решения, позволяющего снизить влияние возникшей проблемы на системы Заказчика.
- **Время решения -** означает промежуток времени с момента уведомления Заказчиком технической поддержки Исполнителя, до момента предоставления Заказчику решения по устранению проблемы**.**

12. Иные требования к работам, услугам и условиям их оказания

Лицензии/ПО считаются принятым после проведения физической инвентаризации и работоспособности программного обеспечения в присутствии представителей сторон и соответствующего подписания Акта приема-передачи согласно заключенного договора. Другие условия, не указанные в данном ТЗ и его приложениях, будут указаны в контракте.

Обязательным условием оказания услуг является соблюдение правил действующего внутреннего распорядка Заказчика, контрольно-пропускного режима, внутренних положений, инструкций и требований, о которых Заказчик уведомит Исполнителя. Заказчик предоставляет Исполнителю список и контактные данные персонала, уполномоченного им на контакты с Исполнителем по решению заявленных проблем, связанных с активацией подписки на ПО.

Детальная форма подачи предложения представлена в закупочной документации.

12.3. Требование к комплектации

ПО должно иметь полную комплектацию, в которую входит весь заказываемый функциональный перечень, необходимых для полноценного функционирования предлагаемого решения в рамках текущего ТЗ. Стоимость ПО должна формироваться исходя из полной комплектации.

12.4. Сведения о новизне

Поставляемое ПО должна быть актуальной последней версии со всеми необходимыми лицензиями на продукт и его составляющими.

12.5. Страхование

Требования не предъявляются, однако Исполнитель несет ответственность сохранности программного обеспечения.

12.6. Матрица распределения ответственности при оказании услуг передаче неисключительных прав на ПО

№	Действие	Исполнитель	Заказчик
1	Предоставление предложения	О	У
2	Регистрация лицензий в персональном кабинете Заказчика учётной записи Правообладателя	О	У
3	Окончательная приёмка	И	О

Условные обозначения матрицы ответственности:

"О" Ответственный	Лежит ответственность за выполнение поставленной задачи. На каждую задачу должно приходиться не менее одного Исполнителя. Степень ответственности распределяется Утверждающим
"У" Утверждающий	Перед ним производится отчет в полученном результате, имеются полномочия, как принимать, так и отвергать предложения, накладывать на них вето. На каждый проект выделяется не более одного Утверждающего
"И" Информируемый	Поступает конечная информация о проделанной работе. Характеризуется односторонней связью

12.7. Матрица распределения ответственности при оказании услуг ТП

Техническое обслуживание/поддержка	**Исполнитель**	**Заказчик**
Доступность системы		
Обнаружение и классификация приоритетности проблемы, открытие запроса для решения у Правообладателя	A	R
Производить настройку ПО по запросу Заказчика	A	R
Регистрировать все запросы на портале Правообладателя	R	A
Обновления, исправления, корректировки программного обеспечения		
Определить время установки	A	R
Установить Программное обеспечения	R	A
Проверить работу установленного программного обеспечения	A	R
Сервисы и рекомендации		
Предоставить технические рекомендации	R	I

R (от англ. Responsible) – непосредственный исполнитель;

A (от англ. Accountable) – ответственное лицо, которое руководит работой исполнителя;
C (от англ. Consulted) – консультант (специалист либо эксперт в предметной области, к чьей помощи прибегает ответственное лицо до принятия конкретных решений);
I (от англ. Informed) – наблюдатель, информируемое лицо (лицо, которое надлежит уведомлять о ходе (либо результатах) выполнения задачи)

13. Используемые термины и сокращения

Сокращение	Расшифровка сокращения
ТЗ	Техническое задание
ПО	Программное обеспечение
ИС	Информационная система
ИТ	Информационные технологии
KPI	Key Performance Indicator, количественно измеримый индикатор эффективности определенной деятельности, а также уровень достижения поставленных целей (результатов)
АРМ пользователя	Автоматизированное рабочее место пользователя.
Service Level (SLA, уровень сервиса)	Одна из ключевых характеристик работы контакт-центра, процент вызовов, которые операторы успели принять за интервал времени, заданный менеджером контакт-центра. У этого показателя есть два компонента процентный и временной.
СУБД	Системы управления базами СУБД данных
REST	Архитектурный стиль взаимодействия компонентов распределённого приложения в сети
API	Описание способов, которыми одна компьютерная программа может взаимодействовать с другой программой
SOAP	Протокол обмена структурированными сообщениями в распределённой вычислительной среде
ТП	Техническая поддержка

14. Перечень приложений

Перечень приложений не предъявляется.

Ответственный исполнитель:
И.о. Начальника отдела эксплуатации _____Н.Ф. Садыков
ИТ-инфраструктуры ДИТ ТБ

Согласовано:

Директор по ИТ ДИТ ТБ _____ У.А. Мавлянов

Ведущий специалист ДИТ ТБ _____ Е.А. Яцкевич

Начальник отдела ИБ ДИБР _____ Р.А. Абдульваат