



«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

Директор Департамента по информационной
безопасности и режиму ООО «UMS»



Олматов Б.А.

« 09 » июль 2025г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

**на поставку, установку, запуск в коммерческую эксплуатацию системы защиты
электронной почты со встроенной фильтрацией SPAM-сообщений
для нужд ООО «UNIVERSAL MOBILE SYSTEMS»**

Ташкент – 2025

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	5
5	Технические требования к Системе	5
6	Требования к Исполнителю	8
7	Требования к безопасности выполнения работ и оказания услуг	9
8	Требования по передаче технических и иных документов по результатам выполненных работ и оказанных услуг	9
9	Требования к обучению персонала Заказчика	9
10	Гарантийные обязательства	10
11	Условия сервисной поддержки и техническое сопровождение	10
12	Иные требования к работам, услугам и условиям их оказания	11
13	Используемые термины и сокращения	12
14	Перечень приложений	12

1 Общие сведения

В настоящем Техническом задании описаны требования к Системе защиты электронной почты со встроенной фильтрацией SPAM-сообщений (далее - Система, ИС), достаточные для описания требований Заказчика к составу ПО, с целью объявления тендера и/или конкурса на приобретение программного обеспечения и услуг для реализации проекта в целом на условиях «под ключ».

Характеристика объекта информатизации представлена в Приложении №1.

1.1 Наименование выполняемых работ и оказываемых услуг

Полное наименование проекта: Система защиты электронной почты со встроенной фильтрацией SPAM-сообщений (далее по тексту – Система).

Работы проводятся на инфраструктуре и площадке Заказчика с использованием действующего оборудования.

В рамках данного Технического задания Исполнитель должен предоставить коммерческое предложение на поставку, установку, внедрение и запуск в коммерческую эксплуатацию программного или программно-аппаратного комплекса Системы защиты электронной почты со встроенной фильтрацией SPAM-сообщений.

1.2 Цели использования выполняемых работ и оказываемых услуг

Основная цель проекта – это внедрение на инфраструктуре ООО «UMS» инструмента (программного обеспечения) обнаружения и защиты от угроз и спама корпоративной почты.

Основные задачи, решаемые Системой:

- защита почтовых ящиков от спама, фишинговых атак и вредоносного ПО;
- обеспечение безопасности передачи данных;
- контроль и анализ почтового трафика;
- обеспечение внутренних политик безопасности и регламентов.

Основное назначение Системы – это защита корпоративной почты сотрудников компании ООО «UMS», от угроз, распространяемых как из вне компании, так и внутри.

2 Основание для реализации проекта

Запланированный на 2025г. план развития Департамента Безопасности и Режимов (Решение Наблюдательного совета, утвержденный Бизнес план и Бюджет ООО «UMS» на 2025 год).

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

Внедрение Система защиты электронной почты должно проводиться совместно с ответственными лицами Заказчика, без нарушения работоспособности существующей ИТ-инфраструктуры Заказчика, с предварительным поверхностным обследованием имеющихся рабочих станций и установленных на них операционных систем. Все работы, требующие остановку каких-либо корпоративных систем должны быть предварительно согласованы с Заказчиком.

В рамках проекта Исполнителем должны быть выполнены следующие этапы работ:

- подготовительный этап;
- пуско-наладочные и интеграционные работы;
- обучение персонала Заказчика.

3.1 Подготовительный этап

Включает в себя взаимодействие с ответственным за Проект персоналом Заказчика и совместное обследование ИТ инфраструктуры Заказчика. На данном этапе сотрудники должны определить:

- наиболее важные детали топологии сети Заказчика;
- анализ виртуальной ИТ-инфраструктуры Заказчика, необходимый объем системных ресурсов для серверной части Системы (количество ОЗУ, количество ядер ЦП и их частота, объем жесткого диска)
- зоны ответственности Заказчика и Исполнителя в ходе развёртывания Системы;
- количество рабочих станций, которые будет защищать Система.

3.2 Пуско-наладочные и интеграционные работы

Во взаимодействии с ответственным за Проект персоналом Заказчика пуско-наладочные работы включают в себя:

- установку и конфигурацию Системы;
- активацию модулей необходимых для мониторинга;
- активацию необходимых лицензий.

В случае обнаружения сбоев в работе Системы по причине ошибок, не связанных с объектами ИТ инфраструктуры Заказчика, Исполнитель обязуется внести коррективы в функционал продукта до подписания акта о выполненных работах.

3.3 Порядок контроля и приемка Системы

Приемка Системы должна производиться путем проведения приемочных испытаний. Приемочные испытания осуществляются приемочной комиссией, в которую входят уполномоченные представители Заказчика и Исполнителя.

Цель приемочных испытаний состоит в подтверждении работоспособности компонентов Системы и соответствии их требованиям ТЗ.

Виды, состав, объем и методы испытаний должны определяться программой приемочных испытаний. Программа приемочных испытаний разрабатывается Исполнителем и согласовывается Заказчиком не позднее, чем за 1 день перед началом испытаний.

Результаты приемочных испытаний должны оформляться протоколом, который подписывается членами приемочной комиссии. По факту успешного проведения приемочных испытаний подписывается Акт завершения приемочных испытаний.

При обнаружении во время приемочных испытаний недостатков, дефектов или иных отклонений от требований ТЗ, соответствующие факты должны фиксироваться в протоколе, в котором в том числе указывается:

- перечень недостатков (дефектов);
- степень влияния отмеченных недостатков на работоспособность системы;
- требуемые сроки устранения недостатков (дефектов).

В течение пяти рабочих дней с момента устранения недостатков, дефектов или иных отклонений от требований к системе, приемочная комиссия должна провести повторные приёмочные испытания соответствующего компонента и принять Систему в постоянную эксплуатацию.

3.4 Обучение персонала.

Обучение согласно п.9 данного ТЗ.

4 Место выполнения работ и оказания услуг

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

Сроки поставки ПО (АПК) будут определены в Договоре между Заказчиком и Исполнителем, но не более 90 календарных дней, со дня подписания договорных отношений Заказчика с Исполнителем.

5 Технические требования к Системе

К Системе предъявляются следующие требования:

5.1 Функциональные требования

5.1.1 Система защиты электронной почты должно представлять собой шлюз безопасности электронной почты.

5.1.2 Система должна поддерживать работу в режимах:

- почтовый сервер;
- прозрачный шлюз;
- шлюз (агент МТА).

5.1.3 Система должна обеспечивать Анти-спам фильтрацию электронной почты.

5.1.4 Система должна обеспечивать Анти-фишинг фильтрации электронной почты.

5.1.5 Система должна обеспечивать Антивирусную фильтрации электронной почты.

5.1.6 Система должна обеспечивать фильтрацию URL в теле электронных писем.

5.1.7 Система должна обеспечивать предотвращение утечек конфиденциальных данных;

5.1.8 Система должна обеспечивать карантин для подозрительных сообщений электронной почты.

5.1.9 Система должна обеспечивать фильтрацию входящей и исходящей электронной почты.

5.1.10 Система должна поддерживать политики защиты и маршрутизация почты на основе атрибутов LDAP (домена).

5.1.11 Система должна поддерживать SMTP-аутентификацию посредством LDAP, RADIUS, POP3 или IMAP протоколов.

5.1.12 Система должна поддерживать очередь сообщений для ошибочных, поврежденных, задержанных и недоставленных сообщений.

5.1.13 Система должна обеспечивать возможность интеграции с внешними RBL (Realtime Blackhole List) сервисами.

5.1.14 Система должна поддерживать технологии Email аутентификации: Domain Key Identified Management (DKIM), Sender Policy Framework (SPF).

5.1.15 Система должна обеспечивать поддержку «черных» и «белых» списков отправителей (Email адрес\Email домен\IP адрес).

5.1.16 Система должна обеспечивать защиту от DDoS атак на почтовую инфраструктуру Заказчика.

5.1.17 Система должна обеспечивать контроль URL в теле письма.

5.1.18 Система должна поддерживать интеграцию с внешними программными решениями класса Sandbox (песочница), для осуществления эффективной защиты от угроз класса "0-day". Письмо, содержащее подозрительные вложение не должны перенаправляться на принимающий почтовый сервер до окончания инспекции (с положительным заключением) на решении класса Sandbox.

Поставляемая Системы защиты электронной почты со встроенной фильтрацией SPAM-

сообщений, должна поставляться в рамках ТЗ без Sandbox, но должно поддерживать работу с данным функционалом в дальнейшем.

5.1.19 Предотвращение утечек конфиденциальных данных, а также идентификация и блокировка контента должна быть возможна, как минимум, по ключевым словам, словарям, регулярным выражениям, хэшу файла.

5.1.20 Контроль содержимого электронных писем, должен разделяться: по типу, числу, размеру вложений.

5.1.21 Система должна поддерживать экспорт журналов всех событий внутри Системы.

5.1.22 Система должна поддерживать мониторинг по протоколу SNMP.

5.1.23 Система должна обеспечивать возможность архивирования входящих и исходящих сообщений на основе политик, с поддержкой различных резервных носителей (HDD, SSD, LTO).

5.1.24 Система должна обеспечивать поддержку отказоустойчивых кластеров в режимах Active-Active, Active-Passive.

5.1.25 Система должна обеспечивать встроенную, основанную на политиках, маршрутизацию почты и управление очередями.

5.1.26 Система должна поддерживать архивирование входящих и исходящих сообщений, с настраиваемой глубиной архива.

5.1.27 Администрирование Системы должно выполняться через графический WEB-интерфейс управления или интерфейс командной строки (CLI).

5.1.28 Количество защищаемых почтовых ящиков или пользователей, не должно быть ограничено лицензией.

5.1.29 Система должна обеспечивать эвристические методы фильтрации почты.

5.1.30 Система должна обеспечивать фильтрацию вложений/содержимого почтового сообщения.

5.1.31 Система должна обеспечивать усиленную проверку заголовков сообщения.

5.1.32 Система должна обеспечивать проверку в реальном времени на спам с помощью «черных» списков URL (SURBL).

5.1.33 Система должна обеспечивать проверку в реальном с использованием Байесовского статистического фильтра (адаптируемая технология защиты от спама, которая работает на основе алгоритмов искусственного интеллекта).

5.1.34 Система должна обеспечивать фильтрацию, по запрещенным словам.

5.1.35 Система должна обеспечивать управление спамом (принять, передать, отклонить или отвергнуть), основанное на блоклисте проверок контрольных сумм спама SHFSH.

5.1.36 Система должна обеспечивать сканирование и анализ графических изображений.

5.1.37 Система должна обеспечивать поддержку общих и пользовательских настраиваемых «черных»/«белых» списков.

5.1.38 Система должна обеспечивать поддержку «черных» списков, формируемых в реальном времени (RBL), третьих фирм (RBL – это каталоги, содержащие списки доменных имен, серверов электронной почты или IP-адресов, которые, как известно, помогают размещать, производить или пересылать спам).

5.1.39 Система должна обеспечивать проверку на ложность IP-адреса отправителя.

5.1.40 Система должна проверку с использованием грейстинга (Greylisting - «серые списки»).

5.1.41 Система должна обеспечивать различные действия при выявлении спама, включая маркировку писем.

5.1.42 Система должна обеспечивать проверку на вирусы SMTP-сообщений.

5.1.43 Система должна обеспечивать поддержку сжатых присоединенных файлов (вложений) и вложенных архивов.

5.1.44 Система должна обеспечивать помещение зараженных файлов на карантин.

5.1.45 Система должна обеспечивать поддержку уведомлений при замене сообщений, либо удалении подозрительных вложений.

5.1.46 Система должна обеспечивать проверку и блокирование вложения по типам файлов.

5.1.47 Система должна поддерживать антивирусный движок и сигнатуры для него собственной разработки (от производителя).

5.2 Требования к протоколированию, уведомлению и отчетности

5.2.1 Система должна обеспечивать протоколирование изменения конфигураций и событий управления.

5.2.2 Система должна обеспечивать протоколирования вирусных инцидентов.

5.2.3 Система должна обеспечивать протоколирование активности модуля противодействия спаму.

5.2.4 Система должна обеспечивать поддержку внешнего Syslog-сервера.

5.2.5 Система должна обеспечивать расширенную систему отчетности с поддержкой пользовательских устройств.

5.2.6 Система должна обеспечивать уведомление о критических событиях и вирусных инцидентах.

5.2.7 Система должна позволять изменять содержимое уведомлений о событиях и инцидентах, по шаблону Заказчика.

5.2.8 Система должна поддерживать полноценную систему отчетности, включающая генерацию отчетов по категориям.

5.2.9 Система должна поддерживать предустановленные шаблоны отчетов.

5.2.10 Система должна обеспечивать формирование отчетов по расписанию.

5.2.11 Система должна обеспечивать формирование и отправку отчетов в PDF-формате.

5.3 Требования к техническим характеристикам решения

5.3.1 Система может быть реализована как в виде программного, так и в виде аппаратно-программного комплекса (АПК).

5.3.2 В случае поставки АПК, он должен удовлетворять следующим условиям:

- количество интерфейсов подключения 10/100/1000 (медь, RJ45): не менее 4;
- наличие встроенного накопителя, для хранения статистической и архивной информации;

- форм-фактор: для монтажа в 19" стойку;

- тип блоков питания: 220V, AC.

5.4 Требования к производительности

5.4.1 Максимальное количество защищаемых доменов электронной почты: не более 20.

5.4.2 Максимальное количество защищаемых почтовых ящиков: не более 2500.

5.4.3 Маршрутизация электронной почты (писем размером 100 Кбайт в час): не менее 50 000.

5.4.4 Маршрутизация электронной почты (писем размером 100 Кбайт в час) с включенным функционалом Антиспам и Антивирус: не менее 40 000.

5.4.5 Маршрутизация электронной почты (писем размером 100 Кбайт в час) с включенными функционалом Антиспам, Антивирус, URL Фильтрация, Sandbox (песочница): не менее 30 000.

5.5 Требования к взаимодействию со сторонними информационными системами.

- Взаимодействие между системами должно проектироваться и настраиваться с учетом требований к информационной безопасности каждой из подсистем.
- Система должна поддерживать интеграцию и взаимодействие с контроллером домена Active Directory.
- Гибкая настройка правил доступа на основе групп, ролей, времени и местоположения.
- Возможность интеграции с существующей системой мониторинга Заказчика (Zabbix).
- Система должна поддерживать виртуальную инфраструктуру (VMware ESX/ESXi).

5.6 Требования к режимам функционирования Системы

Основной режим функционирования Системы – автоматизированный, под управлением администратора.

Система должна обеспечивать возможность работы в следующих режимах:

- штатный режим (непрерывная круглосуточная работа);
- сервисный режим (для проведения обслуживания, реконфигурации и модернизации компонентов);
- автономный режим (в случае отсутствия связи между компонентами системы или с внешними сетями, для доступа к конфигурационной и архивной информации).

5.7 Требования к численности и квалификации персонала поставщика

Для обеспечения поставки программного комплекса и запуска рабочего функционирования Системы в составе персонала поставщика должны присутствовать минимум одна штатная единица инженера технической поддержки.

Инженер технической поддержки должен обладать знаниями в объеме, необходимом для выполнения штатного технического и аварийного обслуживания Системы у Заказчика.

5.8 Требования к аудиту мониторинга и отчетности.

Система должна обеспечивать ведение журнала всех аутентификаций, команд и действий привилегированных пользователей.

Система должна иметь поддержку аудита в реальном времени с возможностью отправки оповещений при выявлении подозрительной активности.

Система должна иметь функционал генерации отчетов о действиях пользователей в формате PDF, CSV и интеграция с BI-системами.

Система должна хранить почтовые логи, не менее 3 мес, с поддержкой политики сохранения данных с возможностью их экспорта.

6 Требования к Исполнителю

К Исполнителю предъявляются следующие требования:

6.1 В рамках закупочной процедуры Исполнитель должен предоставить информацию:

- детальную спецификацию оборудования (если Система поставляется в виде КТС);
- срокам поставки и инсталляции ПО (АПК);
- условиям и стоимости послегарантийной сервисной технической поддержки.
- условиям и стоимости лицензий (подписки) на программное обеспечение с учетом обеспечения требований надежности работы и возможности дальнейшего увеличения числа защищаемых рабочих станций сотрудников ООО «UMS».
- особенностям предлагаемого технического решения.

6.2 Общие требования к Исполнителю

Исполнитель должен удовлетворять следующим требованиям:

- подтвержденный опыт работы по предоставлению обозначенных услуг (поставка ПО) не менее, чем 3 года;
- являться авторизованным партнёром, а также иметь документальное подтверждение на распространение конечным пользователям прав на использование и внедрение реализуемого/внедряемого программного обеспечения;
- не являться неплатежеспособным или банкротом, находится в процессе ликвидации, не должен быть наложен арест, экономическая деятельность Исполнителя не должна быть приостановлена;
- иметь в наличие в своем составе не менее 2 (двух) специалистов, обладающих сертификатами, подтверждающими квалификацию в части установки, настройки, эксплуатации, технической поддержки данного ПО.

Исполнитель обязан соблюдать требования, предъявляемые действующим законодательством Республики Узбекистан к работе с документами и сведениями, содержащими конфиденциальную информацию и не разглашать конфиденциальную информацию, ставшую ему известной в процессе оказания услуг.

6.3 Исполнитель должен включить в состав предложения следующие документы, подтверждающие его соответствие вышеуказанным требованиям:

- копию авторизованного письма о наличии партнерского статуса с компанией производителем;
- копии минимум 2х сертификатов инженеров от компании производителя.
- перечень реализованных ИТ-проектов за последние 3 года.

6.4 Требования к производителю

Компания-Вендор должна существовать на рынке не менее 5 лет, и иметь авторизованных партнеров на рынке Узбекистана.

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

Для всех компонентов решения Исполнитель должен предоставить следующую информацию:

- общее описание технического решения, с описанием преимущества использования предлагаемого решения над существующими аналогами (технико-экономическое обоснование);
- опции решения для ООО «UMS»;
- конкурентные преимущества предлагаемого решения в деталях, а также недостатки решения;
- конфигурацию и технологическую детализацию для каждой опции;
- описание программного обеспечения (function/feature description);

После внедрения Системы, Исполнитель готовит исполнительную документацию (в 2 экземплярах), в печатном виде, с детальным описание Системы, конфигурациями компонентов, схемами интеграции в инфраструктуру Заказчика.

9 Требования к обучению персонала Заказчика

В рамках данного Проекта, Исполнитель обеспечивает дистанционное сертификационное

обучение двух специалистов Заказчика по администрированию данного комплекса.

Факт прохождения обучения должен быть подтвержден соответствующим сертификатом. Программу и время обучения предварительно согласовать с Заказчиком.

10 Гарантийные обязательства

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

Срок гарантии на выполненные работы по внедрению Системы, должен составлять **36 (тридцать шесть) месяцев** и исчисляется со дня подписания Сторонами акта сдачи – приемки работ.

Период опытной эксплуатации должен составлять 1 (один) месяц и исчисляться со дня подписания Сторонами акта сдачи – приемки работ.

11 Условия сервисной поддержки и техническое сопровождение

Срок сервисной поддержки производителя – **36 месяцев**, с момента внедрения ПО. Сервисная поддержка на программные компоненты должна оказываться как производителем, так и партнером.

Исполнитель обязан предоставить информацию об информационных ресурсах компании производителя ПО, для самостоятельного скачивания документации, обновлений, релизов.

Исполнитель осуществляет привязку идентификационных данных ПО в кабинете Заказчика, на сайте Производителя.

Работы по техническому сопровождению ПО (либо АПК) должны включать в себя:

а) Обеспечение непрерывного функционирования серверной части системы защиты EMAIL-спам:

- настройка параметров Системы для оптимизации использования аппаратных и программных ресурсов;

- настройка параметров Системы для управления политикой безопасности;

- тестирование работы Системы в штатном режиме после проведения обновлений.

b) Настройка очистки и оптимизации наборов правил, планирования изменений Системы.

c) Интеграция с существующими системами управления изменениями.

d) Консультации по масштабированию Системы.

e) Доступ к portalу производителя ПО (возможность скачивать обновления, доступ к форуму, доступ к документации).

f) Проведение инструктажа 2-х администраторов Системы в объеме базового и расширенного курсов.

g) Подключение специалиста посредством VPN по требованию ООО «UMS» для решения возникших проблем, консультаций, связанных с функционированием Системы.

h) Восстановление работоспособности программного комплекса:

- восстановление работоспособности системы в штатном режиме не позднее, чем через 2 рабочих дня после сбоя программных средств;

- перенастройка, реконфигурирование, обновление и/или полная переустановка программного комплекса, а также устранение причин, приведших к сбою (при условии сбоя, вызванного продуктами компании);

- возможность отключения Системы на время сбоя для проведения восстановительных работ;
- восстановление активности Системы, после аппаратных сбоев, потеря питания, и т.д.;
- операции восстановления данных из резервных копий.
- предоставление отчетов о проделанной работе.

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 Приложении №2 к данному ТЗ.

12.1 Требование к комплектации

Система должна иметь полную комплектацию, для полноценного функционирования предлагаемого решения в рамках текущего ТЗ. Стоимость ПО должна формироваться исходя из полной комплектации.

12.2 Требование к интеграции

Интеграция должна учитывать особенности работы инфраструктуры Заказчика.

12.3 Сведения о новизне

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

12.4 Страхование

Требования не предъявляются, однако Исполнитель несет ответственность сохранности программного комплекса до момента его официальной передачи Заказчику.

12.5 Матрица распределения ответственности при оказании

Техническое обслуживание	Исполнитель	Заказчик
Доступность системы		
Обнаружение и классификация приоритетности проблемы, открытие запроса для решения у Правообладателя	A	R
Производить настройку ПО Заказчика по запросу	A	R
Предоставлять статистику решения проблем за отчетный период	R	A
Регистрировать все запросы на портале Правообладателя	R	A
Обновления, исправления, корректировки программного обеспечения		
Предоставить метод процедуры	R	A
Определить время установки	A	R
Установить Программное обеспечения	R	A
Проверить работу установленного программного обеспечения	A	R
Сервисы и рекомендации		
Предоставить технические требования	R	R
Внедрение технических требований	R	A
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
АПК	Аппаратный программный комплекс
EMAIL	Почтовый ящик
SPAM	Нежелательные сообщения
БД	База данных
ККД	Компонент контроля действий
ИБ	Информационная безопасность
RBL	Каталоги, содержащие списки доменных имен, серверов электронной почты или IP-адресов, которые, как известно, помогают размещать, производить или пересылать спам
SURBL	Spam URI Real-Time Blocklist(s)
URL	Унифицированный указатель ресурс

14 Перечень приложений

Приложение №1 – Характеристика объекта информатизации.

Приложение №2 – Форма подачи предложения.

ТЗ разработал:

Начальник отдела информационной
безопасности ДИБиР


подпись

Абдульваат Р.А.

Директор ДИБиР


подпись

Олматов Б.А.

Характеристики объекта информатизации

ООО «UMS» - телекоммуникационная компания, оказывающая услуги мобильной связи на всей территории Республики Узбекистан с 1 декабря 2014 года.

ООО «UMS» образован на основании постановления Кабинета Министров Республики Узбекистан №208 «О создании совместного предприятия «Universal Mobile Systems» по оказанию услуг мобильной связи» от 31 июля 2014 года, является одним из ведущих мобильных операторов Республики Узбекистан.

В соответствии с Постановлением Президента Республики Узбекистан №ПП-5187 от 19 июля 2021г. учредителем ООО «UMS» является Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан.

Штатная численность Компании, 1800 человек.

Общее количество потовых ящиков пользователей – 1600шт.

Общее количество потовых ящиков технологических учетных записей – 100шт.

Внутренние почтовые сервера на базе Microsoft Exchange.

Внешние почтовые сервера на базе Postfix.

Форма предложения

Описание	Количество	Стоимость
Программное обеспечение (ПО) и Лицензии, в составе:	3 года (в случае подписки)	
Лицензии и ПО		
Аппаратная часть (если имеется), в составе:		
Спецификация оборудования		
Работы по внедрению ПО, в составе:		
Работы по разработке, инсталляции и конфигурированию системы.		
Работы по интеграции с системами Заказчика		
Обучение сотрудников Заказчика		
Гарантийная и Техническая поддержка в составе:	лет	
Гарантийная поддержка (включая апгрейды на новые версии ПО) от Вендора	3	
Техническая поддержка от Поставщика	3	