

«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.

«02» июля

2025г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

**на поставку, установку и запуск в коммерческую эксплуатацию системы
управления действий привилегированных пользователей (РАМ)
в 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..... | 4 |
| 5 | Назначение Системы и технические требования к ней..... | 5 |
| 6 | Требования к Исполнителю | 12 |
| 7 | Требования к безопасности выполнения работ и оказания услуг | 13 |
| 8 | Требования по передаче технических и иных документов по результатам выполненных работ и оказанных услуг | 13 |
| 9 | Требования к обучению персонала Заказчика..... | 13 |
| 10 | Гарантийные обязательства..... | 13 |
| 11 | Условия сервисной поддержки и техническое сопровождение..... | 14 |
| 12 | Требования к лицензированию Системы | 15 |
| 13 | Иные требования к работам, услугам и условиям их оказания | 16 |
| 14 | Используемые термины и сокращения..... | 17 |
| 15 | Перечень приложений..... | 17 |

1 Общие сведения

В настоящем Техническом задании описаны требования к Система управления действий привилегированных пользователей – Privileged Access Management (PAM), 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 управления действий привилегированных пользователей – Privileged Access Management (PAM) (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 комплекса Системы управления действий привилегированных пользователей – Privileged Access Management (PAM).

1.2 Цели использования выполняемых работ и оказываемых услуг

Основная цель проекта – это внедрение на инфраструктуре ООО «UMS» инструмента контроля и управления действиями привилегированных пользователей, который в свою очередь будет решать следующие задачи:

- 1) автоматизация защиты, управления и организации консолидированного доступа к критически важным системам и конфиденциальным данным;
- 2) автоматизация оперативного мониторинга активности привилегированных пользователей и предотвращения потенциально опасных действий;
- 3) автоматизация сбора статистики и анализа действий привилегированных пользователей;
- 4) автоматизация управления учётными записями привилегированных пользователей.

2 Основание для реализации проекта

Запланированный на 2025г. план развития Департамента Безопасности и Режима (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 системы PAM 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 ИТ-инфраструктуры, в которую будет интегрирована Система РАМ;
- зоны ответственности Заказчика и Исполнителя в ходе развёртывания Системы;
- количество рабочих станций, на которые будет произведена установка агентской части Системы;
- необходимый объем системных ресурсов для серверной части Системы (количество ОЗУ, количество ядер ЦП и их частота, объем жесткого диска).

3.2 Пуско-наладочные и интеграционные работы

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

- инсталляцию и конфигурацию Системы, активацию модулей необходимых для мониторинга, включая конфигурацию смежного ПО (СУБД);
- инсталляцию и конфигурацию агентов Системы на 5 рабочих станций для проведения предварительного тестирования работы ПО.

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».

5 Назначение Системы и технические требования к ней

Назначение Системы заключается в централизованном управлении учетными записями привилегированных пользователей, с расширенными возможностями.

Система должна вести полную видео и текстовую фиксацию всех действий контролируемых работников и в режиме реального времени выявлять действия, не соответствующие заданным политикам безопасности Заказчика и оповещать об этом сотрудников ИБ.

Дополнительно, Система должна использоваться:

- как средство для сбора доказательной базы при расследовании ИТ инцидентов.
- как инструмент контроля над предоставлением удаленного доступа с повышенными правами (администрирующего персонала и внешних подрядчиков) к информационным ресурсам Компании (с фиксацией записи и хранения сеансов удаленного доступа).

К Системе предъявляются следующие требования:

5.1 Требования к Системе в целом

5.1.1 Требования к структуре

Система РАМ должна иметь следующий состав:

а) Модуль управления сессиями.

Модуль управления сессиями должен обеспечивать встроенный прокси-режим для предоставления доступа привилегированным пользователям к целевым серверам и устройствам по протоколам: SSH, SCP/SFTP, Telnet, RDP, VNC, HTTP, HTTPS.

Модуль управления сессиями должен обеспечивать возможность использования не менее 30 пользователями Системы РАМ.

б) Модуль управления паролями.

Модуль управления паролями должен обеспечивать защищенное хранение учетных данных в зашифрованном виде, осуществлять периодическое изменение паролей на целевых серверах и устройствах в соответствии с заданной политикой, иметь функционал для предоставления одноразовых паролей для работы внешних систем, либо внешних пользователей.

Модуль управления паролями должен обеспечивать хранение не менее 5 000 учетных записей с распределением доступа между пользователями Системы РАМ.

в) Модуль аудита.

Модуль аудита должен обеспечивать выполнение аудита и синхронизации фактически настроенных на целевых серверах и устройствах учетных записей пользователей с учетными записями, созданными в Системе РАМ для конкретных целевых серверов и устройств, формировать отчеты по доступу, статистику по подключениям и сессиям, предоставлять возможность проведения анализа событий аудита, фильтрацию по пользователю, дате, серверу или устройству, IP-адресу, протоколу.

г) Модуль мультифакторной аутентификации.

Модуль мультифакторной аутентификации должен обеспечивать управление дополнительными факторами для подтверждения полномочий пользователей: программный и аппаратный OTP, SMS, Telegram, Push, собственное мобильное приложение, IP адрес.

Модуль мультифакторной аутентификации должен обеспечивать возможность использования таким же количеством пользователей Системы РАМ, как и Модуль управления сессиями.

е) Модуль управления доступа к данным.

Модуль управления доступа к данным должен обеспечивать встроенный функционал организации доступа к целевым базам данных привилегированными пользователям по протоколам СУБД: Oracle, MS SQL Server, PostgreSQL, MySQL и др.

Модуль управления доступом должен обеспечивать возможность подключения к не менее 5 серверам управления базами данных.

f) Модуль управления доступом к сетевым устройствам по протоколам RADIUS

Модуль управления доступом к сетевым устройствам по протоколам RADIUS должен обеспечивать единый AAA сервис (аутентификация, авторизация, аккаунтинг) для сетевых устройств в инфраструктуре Заказчика.

Модуль управления доступом к сетевым устройствам по протоколам RADIUS должен обеспечивать предоставление AAA сервиса, к не менее 300 сетевых устройств.

Возможность создания произвольных ресурсов с помощью написания пользовательского коннектора. Данный коннектор должен позволять самим написать без привлечения интегратора и производителя ПО. Доступ и документация для разработки пользовательского коннектора должны быть открыты и предоставлены. Данный функционал не должен каким-либо образом лицензироваться и взимать дополнительную плату за пользования им и должен быть включен в состав РАМ

Требование к структуре Системы РАМ и ее модулям уточняются на подготовительном этапе.

5.1.2 Требования к архитектуре Системы

Система РАМ должна быть реализована с использованием отказоустойчивой архитектуры (не менее 2-х серверов). Выход из строя любого из компонентов Системы РАМ не должен приводить к остановке сервисов Системы РАМ. Между компонентами Системы РАМ должна быть настроена постоянная репликация (синхронизация данных). При этом каждый компонент должен являться полноценным функциональным элементом и обеспечивать работу и выполнение всех возложенных на него функций при отказе (выключении) одного из них. Показатель доступности Системы РАМ должен составлять – не менее 99.95%.

Сервера Системы РАМ должны быть размещены на разных хостах используемых систем виртуализации. Кластеризация и дублирование компонентов без дополнительного лицензирования. Поддержка работы в распределенной инфраструктуре (филиалы, ЦОДы).

Поддерживаемые режимы отказоустойчивой конфигурации:

- Active-active
- Active-passive

Система РАМ должна поддерживать возможность работы пользователей с целевыми серверами и устройствами, расположенными на разных площадках Заказчика (региональные офисы Заказчика), как из внутренней сети, так и посредством сети Интернет.

Поддерживаемая среда установки: физические и виртуальные сервера, облако Universal Mobile Systems».

Архитектура Системы РАМ должна исключать возможность прямого доступа привилегированных пользователей к целевым серверам и устройствам за счет разграничения прав доступа на сетевом уровне и на уровне серверов и устройств, за исключением случаев сбоя Системы РАМ и необходимости обеспечения непосредственного (Bypass) доступа администраторов к серверам и устройствам.

Архитектура Системы РАМ должна предусматривать выделенные серверы для хранения записи сессий привилегированных пользователей (не менее 2-х серверов).

Требование к архитектуре Системы РАМ уточняются на подготовительном этапе.

5.1.3 Требования к способам подключения к сессиям:

- С помощью веб-консоли
- С помощью десктопного клиента от производителя РАМ

5.1.4 Требования к установке РАМ:

- Наличие мастера установки (визарда)

- Наличие мастера обновлений
- Наличие мастера конфигураций

5.1.5 Требования к вычислительным ресурсам для функционирования

Техническое обеспечение (вычислительные ресурсы) для функционирования Системы РАМ предоставляются Заказчиком в соответствии с рекомендациями Исполнителя по результатам подготовительного этапа и разработки целевой архитектуры Системы РАМ.

Программные компоненты Системы РАМ должны позволять выполнять установку и работу в среде виртуализации VMware ESX 7.0 и новее.

5.2 Требования к функциям (задачам), выполняемым Системой РАМ

Система РАМ должна выполнять следующие функции (задачи):

5.2.1 Требования к сервисам авторизации

- а) реализация RADIUS-сервера для сетевых устройств;
- б) возможность подключения к серверам и устройствам по принципу единого входа (Single-Sign-On) через веб-портал.

Архитектура Системы РАМ должна реализовывать схему доступа Single-Sign-On таким образом, чтобы привилегированные пользователи могли получить доступ к серверам и устройствам как по своим локальным и/или доменным учетным записям, так и с возможностью подмены учетной записи пользователя на технологическую (специальную) учетную запись с правами привилегированного пользователя без отображения пароля в процессе доступа к серверам и устройствам.

5.2.2 Требования к веб-порталу Системы РАМ

- а) работа в режиме прокси-сервера без установки агентского ПО на сервера и устройства (включая АРМ пользователей);
- б) обеспечение возможности подключения привилегированного пользователя к серверам и устройствам через веб-портал Системы РАМ (далее -- веб-портал) с использованием веб-браузера;
- в) применение протокола HTTPS как при доступе к веб-порталу Системы РАМ, так и при доступе к серверам и устройствам таким образом, что отображение графического интерфейса управления серверами и устройствами передается в режиме защищенной веб-сессии по протоколу HTTPS от серверов Системы РАМ к АРМ привилегированных пользователей;
- г) поддержка работы с последними версиями веб-браузеров (Microsoft Edge, Google Chrome);
- д) аудит действий администраторов и пользователей Системы РАМ.

5.2.3 Требования к управлению пользователями

- а) предоставление возможности реализации ролевой модели доступа пользователей к консоли управления Системы РАМ без ограничения количества пользователей и ролей;
- б) поддержка групп пользователей (создание, удаление, изменение, управление членством пользователей в группе, назначение прав доступа к серверам и устройствам).
- в) Система должна иметь возможность создания новых кастомных ролей с произвольным набором прав доступа к функциям системы: количество новых ролей не должно быть ограничено, количество функций не должно быть ограничено в рамках возможностей РАМ к данным ролям. Например, администраторы одного филиала должны иметь другие права, чем администраторы другого филиала

5.2.4 Требования к управлению паролями и ключами пользователей

- а) централизованное, безопасное хранение учетных записей;
- б) обновление и ротация паролей в соответствии с заданной политикой;
- в) генерация паролей с учетом заданной политики сложности паролей;
- г) использование механизма одноразовых паролей;
- д) формирование отчетов по использованию учетных записей;

- f) поиск локальных учетных записей для заданного диапазона IP-адресов серверов и устройств;
- g) хранение истории изменения паролей (фактов изменения паролей);
- h) управление SSH-ключами, включая хранение и изменение на целевых серверах и устройствах;
- i) возможность создания и управления учетными записями с использованием API;
- j) Система РАМ должна предоставлять возможность пользователю изменять пароли учетной записи в интегрированных с решением серверах и устройствах в зоне его ответственности;
- k) Система РАМ должна позволять пользователю сбросить или восстановить забытый пароль с помощью разных механизмов.
- l) Система РАМ должна обладать функционалом настройки сложности генерируемого случайного и устанавливаемого вручную администратором Системы пароля для учетных записей: длина, используемые символы, запрет использования спецсимволов в начале пароля, максимальное число последовательных спецсимволов, запрещенные и обязательные символы, количество предыдущих паролей, которые нельзя использовать повторно, запрет использования пробела.

5.2.5 Требования к мультифакторной авторизации

- a) возможность использования мультифакторной аутентификации при подключении привилегированного пользователя к серверам и устройствам через веб-портал Системы РАМ с применением собственного мобильного приложения для получения программного или аппаратного кода OTP;
- b) встроенные механизмы применения мультифакторной авторизации при доступе к Системе РАМ с возможностью применения одноразового пароля (OTP) в собственном мобильном приложении для мобильных платформ на базе операционных систем iOS и Android на алгоритме SHA-512;
- c) предоставление доступа без раскрытия пароля привилегированной учетной записи. Привилегированная сессия на целевом ресурсе должна открываться прозрачно для пользователя без возможности получить пароль используемой учетной записи в явном виде;
- d) поддержка алгоритма TOTP (RFC6238), совместимого с другими мобильными приложениями, на алгоритме SHA-512;
- e) поддержка аппаратных TOTP токенов;
- f) поддержка отправки SMS кодов;
- g) поддержка Telegram;
- h) поддержка Push в собственном мобильном приложении;
- i) подключение должно реализовываться через двухфакторную аутентификацию с различными вариантами:
 - Вариант №1:
 - 1. Первый фактор: системный пароль пользователя
 - 2. Второй фактор: одноразовый пароль (OTP), генерируемый аппаратным токеном eToken Pass или аналогом
 - Вариант №2:
 - 1. Первый фактор: системный пароль пользователя
 - 2. Второй фактор: одноразовый пароль (OTP) мобильного единого собственного приложения
 - Вариант №3:
 - 1. Первый фактор: системный пароль пользователя
 - 2. Второй фактор: Push уведомление мобильного приложения
 - Вариант №4:
 - 1. Первый фактор: системный пароль пользователя
 - 2. Второй фактор: SMS

- Вариант №5:

1. Первый фактор: системный пароль пользователя
2. Второй фактор: Telegram OTP.

5.2.6 Требования к контролю доступа пользователей

а) контроль доступа привилегированных пользователей к серверам и устройствам с использованием протоколов SSH, SFTP, TELNET, RDP, VNC, HTTP, HTTPS в том числе с использованием нестандартных сетевых портов;

б) возможность подключения по протоколу SSH с помощью односторонней команды, когда все параметры кроме пароля указываются в командной строке.

в) обеспечение возможности изменения сетевых портов, используемых для подключения к серверам и устройствам, на произвольные (настраиваемые администратором Системы РАМ);

г) обеспечение одновременного доступа к одному и тому же серверу, и устройству для не менее 20 пользователей;

д) управление доступом в рамках сессий привилегированных пользователей к веб-ресурсам по протоколам HTTP/HTTPS на уровне доступа к URL-адресам;

е) управление доступом в рамках сессий привилегированных пользователей к веб-ресурсам по протоколам HTTP/HTTPS на уровне доступа к контенту веб-ресурса (блокировка доступности определенных страниц веб-ресурса).

5.2.7 Требования к контролю доступа по протоколу SSH

а) обеспечение возможности подключения привилегированного пользователя к серверу или устройству по протоколу SSH с использованием установленного на АРМ пользователя ПО SSH-клиента (Putty, SecureCRT, MobaXterm, встроенный SSH-клиент Windows, iTerm2, консольный клиент OpenSSH);

б) при работе по протоколу SSH возможность контролируемой передачи файлов между сервером или устройством и АРМ пользователя с использованием протокола передачи файлов SFTP.

5.2.8 Требования к контролю доступа по протоколам RDP и VNC:

а) обеспечение изменения расширения экрана при доступе к графическим интерфейсам по протоколам RDP и VNC, просмотр в режиме «полного экрана»;

б) при работе по протоколу RDP возможность контролируемой передачи файлов между сервером и АРМ пользователя;

в) при работе по протоколу RDP возможность использования и контроля использования буфера обмена как локального АРМ пользователя, так и удаленного сервера.

г) для RDP подключений в системе должна иметься возможность запретить или разрешить доступ в терминальной сессии к следующим локальным ресурсам: нативный запрет проброса смарт-карт и аудиоустройств, локальные диски, буфер обмена, принтеры, порты. Необходимо для применения в распределенной инфраструктуре чтобы не создавать сложности с единообразным применением политик безопасности

д) должна быть возможность кастомизировать параметры RDP-файлов, используемых для подключения к ресурсам.

5.2.9 Требования к контролю доступа к серверам управления базами данных

а) поддержка нативных протоколов подключений к различным СУБД MySQL, MS SQL Server, PostgreSQL, Oracle с подключением с использованием ПО клиентов СУБД (DBeaver, NaviCat, DataGrip, MySQL Workbench, PL/SQL Developer, MS SQL Server Management Studio, pgAdmin и др.);

б) логирование SQL-запросов (текстов запросов и команд), выполняемых пользователями, при подключениях к различным СУБД MySQL, MS SQL Server, PostgreSQL, Oracle.

5.2.10 Требования к контролю доступа к сетевым устройствам по протоколу RADIUS

а) обеспечение взаимодействия сетевых устройств с Системой РАМ по протоколам

RADIUS для организации AAA-сервиса;

б) обеспечение аутентификации пользователей при входе на сетевые устройства без создания локальных учетных записей с помощью обращения по протоколу RADIUS Системе РАМ с выдачей соответствующего уровня привилегий в рамках сессии доступа на сетевые устройства;

с) обеспечение обработки и получения данных аккаунтинга от сетевых устройств по протоколам RADIUS и хранение журналов.

5.2.11 Требования к контролю, записи, просмотру и анализу сессий привилегированных пользователей

а) контекстный поиск по списку введенных команд пользователя в журналах действий в рамках сессий доступа привилегированных пользователей к серверам и устройствам по протоколам RDP, VNC, SSH, TELNET;

б) непрерывная запись действий привилегированных пользователей при подключении к серверам и устройствам (видеозапись, логирование введенных команд) по протоколам RDP, VNC, SSH, TELNET;

с) Поддержка возможности ведения разных типов записей сеансов доступа для разных учетных записей. Например, для администраторов домена – видеозапись и текстовую запись, для администраторов БД – снятие скриншотов.

д) Наличие встроенного видеоплеера в РАМ для просмотра сессий, без необходимости установки сторонних приложений. Отсутствие зависимости от сторонних инструментов для просмотра и анализа записей

е) просмотр записи действий привилегированных пользователей в формате эмуляции видео за указанный администратором интервал времени;

ф) фильтрация вводимых привилегированными пользователями команд в рамках сессий доступа к серверам на базе ОС семейства Linux/Unix, сетевые устройства и др.;

г) фильтрация вводимых привилегированными пользователями команд в рамках сессий доступа к серверам и устройствам по протоколам SSH (сервера на базе ОС семейства Linux/Unix, сетевые устройства и др.);

h) контроль активных сессий в режиме реального времени;

и) просмотр активности и действий пользователя (листинг команд, видеозапись RDP/VNC-сессий и SSH/TELNET-сессий) в выбранный временной промежуток;

j) возможность дополнительного контроля действий в рамках сессий доступа привилегированных пользователей к серверам и устройствам по протоколам RDP, VNC, SSH, TELNET, обеспечивающая механизмы просмотра активной сессии в рамках реального времени, прерывание активной сессии в рамках реального времени, отправку уведомлений привилегированному пользователю;

к) возможность дополнительного контроля действий в рамках сессий доступа привилегированных пользователей к серверам и устройствам по протоколам SSH, обеспечивающая механизмы блокировки команд по спискам разрешенных и запрещенных команд;

l) механизмы согласования выполнения привилегированных команд и действий в рамках сессий администрирования с ответственным за эксплуатацию серверов или устройств администратором;

m) наличие функционала многоуровневого контроля подключений к серверам и устройствам (многоуровневое согласование доступа);

n) возможность экспорта команд пользователя для указанного сервера или устройства за выбранный интервал времени (в рамках разных сессий) и/или в рамках выбранной сессии с отметкой времени ввода соответствующих команд;

о) возможность экспорта записей сессий пользователей в видеофайл формата MPEG4 для

передачи на анализ внешнему аудиту.

5.2.12 Требования к контролю передачи файлов и использования буфера обмена

а) контроль разрешений на передачу данных (файлов) в рамках сессий привилегированных пользователей;

б) теневое копирование файлов, передаваемых в рамках сессии привилегированных пользователей.

5.3 Требования к характеристикам взаимосвязей создаваемой Системы РАМ со смежными системами, требования к ее совместимости

В процессе создания Системы РАМ должна быть выполнена интеграция с существующими системами Заказчика:

- интеграция с системой идентификации пользователей Заказчика (Active Directory, LDAP);
- интеграция с сервисом DNS в инфраструктуре Заказчика;
- интеграция с сервисом резервного копирования;
- интеграция с сервисом точного времени (NTP);
- должна присутствовать возможность интеграции со сторонними решениями посредством API, Syslog, RADIUS;
- должна присутствовать возможность интеграции и взаимодействие со следующими классами решений:

- SIEM, по таким требованиям:
 - Через Syslog с передачей в режиме реального времени
 - Форматы отправляемого лога: LEEF, CEF.
 - Фильтрация лога перед отправкой.
- ITDR, по таким требованиям:
 - Через Syslog с передачей в режиме реального времени
 - Форматы отправляемого лога: LEEF, CEF.
- IDM, по таким требованиям:
 - Автоматическое создание учетных записей сотрудников в хранилищах аутентификационной информации при приеме сотрудника на работу;
 - Ограничение доступа в приложения в период отпуска или болезни сотрудника;
 - Ограничение или прекращение доступа после издания приказа об увольнении или отстранении сотрудника;
 - В области управления и контроля доступа к ресурсам и в помещения компании.
- MFA, по таким требованиям:
 - Возможность интеграции системы аутентификации в систему контроля доступа привилегированных учетных записей с использованием стандарта RADIUS;
 - Должен поддерживаться механизм RADIUS Challenge-Response;
 - Поддержка обязательных технологий аутентификации для второго фактора.
- Обязательно наличие собственного единого мобильного приложения для Android и iOS систем многофакторной аутентификации и контроля доступа привилегированных учетных записей
- Сборщик логов:
 - Возможность отправки текстового лога сессии по протоколу Syslog.

Требования по интеграции со смежными системами и сервисами, а также их перечень уточняются на подготовительном этапе.

5.4 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).

5.5 Требования к численности и квалификации персонала поставщика

Для обеспечения поставки программного комплекса и запуска рабочего функционирования Системы в составе персонала Поставщика/Исполнителя 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.

5.6 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 логи, не менее чем за 1 месяц, с возможностью их экспорта.

5.7 Требования к языку интерфейса.

Система должна обладать интерфейсом на русском и английском языках.

6 Требования к Исполнителю

К Исполнителю предъявляются следующие требования:

6.1 В рамках закупочной процедуры Исполнитель должен предоставить информацию:

- детальную спецификацию с разбиением стоимости на ПО (лицензии), работы и интеграцию, обучение, техническую поддержку;
- срокам поставки и пуско-наладки Системы;
- срокам интеграции в существующую инфраструктуру ООО «UMS»;
- условиям и стоимости послегарантийной сервисной технической поддержки;
- возможности дальнейшего увеличения числа привилегированных пользователей ООО «UMS»;
- особенностям предлагаемого технического решения.

6.2 Общие требования к Исполнителю

Исполнитель должен удовлетворять следующим требованиям:

- подтвержденный опыт работы по предоставлению обозначенных услуг, не менее чем 3 года;
- являться авторизованным партнёром или производителем, а также иметь документальное подтверждение на распространение конечным пользователям прав на использование и внедрение реализуемого/внедряемого программного обеспечения;
- Исполнитель обязуется предоставить гарантийное письмо о намерении прохождения экспертизы, либо сертификат о прохождении экспертизы на соответствие требованиям обеспечения информационной и кибербезопасности, полученный в ГУП «Центр кибербезопасности».

- не являться неплатежеспособным или банкротом, находится в процессе ликвидации, не должен быть наложен арест, экономическая деятельность Исполнителя не должна быть приостановлена;

- иметь в наличии не менее 2 (двух) сертифицированных специалистов, обладающих квалификацией 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 Участник должен включить в состав предложения следующие документы, подтверждающие его соответствие вышеуказанным требованиям:

- копию авторизованного письма (MAF);
- копии минимум 2х сертификатов инженеров от компании производителя;
- перечень собственных проектов за последние 3 года;
- копию лицензий на оказание услуг по данному направлению.

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

В рамках проекта Исполнитель готовит Рабочий проект на Систему РАМ в печатном виде, в 2 экземплярах, а также в электронном виде, в формате PDF.

Для всех компонентов решения Участник должен предоставить следующую информацию:

- общее описание технического решения, с описанием преимуществ 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);
- информацию (в виде презентации) по методам достижения минимального уровня TCO (Total Cost of Ownership) за счет предлагаемого в проекте оборудования, функционала и т.п. уникальных решений производителя. Участник должен провести презентацию предлагаемого решения в г. Ташкент.

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 установленного программного обеспечения.

Срок гарантии на выполненные работы по внедрению системы РАМ, должен составлять **12 (двенадцать) 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 – **12 месяцев**, с момента внедрения Системы. 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 Системы должны включать в себя:

а) Обеспечение непрерывного функционирования серверной части системы мониторинга действий привилегированных пользователей:

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

- настройка параметров компонента для оптимизации использования внутренних ресурсов (политики, определяющие алгоритмы оценки риска)

- настройка параметров БД для обеспечения наиболее эффективного процесса хранения и выборки данных;

- настройка параметров Системы для обеспечения полноценного функционирования данного компонента;

- настройка параметров Системы для управления политикой безопасности с ударением на приложения;

- тестирование работы компонентов системы в штатном режиме после проведения обновлений.

б) Обеспечение непрерывного функционирования клиентской части Системы:

- настройка автоматического составления полного списка всех выполненных изменений приложения для внутренних и внешних требований в соответствии с требованиями ООО «UMS»;

- генерация автоматизированных отчетов аудита и соблюдения соответствия правилам;

- настройка отслеживания изменений политик сетевой безопасности;

- тестирование работы клиентских компонентов Системы в штатном режиме после проведения обновлений.

с) Настройка очистки и оптимизации наборов правил, планирования изменений и выявление потенциально опасных и не обеспечивающих соответствия правила.

д) Интеграция с существующими системами управления изменениями.

е) Консультации по масштабированию Системы.

ф) Расширенный доступ к русскоязычному portalу (возможность скачивать обновления, доступ к форуму, доступ к русскоязычной документации и постоянно обновляемому набору русскоязычных правил, отчетов, мониторов данных и т.д.). без ограничений по количеству пользователей. Документация должна быть доступна онлайн и в открытом доступе без

регистрации: руководство администратора и пользователя, руководство по установке и настройке Системы, API-документация, инструкции по установке, обновлению.

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

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

i) Восстановление работоспособности программного комплекса:

- восстановление работоспособности системы в штатном режиме не позднее, чем через 12 часов 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 РАМ на время сбоя (Bypass) для проведения восстановительных работ;

- восстановление активности отдельных компонентов программного комплекса, возникших вследствие нештатных ситуаций (аппаратные сбои, потеря питания);

- операции восстановления данных из резервных копий. Предоставление отчетов о проделанной работе.

Сервисная поддержка должна производиться квалифицированными специалистами производителя.

Сервисная поддержка производителя должна предоставляться в режиме **24/7/365** на русском или узбекском языках

- Сервисная поддержка должна предоставлять и включать следующие виды услуг:
 - Не ограниченное количество обращений в ТП
 - Не ограниченное кол-во пользователей, имеющих доступ к технической поддержке
 - Предоставление новых версий Системы, вышедших в период действия договора технической поддержки
 - Решение инцидентов, связанных с работой Системы.
 - Оказание консультаций по эксплуатации Системы.
 - Предоставление доступа к “Базе знаний” - возможность просмотра базы часто встречающихся проблем и вопросов, возникающих при внедрении и эксплуатации Системы.
- Сервисная поддержка должна оказываться по следующим каналам:
 - Телефон горячей линии. Заявки должны приниматься круглосуточно без выходных
 - Web-система приема заявок. Заявки должны приниматься круглосуточно без выходных
 - Электронная почта
 - ВКС
- SLA:
 - Ответ на критичные инциденты — ≤ 4 часа.
 - Для инцидентов средней серьезности (частичная потеря функциональных возможностей - единичные ошибки, при этом основные функции Системы не нарушены) - 24 (двадцать четыре) рабочих часа.

12 Требования к лицензированию Системы

Perpetual (бессрочная) лицензия на **30** пользователей Системы, кто получает доступ к ресурсам, без ограничений по количеству активных подключений к Системе, без ограничений целевых систем к которым пользователи получают доступ.

Техническая поддержка уровня 24/7/365 должна быть включена в лицензию на 12 месяцев.

Должна быть предоставлена возможность смены типа лицензирования, если в ходе эксплуатации Системы возникнет такая необходимость на такие виды лицензирования как:

- По количеству активных подключений в Системе.
- По количеству ресурсов, к которым пользователи получают доступ.

Кластеризация и дублирование всех компонентов РАМ не должны дополнительно лицензироваться, без дополнительных финансовых оплат

Количество выдаваемых инсталляций (дистрибутивов) не должно лицензироваться и ограничиваться, Лицензия должна выдаваться на суммарное количество пользователей Системы которые должны пользоваться РАМ

Отсутствие штрафных санкций и дополнительных финансовых обязательств для ООО «Universal Mobile Systems» в случае несвоевременного продления ТП

13 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 лицензий на ПО.

Детальная форма подачи предложения представлена в Приложении №1 к данному ТЗ.

13.1 Требование к комплектации

Система/ПО должна иметь полную комплектацию, в которую входит весь перечень заказываемых программных средств необходимых для полноценного функционирования предлагаемого решения в рамках текущего ТЗ. Стоимость продукта/ПО должна формироваться исходя из полной комплектации.

13.2 Требование к интеграции

Интеграция должна учитывать особенности работы инфраструктуры Заказчика.

13.3 Сведения о новизне

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

13.4 Страхование

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

13.5 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 |

Форма предложения

| Описание | Количество | Стоимость |
|---|------------|-----------|
| Программное обеспечение (ПО) и Лицензии, в составе: | | |
| Лицензии и ПО | | |
| Работы по внедрению ПО, в составе: | | |
| Работы по разработке, инсталляции и конфигурированию системы. | | |
| Работы по интеграции с системами Заказчика | | |
| Обучение сотрудников Заказчика | | |
| Гарантийная поддержка | 12 мес | |

| | | |
|--|---|---|
| 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)

14 Используемые термины и сокращения

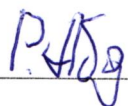
| Сокращение | Расшифровка сокращения |
|-----------------------------|---|
| ТЗ | Техническое задание |
| ПО | Программное обеспечение |
| ИС | Информационная система |
| ИТ | Информационные технологии |
| АПК | Программно-аппаратный комплекс |
| РАМ | Система управления действий привилегированных пользователей |
| БД | База данных |
| ККД | Компонент контроля действий |
| ИБ | Информационная безопасность |
| ОТР | Сокращение от One Time Password (одноразовый пароль) |
| RADIUS | Протокол сетевого доступа |
| Single-Sign-On | Технология единого входа |
| АРМ | Автоматизированное рабочее место |
| RFC6238 (TOTP) | TOTP (Time-based one-time Password algorithm) |
| Putty, SecureCRT, MobaXterm | SSH-клиент |
| RDP и VNC | Протоколы удаленного доступа |

15 Перечень приложений

Приложение №1 – Форма подачи предложения.

Разработано:

Начальник отдела информационной безопасности ДИБиР


подпись

Абдульваат Р.А.

Директор ДИБиР


подпись

Олматов Б.А.