«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»
Генеральный директор
ООО «UNIVERSAL MOBILE SYSTEMS»

_____ С.Х. Арипов
«__» _____ 2022 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на модернизацию системы безопасного удаленного доступа к корпоративным ресурсам, с централизованным управлением политиками информационной безопасности (приобретение лицензий, услуги по внедрению программного обеспечения и организации обучения)
для нужд ООО "UMS"
(Общество с ограниченной ответственностью «Universal Mobile Systems»)

город Ташкент

2022 год

Оглавление

Используемые термины и сокращения

Сокращение	Расшифровка сокращения
ТЗ	Техническое задание
ПО	Программное обеспечение
ИС	Информационная система
ИТ	Информационные технологии
VPN	Виртуальная частная сеть
LAN	Локальная вычислительная сеть
ЦОД	Центр обработки данных
Подписка	Доступ к сервисам производителя ПО
SLA	Service Level Agreement - Соглашение об уровне сервиса
SSL	Криптографический протокол
TLS	Протокол защиты транспортного уровня
IPsec	Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP
IKEv1, IKEv2	Набор протоколов IPsec, используемый для обеспечения защищённого взаимодействия в виртуальных частных сетях
AES, 3DES	Алгоритмы блочного шифрования
RSA	Криптографический алгоритм с открытым ключом
SHA	Алгоритм криптографического хеширования
LDAP	Протокол позволяющий производить операции аутентификации
RDP	Протокол удалённого рабочего стола

1 Общие сведения

Настоящее Техническое задание к закупке ПО для удаленного доступа разработано в соответствии с Государственным стандартом РУз O‘z DSt 1987:2018 «Информационная технология. Техническое задание на создание информационной системы».

В настоящем Техническом задании описаны общие требования к программному обеспечению для безопасного удаленного доступа, достаточные для однозначного и точного описания требований Заказчика к модернизируемой системе с целью объявления тендера и/или конкурса на приобретение программного обеспечения и услуг для реализации проекта в целом на условиях «под ключ».

1.1 Полное наименование и условное обозначение Системы

Система безопасного удаленного доступа к корпоративным ресурсам, с централизованным управлением политиками информационной безопасности (далее – ИС, Система).

1.2 Наименования организации-Заказчика и организации-Исполнителя

Модернизация Системы проводится на инфраструктуре и площадке Заказчика с использованием действующего оборудования.

Заказчик: (далее по тексту – Заказчик)
ООО «UMS», 100000 г. Ташкент, пр-кт А.Темура, 24, +99897 4038100, info@mobi.uz. ИНН: 303020732;

Владелец Системы:
ООО «UMS» (Заказчик), 100000 г. Ташкент, ул.А.Темура-24, +99897 4038100, info@mobi.uz;

Исполнитель:
Исполнитель выбирается на основании закупочной процедуры по предмету приобретения программного обеспечения, услуг по внедрению программного комплекса согласно настоящему ТЗ.

1.3 Плановые сроки начала и окончания работ по модернизации Системы

Продолжительность работ: 7 недель.
Ориентировочная дата начала: Июль 2022 года.
Ориентировочная дата окончания: Август 2022 года.

2 Назначение и цели модернизации ИС

2.1 Назначение Системы

Назначение Системы заключается в предоставлении сотрудникам компании безопасного удаленного доступа к корпоративным ресурсам предприятия, и централизованном управлении политиками информационной безопасности со стороны администраторов Системы.

2.2 Цели модернизации Системы

Целью модернизации Системы является создание надежного, современного, безопасного инструмента для удаленного доступа сотрудников к корпоративным ресурсам компании, а также внедрение функционала централизованного управления политиками информационной безопасности способного работать как с проводными, так и беспроводными (WiFi) сетями, работающими на предприятии.

2.3 Задачи Проекта

Ключевыми задачами проекта, обеспечивающими достижение поставленной цели, являются:

– создание современной программной платформы для удаленного доступа сотрудников к корпоративным ресурсам;

– организация возможности разграничения сетевого доступа к корпоративным системам;

– создание инструмента контроля доступа и аутентификации пользователей беспроводной сети Заказчика для доступа к корпоративным ресурсам;

– автоматизация процессов предоставления прав удаленного доступа к корпоративным
информационным системам;

– обеспечение высочайшей сетевой безопасности корпоративных ИТ-систем;

– контроль и анализ трафика между сетями.

2.4 Предпосылки к внедрению Системы

Текущая информационная инфраструктура не предусматривает надлежащий контроль пользовательского доступа к сети, включая идентификацию и расширенную проверку пользователей для возможности определения соответствия корпоративным политикам безопасности и применения соответствующего уровня доступа.

2.5 Основание для реализации проекта

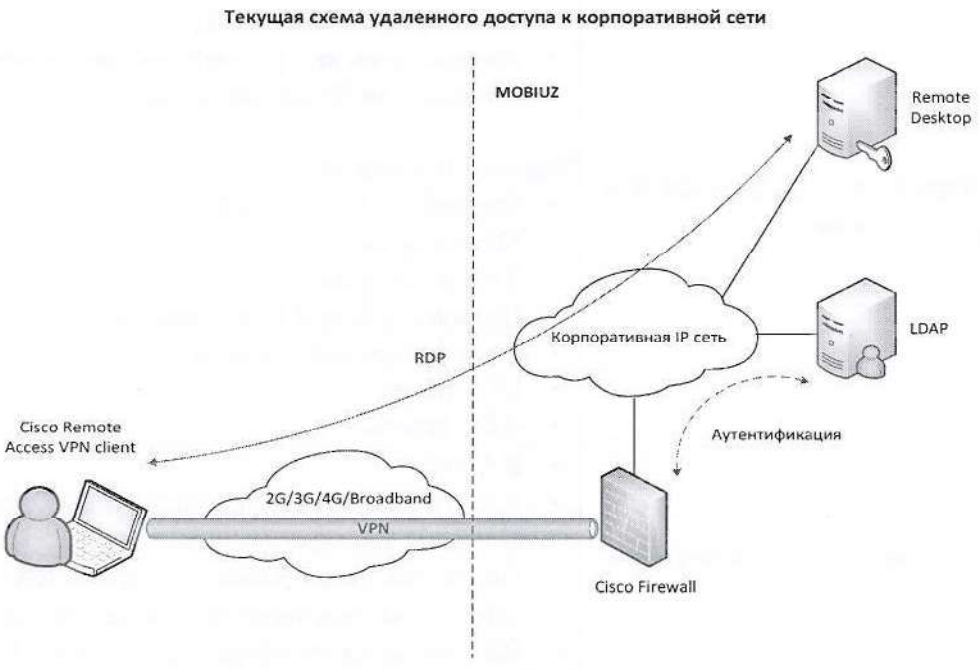
Основанием для проекта является запланированный на 2022г. план развития ИТ.

3 Характеристики объекта модернизации

3.1 Краткие сведения об объекте автоматизации

Действующая структурная схема удаленного доступа к корпоративной сети приведена на **Ошибка! Источник ссылки не найден.**.

Рисунок 1



4 Основные требования к ПО

4.1 Требования к ПО в части безопасного удаленного доступа

№	Параметр	Значение
1	Поддерживаемые операционные системы (платформы)	• Windows • MacOS • Linux • iOS • Android • Windows Phone/Mobile • BlackBerry • ChromeOS
2	Доступ к ПО	Техническая поддержка и право на программное обеспечение включены во все основанные на сроке лицензии
3	Поддержка протоколов туннелирования	• SSL (TLS 1.2 и DTLS), • IPsec IKEv2
4	Поддержка функций «Mobility friendly»	• VPN-соединение остается активным во время изменения IP-адреса, потери соединения, гибернации или ожидания • При обнаружении доверенной сети VPN-соединение может автоматически отключаться, когда конечный пользователь находится в офисе, и подключаться, когда пользователь находится в удаленном местоположении.
5	Шифрование	• AES-256; • 3DES-168; • Шифрование следующего поколения, включая алгоритмы NSA Suite B, ESPv3 с IKEv2, 4096-битные ключи RSA, • улучшенный SHA2 (SHA-256 и SHA-384).
6	Варианты развертывания и подключения	• Предварительное развертывание, через установщика Microsoft; • Автоматическое развертывание помощью ActiveX (только для Windows) и Java. Режимы подключения: • Standalone by system icon • Stealth agent • Temporal agent • Browser-initiated (web launch) • Clientless portal initiated • CLI initiate • API initiated
7	Варианты аутентификации	• RADIUS; • RADIUS с истечением пароля (MSCHAPv2) для NT LAN Manager (NTLM); • Поддержка одноразового пароля RADIUS (OTP) (атрибуты состояния и ответного сообщения); • RSA SecurID (включая интеграцию SoftID);

		• Active Directory или Kerberos; • Встроенный центр сертификации (CA); • Цифровой сертификат или смарт-карта (включая поддержку машинного сертификата), выбираемые автоматически или пользователем; • Облегченный протокол доступа к каталогам (LDAP) с истечением срока действия пароля и устареванием • Общая поддержка LDAP; • Комбинированная многофакторная аутентификация сертификата и имени пользователя и пароля (двойная аутентификация)

4.2 Требования к ПО в части контроля доступа к сети

Система контроля доступа к сети должна удовлетворять, как минимум, следующим требованиям:

- Должна быть предусмотрена возможность развертывания системы в существующей системе виртуализации VMWare;
- Система должна предусматривать отказоустойчивую схему 1+1;
- Контроль доступа к сети должен обеспечиваться для проводного и беспроводного сегментов сети, а также для удаленных пользователей, подключающихся по Remote Access VPN;
- Наличие поддержки работы системы согласно стандарту 802.1x. Система в данном случае выступает как сервер AAA (Аутентификация, авторизация и учет);
- Система должна быть рассчитана на 2 000 одновременных пользовательских сессий/подключений;
- Наличие поддержки протокола RADIUS для обеспечения функций аутентификации и авторизации пользователей и конечных устройств, подключающихся к проводному и беспроводному сегментам сети, а также к удаленным подключениям VPN;
- Наличие поддержки механизма RADIUS CoA (Change of Authorization) для возможности назначения и изменения уровня пользовательского доступа к сети в зависимости от условий подключения;
- Наличие поддержки протокола EAP (EAP-TLS, EAP MS-CHAP, PEAP);
- Обеспечение одновременной пользовательской и машинной аутентификации с использованием доменных учетных данных и сертификатов в рамках одной пользовательской сессии;
- Наличие поддержки использования различных полей пользовательского сертификата, таких как Common Name, Subject Alternative Name, Serial Number, SAN-Email и SAN-DNS, для идентификации пользователя в процессе аутентификации;
- Наличие поддержки локальной базы пользователей;
- Наличие поддержки локальной базы устройств на основе MAC адресов;

- Наличие поддержки интеграции с корпоративным каталогом Active Directory. Должна обеспечиваться возможность осуществления авторизации на основе принадлежности пользователей к группам в Active Directory;
- Наличие возможности определения последовательности проверки баз данных пользователей;
- Обеспечивать мониторинг путем обнаружения и управления подключающихся к сети оконечных устройств для предоставления соответствующих сервисов и уровней доступа;
- Обеспечивать предотвращение несанкционированного доступа к сети для защиты корпоративных активов;
- Наличие поддержки встроенной консоли мониторинга и устранения неполадок для упрощения работы специалистов службы поддержки и администраторов;
- Наличие поддержки применения листа контроля доступа или соответствующего идентификатора VLAN для пользователя в результате процесса авторизации;
- Наличие поддержки функции проверки операционной системы пользовательского устройства на предмет наличия соответствующих версий операционной системы, установленных приложений, антивирусного программного обеспечения, параметров в системном регистре, статус активности программных компонентов. Система должна быть рассчитана на одновременную проверку не менее 2 000 пользовательских устройств. Поддержка возможности применения политики доступа в зависимости от статуса соответствия заданным параметрам;
- Наличие встроенной службы центра сертификации;
- Наличие поддержки функции автоматического определения типа и версии программного обеспечения подключаемого пользовательского устройства. Система должна быть рассчитана на одновременное подключение не менее 2 000 пользовательских устройств;
- Система должна быть совместима с существующим активным оборудованием (коммутаторами, устройствами безопасности, контроллерами беспроводной сети) сетевой инфраструктуры;
- Наличие поддержки аутентификации и авторизации для административного доступа к оборудованию сети с возможностью авторизации вводимых команд на сетевом оборудовании и ведением журнала по ним;
- Сервисная поддержка решения должна быть рассчитана не менее чем на 3 года;
- Срок действия лицензии должен быть не менее 3 лет.

4.3 Требования к архитектуре

Для работы Системы должно использоваться система виртуализации на базе гипервизора VMware ESXi.

Отказоустойчивость системы должна достигаться путем создания кластера из виртуальных машин состоящего минимум из 2 нод.

Целевая структурная схема удаленного доступа к корпоративной сети, с централизованным управлением политиками информационной безопасности приведена на Рисунке 2.

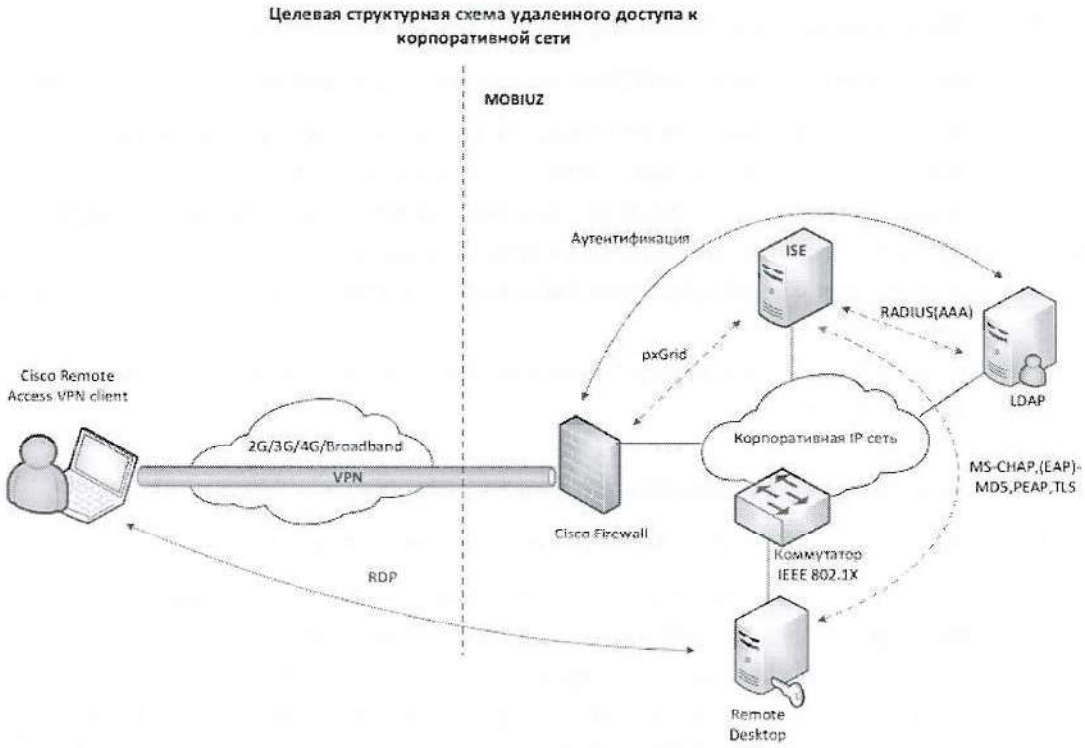


Рисунок 2

4.4 Требования к взаимодействию с информационными системами

4.4.1 Интеграция с MS Active Directory и MS Exchange

Система должна обеспечивать интеграцию с решениями MS Active Directory и MS Exchange:

- поддержка Microsoft Active Directory 2003, 2008, 2008R2, 2012, 2012R2, 2016;
- поддержка комплексной проверки подлинности и авторизации в доменах Microsoft Active Directory с несколькими лесами;
- группировка несколько разрозненных доменов в логические группы.

4.4.2 Интеграция с Cisco Firepower

Система должна обеспечивать интеграцию с решением Cisco Firepower:

- наличие поддержки политик на основе контекста удостоверения, такого как тип устройства, местоположение, группы пользователей;
- поддержка обмена атрибутами групп безопасности;
- поддержка возможности обмена информацией профиля конечной точки и IP-адресом;
- возможность использования атрибутов обмена в политиках управления доступом для разрешения/запрета доступа по мере необходимости;
- возможность действий по исправлению, такое как отправка CoA (изменение авторизации) и помещение пользователя в карантин путем применения DACL.

4.4.3 Интеграция с корпоративной WiFi сетью Заказчика

Система должна обеспечивать интеграцию с корпоративной WiFi сетью Заказчика:

- поддержка возможности создания гостевых учетных записей для посетителей и аутентификация их в целях аудита;
- поддержка предоставления гостевого доступа в режиме «точка доступа» (предоставление доступа без учетных данных);
- поддержка предоставления гостевого доступа в режиме самостоятельной регистрации;
- поддержка предоставления гостевого доступа в режиме «спонсируемый гостевой доступ».

4.4.4 Интеграция с системой мониторинга Zabbix

Система должна обеспечивать интеграцию с мониторинга Zabbix:

- поддержка протокола сетевого управления SNMP версий v1, v2, v3;
- поддержка системной диагностики и статистики стандарта отправки и регистрации сообщений о происходящих в системе событиях syslog:
- сбор и отправка сообщений syslog на удаленно сконфигурированную цель;
- поддержка интеграции с системами мониторинга с помощью REST API.

5 Общие требования к квалификации Исполнителя

5.1 Исполнитель должен обладать опытом и ресурсами, необходимыми для реализации проекта и оказания услуг по его интеграции, а также являться официальным партнером производителя программных средств, предлагаемых в решении. Уровень партнерства должен быть не ниже Premier Partner.

5.2 Для выполнения работ по модернизации Системы требуется квалифицированный персонал, в количестве не менее 2 человек, прошедших обучение, и имеющих соответствующие сертификаты.

5.3 Исполнитель должен предоставить информацию по:

- системным требованиям для полноценного функционирования программного комплекса;
- условия лицензирования ПО (срок действия лицензий, порядок взимания платы и т.п.);
- порядок лицензирования ПО (объем, функционал, вид лицензий (срочные/бессрочные, по пользователям/без ограничений), и т.д.);
- тип сервисной поддержки (подписка, непрерывность сервиса, наличие штрафных санкций при несвоевременном продлении поддержки).

5.4 Исполнитель должен обеспечить высокое качество оказываемых услуг, их результата и соответствие нормам и стандартам, действующим в Республике Узбекистан.

5.5 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.

6 Состав и содержание работ по модернизации Системы

В рамках проекта Исполнителем должны быть выполнены следующие этапы работ:

- подготовительный этап, с обследованием существующей инфраструктуры Заказчика;
- техническое проектирование;
- инсталляционные работы;
- обучение персонала Заказчика.

6.1 Подготовительный этап.

Включает проведение обследования существующей инфраструктуры Заказчика, с уточнением и согласованием требований со стороны Заказчика. На данном этапе Исполнитель должен осуществить сбор исходных данных, таких как:

- конфигурация существующего сетевого оборудования;
- детали архитектуры сети передачи данных Заказчика;
- сведения о настройках смежных систем (WiFi, AD), которые необходимо интегрировать в предлагаемое решение;
- зоны ответственности Заказчика и Исполнителя в ходе инсталляции ПО;
- порядок и методики приёмки Системы в эксплуатацию;
- сведения о вероятных простоях инфраструктуры Заказчика в ходе реализации проекта.

Завершение работ по данному этапу должно быть зафиксировано в отчетном документе, оформленном в качестве концепции по реализации данного проекта, предоставляемом Исполнителем в проектной документации.

6.2 Техническое проектирование.

Данный этап включает разработку комплекта документации в соответствии с требованиями к документированию. Проектная документация на Систему, должна быть выполнена на русском языке и должна содержать:

- техническое задание на проектирование;
- рабочий проект, в который включаются:

a) пояснительная записка к техническому проекту,
b) архитектура решения и схема взаимодействия его подсистем,
c) конфигурации используемого программного обеспечения;

- программу и методику приемочных испытаний;
- комплект инструкций для сетевых администраторов Заказчика.

6.3 Инсталляционные работы

Данный этап включает в себя следующие работы:

- установка ПО в среду виртуализации VMware;
- установка ПО, сервисных пакетов и всех обновлений;
- активация лицензий на ПО и все компоненты, входящие в его состав;
- интеграция с Active Directory для аутентификации пользователей;

- настройка конфигураций и политик безопасности;
- проведение необходимых тестов, подтверждающих нормальное функционирование Системы;
- настройка технологии отказоустойчивости модулей и компонентов, входящих в состав ПО;
- демонстрация работоспособности базовой конфигурации Системы Заказчику;
- краткий инструктаж системных администраторов Заказчика;
- постановка установленного ПО на мониторинг. Настройка отправки сообщений о возникновении аварийных ситуаций по протоколу SNMP, в систему мониторинга Заказчика (Zabbix).

6.4 Обучение персонала Заказчика.

В рамках проекта, Исполнитель обеспечивает локальное либо дистанционное сертифицированное обучение двух специалистов Заказчика. Факт прохождения обучения должен быть подтвержден соответствующим сертификатом. Программу обучения предварительно согласовать с Заказчиком.

7 Требования по правилам сдачи и приёмки

Исполнитель в течение 12 (двенадцать) рабочих дней с даты получения Исполнителем от Заказчика авансового платежа, предоставляет Заказчику лицензии на ПО и право доступа к репозиториям с дистрибутивами.

Исполнитель перед началом инсталляционных работ Исполнитель осуществляет регистрацию/привязку программных продуктов и сервисных и контрактов к учетной записи в персональном кабинете Заказчика.

Выявленные при приемке Услуг недостатки и отступления от условий заключенного Договора устраняются Исполнителем за свой счет в течение 10 (десяти) рабочих дней.

8 Требования к составу и содержанию работ по подготовке Системы к вводу в эксплуатацию

В ходе выполнения проекта требуется выполнить работы по подготовке к вводу Системы в действие. При подготовке к вводу в эксплуатацию Системы Заказчик должен обеспечить выполнение следующих работ:

a) Определить ответственных за эксплуатацию Системы;
b) Обеспечить обучении работе с Системой, проводимом Исполнителем;
c) Обеспечить выполнение требований, предъявляемых к техническим средствам, на которых должно быть развернуто программное обеспечение;
d) Совместно с Исполнителем подготовить план интеграции технических средствах Заказчика с Системой;
e) Ввести Систему в эксплуатацию.

Требования к составу и содержанию работ по подготовке к вводу Системы в эксплуатацию, включая перечень основных мероприятий и их исполнителей, должны быть уточнены на стадии подготовки рабочей документации и по результатам испытаний.

Сроки ввода Системы в эксплуатацию определяются Заказчиком и согласуются с Исполнителем.

В период подготовки к началу эксплуатации Исполнитель занимается:

- оптимизацией настроек программных средств и компонент,
- обучением персонала работе с Системой,
- настройкой мониторинга всех компонентов Системы.

9 Требование к документированию

Проектная документация должна быть выполнена на русском языке и содержать:

- рабочий (технический) проект, в который включаются:
  a) пояснительная записка к техническому проекту;
  b) архитектура программного решения и схема взаимодействия его подсистем;
  c) конфигурации используемого оборудования Заказчика и программного обеспечения;
  d) программу и методику приемочных предварительных и приемочных испытаний;
- комплект эксплуатационной документации, предоставляемой производителем для всех подсистем решения;
- комплект инструкций для сетевых администраторов и администраторов ИБ.

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

- стоимость предложения, включающего в себя структуру затрат по TCO (Total Cost of Ownership) на 3 года;
- стоимость внедрения;
- стоимость лицензий;
- стоимость ТП на 3 года;

Технико-коммерческое предложение должно включать:

- описание ПО (лицензий) и услуг;
- план управления проектом;
- описание технической поддержки 24x7x365, в соответствии с п.10-12;
- программу и условия обучения персонала Заказчика.

Для оценки критериев совокупного владения Системой, Исполнитель должен предоставить информацию об используемых методах достижения минимального уровня TCO (Total Cost of Ownership) за счет предлагаемого решения, функционала и уникальных решений производителя сроком на не менее 5 лет.

10 Гарантийные обязательства

10.1 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.

10.2 Период опытной эксплуатации должен составлять 1 (один) месяц и

исчисляться со дня подписания Сторонами акта сдачи – приемки работ.

10.3 Период сервисной поддержки со стороны Исполнителя/Вендора должен составлять 36 (тридцать шесть) месяцев, со дня ввода системы в эксплуатацию.

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

11 Условия сервисной поддержки

11.1 Исполнитель должен подтвердить наличие статуса авторизованного сервисного партнера Вендора решения на территории Республики Узбекистан.

11.2 Исполнитель должен предоставить единый номер службы технической поддержки.

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:

- через веб-сайт компании Исполнителя;
- по бесплатному на территории Узбекистана телефону;
- по электронной почте.

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

Заявка		**Критический**	**Сильное влияние**	**Слабое влияние**	**Запрос на информацию**
Техническое сопровождение	Режим обслуживания	24x7	24x7	8x5	8x5
	Время реакции (не более)	30 мин	30 мин	60 мин	60 мин
	Время восстановления	4 часа	8 часов	24 часа	-
	Время решения*	24 часа	48 часов	30 РД	30 РД

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 неисправности Заказчиком, технической поддержки Исполнителя, в течение которого инженеры Исполнителя должны приступить к процедуре выявления неисправности.
- **Время восстановления** – промежуток времени с момента уведомления о возникшей неисправности Заказчиком технической поддержки Исполнителя, до момента восстановления полноценного функционирования оборудования,

или поиска обходного решения, позволяющего снизить влияние возникшей неисправности на системы Заказчика.

- **Время решения** - означает промежуток времени с момента уведомления Заказчиком технической поддержки Исполнителя, до момента предоставления Заказчику решения по устранению проблемы.

12 Дополнительные требования

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.

13 Перечень приложений

Перечень приложений не предъявляется.

14 Матрица распределения ответственности при оказании Услуг

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, решить оставаться ли на новом программном обеспечении или откатиться на старое программное обеспечение	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)

Разработано: _____ Е.А. Яцкевич

Согласовано:

Заместитель генерального директора по технике и ИТ _____ А.Р. Абдурахманов

Директор по безопасности _____ М.М. Чудин

Директор по ИТ ДИТ ТБ _____ А.Б. Стеклянов

Начальник отдела ДИТ ТБ _____ Р.А. Абдульваат

Начальник отдела управления проектами ДУП ТБ _____ Ф.Ш. Садыкбаев