

«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 по информационной безопасности
и режиму ООО «UMS»



 Олматов Б.А.
03» июня 2026г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на поставку, установку и запуск в эксплуатацию
Системы защиты конечных узлов (конечных точек) EDR/XDR
для нужд ООО «UNIVERSAL MOBILE SYSTEMS»

Ташкент – 2026

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	10
7	Требования к безопасности выполнения работ и оказания услуг	11
8	Требования по передаче технических и иных документов по результатам выполненных работ и оказанных услуг	11
9	Требования к обучению персонала Заказчика	12
10	Гарантийные обязательства	12
11	Условия сервисной поддержки и техническое сопровождение	12
12	Требования к технической поддержке	13
13	Иные требования к работам, услугам и условиям их оказания	14
14	Используемые термины и сокращения	15
15	Перечень приложений	16

1 Общие сведения

В настоящем Техническом задании описаны требования к Системе защита конечных узлов (конечных точек) EDR/XDR (далее - Система, ИС), достаточные для описания требований Заказчика к составу ПО, с целью объявления тендера и/или конкурса на приобретение ПО 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 защита конечных узлов (конечных точек) EDR/XDR (далее по тексту – Система).

Работы проводятся на инфраструктуре и площадке Заказчика.

В рамках данного Технического задания Исполнитель должен предоставить коммерческое предложение на поставку ПО, интеграцию и запуск в эксплуатацию программного комплекса EDR/XDR.

1.2 Цели использования выполняемых работ и оказываемых услуг

Основная цель проекта – это внедрение на инфраструктуре ООО «UMS» ПО Системы защиты конечных узлов (конечных точек) EDR/XDR.

Основные задачи, решаемые Системой:

- обнаружение сложных кибератак и аномалий на конечных точках и в сетевой инфраструктуре;
- централизованный сбор, корреляция и анализ телеметрии безопасности из различных источников;
- раннее выявление целевых атак, вредоносной активности и попыток компрометации;
- снижение времени обнаружения и реагирования на инциденты информационной безопасности;
- автоматизация реагирования на инциденты и минимизация влияния атак на бизнес-процессы;
- повышение прозрачности инцидентов за счёт визуализации цепочек атак и контекста угроз;
- поддержка расследования инцидентов и цифровой форензики;
- повышение общего уровня защищённости ИТ-инфраструктуры ООО «UMS».

Основное назначение Системы – это обеспечение централизованного обнаружения, анализа и реагирования на инциденты информационной безопасности в ИТ-инфраструктуре ООО «UMS», с целью минимизации рисков киберугроз и снижения их влияния на бизнес-процессы.

2 Основание для реализации проекта

Запланированный на 2026г. план развития Департамента безопасности и режима (утвержденный Бизнес план и Бюджет ООО «UMS» на 2026 год).

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

Внедрение Системе защита конечных узлов (конечных точек) EDR/XDR должно проводиться совместно с ответственными лицами Заказчика, без нарушения работоспособности существующей ИТ-инфраструктуры Заказчика, с предварительным поверхностным обследованием имеющихся устройств. 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;
- зоны ответственности Заказчика и Исполнителя в ходе развёртывания Системы;
- количество конечных точек, 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 программной части Системы;
- интеграцию в сетевую инфраструктуру Заказчика;
- 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 представителями 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 Системы 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 технические требования.

5.1 Архитектура и модель поставки

5.1.1 Решение должно относиться к классу Extended Detection and Response (XDR) и обеспечивать корреляцию событий безопасности из конечных точек, сетевых источников и облачных сред в рамках единой платформы.

5.1.2 Платформа должна поддерживать централизованную консоль управления с возможностью работы в режиме 24×7.

5.1.3 Допускается использование облачной модели (SaaS) при условии:

- изоляции данных Заказчика;
- размещения данных в сертифицированных дата-центрах;
- использования шифрования данных при передаче и хранении.

5.1.4 Архитектура решения должна обеспечивать горизонтальное масштабирование без остановки сервисов.

5.2 Защита конечных точек (Endpoint Protection & EDR)

5.2.1 Решение должно обеспечивать защиту конечных точек (Windows, Linux, macOS) с использованием:

- поведенческого анализа;
- машинного обучения;
- анализа цепочек атак.

5.2.2 Агент конечной точки должен объединять функции предотвращения, обнаружения и реагирования без необходимости установки отдельных компонентов.

5.2.3 Должны поддерживаться следующие функции:

- предотвращение эксплуатации уязвимостей;
- защита от файловых и безфайловых атак;
- защита от вредоносных скриптов;
- детектирование атак типа ransomware.

5.2.4 Агент должен обладать низким потреблением системных ресурсов и поддерживать автоматическое обновление.

5.3 XDR-корреляция и аналитика

5.3.1 Решение должно обеспечивать автоматическую корреляцию телеметрии из различных источников безопасности в рамках единого инцидента.

5.3.2 Должна поддерживаться аналитика, основанная на:

- поведенческих моделях;
- машинном обучении;
- анализе тактик, техник и процедур (TTP) атакующего.

5.3.3 Платформа должна обеспечивать визуализацию цепочки атаки (attack storyline) с указанием первичного вектора компрометации и последующих шагов злоумышленника.

5.3.4 Должен быть реализован механизм снижения количества ложноположительных срабатываний за счёт автоматической корреляции и контекстного анализа.

5.4 Интеграция с сетевой безопасностью

Должна обеспечиваться возможность автоматической блокировки сетевых соединений, IP-адресов и доменов в рамках сценариев реагирования.

5.5 Реагирование и автоматизация (SOAR-функции)

5.5.1 Решение должно обеспечивать автоматизированные сценарии реагирования на инциденты безопасности с более чем 100 готовыми плейбуками от производителя, включая:

- изоляцию конечной точки;
- завершение вредоносных процессов;
- блокировку файлов по хэшу;
- сбор форензик-артефактов.

5.5.2 Должна поддерживаться возможность создания кастомных сценариев реагирования без написания программного кода.

5.5.3 Реагирование должно быть доступно как в автоматическом, так и в ручном режимах.

5.6 Threat Intelligence

5.6.1 Решение должно использовать глобальные источники киберугроз, обновляемые в режиме, близком к реальному времени.

5.6.2 Должна поддерживаться автоматическая корреляция инцидентов с актуальными индикаторами компрометации (IoC).

5.6.3 Платформа должна обеспечивать обогащение инцидентов контекстной информацией об угрозах без необходимости подключения сторонних сервисов.

5.7 Управление, отчётность и аудит

5.7.1 Платформа должна обеспечивать:

- ролевую модель доступа (RBAC);
- аудит действий пользователей;
- хранение всей собираемой сервисной информации о событиях (телеметрии) не менее 30 дней, хранение истории инцидентов до 12 месяцев.

5.7.2 Должна поддерживаться возможность формирования:

- оперативных дашбордов;
- отчётов для руководства отдела ИБ;
- выгрузки данных в внешние SIEM-системы.

5.7.3 Интерфейс управления должен поддерживать английский язык.

5.8 Интеграция с ИТ-инфраструктурой

5.8.1 Решение должно поддерживать интеграцию с:

- с платформы поддерживающие REST API;
- Active Directory / LDAP;
- с внешними Syslog Receivers для отправки оповещений и логов аудита

5.8.2 Наличие публичного, документированного REST API обязательно.

5.9 Эксплуатационные требования

– обновления сигнатур, моделей детектирования и компонентов аналитики должны выполняться автоматически.

– решение должно обеспечивать непрерывную защиту при обновлении компонентов.

– Вендор должен обеспечивать техническую поддержку не ниже уровня 24×7

5.10 Возможности удаленного подключения

Предлагаемое решение должно обеспечивать возможность запуска командной строки с полной поддержкой команд на конечном устройстве, через соединение в режиме реального времени.

5.11 Сертификация:

Предлагаемое решение должно иметь сертификацию ISO 27001.

5.12 Контроль устройств

Предлагаемое решение должно:

- обеспечивать управление шифрованием для операционных систем Windows и macOS;
- обеспечивать функции контроля USB-устройств для операционных систем Windows и macOS.

5.13 Требования к производительности и масштабируемости

5.13.1 Решение должно обеспечивать стабильную обработку телеметрии от:

- не менее 10 000 конечных точек в рамках одного логического тенанта;
- с возможностью последующего масштабирования без изменения архитектуры.

5.13.2 Платформа должна поддерживать потоковую обработку событий безопасности в режиме, близком к реальному времени.

5.13.3 Производительность аналитических и корреляционных механизмов не должна снижаться при:

- включении поведенческого анализа;
- использовании машинного обучения;
- активации автоматических сценариев реагирования.

5.13.4 Агент конечной точки не должен потреблять в среднем более:

- 5% CPU в штатном режиме;
- 500 МБ оперативной памяти;
- 1 ГБ дискового пространства.

5.13.5 Решение должно обеспечивать отказоустойчивость компонентов аналитики и управления без потери данных и телеметрии.

5.14 Требования к интеграции с ИТ- и ИБ-системами

5.14.1 Интеграция с системами управления учетными записями

а) Решение должно поддерживать интеграцию с:

- Microsoft Active Directory;
- LDAP-совместимыми каталогами.

б) Интеграция должна обеспечивать:

- получение информации о пользователях, группах и ролях;
- корреляцию событий безопасности с учетными записями пользователей;
- использование данных каталогов для построения контекста инцидентов.

с) Должна поддерживаться автоматическая синхронизация учетных записей без необходимости ручного администрирования.

5.14.2 Интеграция с SIEM системой

а) Решение должно обеспечивать двустороннюю интеграцию с внешними SIEM-системами, включая:

- передачу инцидентов и алертов;
- передачу обогащённых событий;

б) Интеграция должна быть реализована через:

- REST API;
- Syslog;
- нативные коннекторы.

с) Решение должно поддерживать использование в качестве:

- источника событий для SIEM;
- автономной XDR-платформы без обязательного подключения SIEM.

5.14.3 Интеграция должна обеспечивать:

- получение телеметрии безопасности;

- выявление фишинговых атак и компрометации учетных записей/

5.14.4 API и расширяемость

- d) Решение должно предоставлять публичный, документированный REST API для:
 - получения событий и инцидентов;
 - управления объектами защиты;
 - запуска сценариев реагирования.
- e) API должно поддерживать:
 - аутентификацию по токенам;
 - разграничение прав доступа;
 - журналирование обращений.
- f) Использование API и интеграций не должно требовать приобретения дополнительных лицензий.

5.14.5 Автоматизация и оркестрация

- g) Решение должно поддерживать интеграцию с ITSM-системами для:
 - автоматического создания инцидентов;
 - передачи статусов расследования;
 - закрытия инцидентов по результатам реагирования.
- h) Должна поддерживаться возможность использования интеграций в рамках:
 - автоматических playbook-ов;
 - полуавтоматических сценариев реагирования.
- i) Интеграции должны настраиваться через графический интерфейс без написания программного кода.

5.14.6 Лицензирование и комплект поставки

5.14.6.1 Лицензирование решения должно осуществляться по количеству защищаемых конечных точек с возможностью гибкого увеличения лицензируемого объёма.

5.14.6.2 В стоимость лицензии должны быть включены:

- функции предотвращения атак на конечных точках;
- функции обнаружения и реагирования (EDR/XDR);
- централизованная консоль управления;
- аналитика на основе машинного обучения и поведенческих моделей;
- встроенные сценарии автоматического реагирования;

5.14.6.3 Дополнительная оплата за:

- корреляцию инцидентов;
- визуализацию цепочек атак;
- автоматическое реагирование;
- базовые отчёты и дашборды

не допускается.

5.14.6.4 Лицензия должна включать право использования решения:

- в круглосуточном режиме;
- без ограничений на количество инцидентов и событий.

5.14.6.5 В рамках лицензии должно предоставляться:

- регулярное обновление сигнатур;
- обновление аналитических моделей;
- обновление функциональных компонентов платформы.

5.14.6.6 Лицензия должна включать:

- техническую поддержку уровня 24×7;
- доступ к базе знаний и рекомендациям по реагированию.

5.14.6.7 Лицензирование не должно зависеть от:

- объема обрабатываемого трафика;
- количества аналитических правил;
- числа пользователей консоли управления.

5.14.6.8 Срок действия подписки – не менее 36 месяцев с возможностью продления.

5.14.6.9 Должна поддерживаться возможность приобретения лицензий сроком 36 месяцев.

5.15 Количественные требования к XDR-решению

№	Показатель	Требование
1	Количество защищаемых конечных	не менее 2000
2	Готовые правила детектирования	не менее 350
3	Готовые сценарии реагирования	не менее 50
4	Автоматическое построение цепочек	обязательно
5	Потребление ресурсов агентом (CPU)	не более 5 % в штатном режиме
6	Лицензирование по конечным точкам	обязательно, без ограничений по событиям и объему информации, собираемой с конечных
7	SLA доступности платформы	не менее 99,9 %

5.16 Требования к взаимодействию со сторонними информационными системами.

Система должна поддерживать виртуальную инфраструктуру VMware ESXi для развертывания программного компонента (виртуальный аплайанс), предназначенный для агрегации, предварительной обработки и безопасной передачи данных от локальных источников и сегментированных сетей в консоль управления

5.17 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);
- автономный режим (в случае отсутствия связи между компонентами системы или с внешними сетями, для доступа к конфигурационной и архивной информации).

5.18 Требования к численности и квалификации персонала Исполнителя.

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

5.19 Требования к аудиту, мониторингу и отчетности

Система должна обеспечивать аудит действий пользователей и администраторов, регистрацию событий безопасности и эксплуатации, а также мониторинг состояния и доступности компонентов.

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

Все события должны журналироваться с указанием даты и времени, источника и результата действия.

Должна быть обеспечена защита журналов от несанкционированного изменения и удаления.

Отчёты должны быть доступны по запросу и/или по расписанию, с возможностью экспорта в стандартные форматы (PDF, CSV).

Срок хранения аудиторских и мониторинговых данных (логов) – не менее 12 месяцев.

5.20 Решение должно поддерживать возможность контроля уязвимостей и использования сетевого сканера уязвимостей на базе промежуточного (прокси) сервера от производителя для выполнения сканирование сети и активов без установленных агентов.

5.20.1 Решение должно поддерживать расширение в рамках единой платформы для контроля уязвимостей:

- содержать алгоритмы ранжирования критичности, которые учитывают наличие защитных механизмов (активные правила предотвращения платформы обнаружения и реагирования), способных автоматически блокировать эксплуатацию конкретной уязвимости;

- обеспечивать автоматический сбор данных об уязвимостях из сторонних сканеров уязвимостей и их интеграцию в единую систему управления уязвимостями;

- содержать специальную панель мониторинга для визуализации наиболее критичных рисков, динамики изменения уровня риска во времени и прогресса их устранения;

- обеспечивать автоматизированные встроенные плейбуки для устранения уязвимостей, включая поддержку полностью автоматизированных действий для устранения критических уязвимостей без ручного вмешательства;

- предоставлять визуализацию «путей атаки», показывающую, какие уязвимости на конкретных узлах могут быть использованы для продвижения злоумышленника внутри сети;

- предоставлять механизм оценки риска уязвимостей, учитывающий не только оценку CVSS, но и наличие признаков эксплуатации данной уязвимости EPSS;

- возможность добавления дополнительного модуля для контроля внешней поверхности атаки и оценки внешних уязвимостей и векторов атак извне, коррелируемых с другими угрозами в рамках единой платформы;

- содержать возможность автоматического сопоставления обнаруженных уязвимостей с активными инцидентами ИБ, зафиксированными на платформе обнаружения и реагирования.

5.21 Решение должно поддерживать возможность контроля передачи данных в LLM и облачные хранилища и предотвращения утечек данных на конечных точках в рамках единой платформы управления угрозами и единого агента, устанавливаемого на конечные точки.

5.22 Решение должно поддерживать возможность применения специального модуля для выявления и удаления фишинговых писем за счет продвинутого анализа содержимого при помощи AI на предмет намерений, содержащихся в письме

6 Требования к Исполнителю

6.1 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 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».

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.

6.2 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.

6.3 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

При выполнении работ предъявляются следующие требования по безопасности:

7.1 Все работы по установке, настройке и вводу в эксплуатацию программного комплекса должны выполняться в соответствии с требованиями электробезопасности, а также действующими внутренними нормативными документами.

7.2 Исполнитель несет полную ответственность за соблюдение требований информационной безопасности в процессе выполнения работ.

7.3 Работы допускается выполнять исключительно в согласованные сроки и временные окна, утверждённые Заказчиком.

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

После завершения внедрения и ввода Системы в промышленную эксплуатацию Исполнитель обязан подготовить рабочую (исполнительную) документацию, отражающую фактически реализованное состояние Системы.

Документация предоставляется:

- в 2 (двух) экземплярах на бумажном носителе;
- в электронном виде (форматы: DOCX и PDF).

Обязательный состав документации:

- общее описание Системы;
- архитектурные и сетевые схемы;
- перечень и конфигурация программных компонентов;
- описание интеграций с инфраструктурой Заказчика;
- сетевая адресация (IP, порты, протоколы);
- краткая эксплуатационная документация;
- описание реализованных мер информационной безопасности.

Документация должна быть актуальной, полной и соответствовать фактической реализации Системы, а также достаточной для её эксплуатации без привлечения Исполнителя.

9 Требования к обучению персонала Заказчика

В рамках данного ТЗ, Исполнитель обеспечивает следующие программы обучения;

а) сертифицированное обучение двух специалистов ИБ Заказчика по администрированию данного комплекса.

Количество слушателей: 2 человека.

Формат: очное / онлайн, с практическими занятиями.

Язык обучения: русский / английский.

Материалы: презентации, инструкции, лабораторные работы.

По итогам обучения Исполнитель предоставляет:

- учебные материалы;
- записи занятий;
- подтверждение прохождения обучения (сертификаты).

б) обучение пользователей системы.

Количество слушателей: до 10 человек.

Формат: демонстрационный + практический.

Цель обучения: освоение функциональных возможностей системы.

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 программного обеспечения, установленных производителем в документации и отсутствия несанкционированного вмешательства в работу установленного 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 действия подписки на ПО – **36 (тридцать шесть) месяцев**.

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 (тридцать шесть) месяцев**, с момента внедрения ПО. Сервисная поддержка на программные компоненты должна оказываться как производителем, так и Исполнителем.

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 сервисному сопровождению ПО должны включать в себя:

а) Обеспечение непрерывного функционирования программной части Системы EDR/XDR:

- настройка параметров Системы для оптимизации использования аппаратных

(серверных) ресурсов Заказчика;

- настройка параметров Системы для управления политикой безопасности;
- тестирование работы Системы в штатном режиме после проведения обновлений.

b) Интеграция с существующими системами управления и мониторинга Заказчика.

c) Консультации по масштабированию Системы.

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

e) Проведение инструктажа 2-х администраторов Системы в случае обновления Системы.

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

g) Восстановление работоспособности Системы:

- 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 (режим байпас);

- восстановление активности Системы, после программных сбоев, потеря питания, и т.д.;

- операции восстановления данных из резервных копий.

- предоставление отчетов о проделанной работе.

12 Требования к технической поддержке

12.1 Исполнитель обязан обеспечить техническую поддержку поставляемого программного комплекса в течение 36 месяцев.

12.2 Поддержка должна оказываться производителем ПО либо авторизованным сервисным партнером производителя.

12.3 Уровень поддержки должен предусматривать возможностью эскалации на уровень производителя (L3).

12.4 Поддержка должна распространяться на:

- программную часть (software).

12.5 Поддержка должна предоставляться в режиме:

- 24×7×365 – для критичных инцидентов;
- не ниже 8×5 – для некритичных (по согласованию с Заказчиком).

12.6 Время реакции на инциденты:

- Критический (P1): не более 15–30 минут;
- Высокий (P2): не более 1 часа;
- Средний (P3): не более 4 часов;
- Низкий (P4): не более 1 рабочего дня.

12.7 Время восстановления (или обходного решения):

- P1: не более 4 часов;
- P2: не более 8 часов;
- P3: до 2 рабочих дней;
- P4: по согласованию с Заказчиком.

12.8 Исполнитель должен предоставлен единый канал регистрации заявок на ТП:

- Service Desk (portal);
- телефон горячей линии;

- e-mail.

13 Иные требования к работам, услугам и условиям их оказания

13.1 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.

13.2 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.

13.3 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.

13.4 Требование к интеграции

Интеграция должна учитывать особенности работы инфраструктуры Заказчика.

13.5 Сведения о новизне

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

13.6 Страхование

Требования не предъявляются.

13.7 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)

14 Используемые термины и сокращения

Сокращение	Расшифровка сокращения
ТЗ	Техническое задание
ПО	Программное обеспечение
ИС	Информационная система
ИТ	Информационные технологии
БД	База данных
ИБ	Информационная безопасность
WEB	World Wide Web
Endpoint	Конечное устройство (сервер, рабочая станция, виртуальная машина), на котором установлен агент EDR/XDR
Agent	Программный модуль, устанавливаемый на endpoint и обеспечивающий сбор телеметрии, защиту и взаимодействие с платформой EDR/XDR
EDR	Endpoint Detection and Response
NGFW	Next-Generation Firewall
SOC	Security Operations Center
SIEM	Security Information and Event Management
IOC	Indicator of Compromise
MITRE ATT&CK	База знаний о тактиках и техниках злоумышленников. Используется для классификации инцидентов
Malware	Вредоносное программное обеспечение
Ransomware	Тип вредоносного ПО, осуществляющий шифрование данных с целью выкупа
Phishing	Метод социальной инженерии, направленный на получение конфиденциальных данных
Lateral Movement	Перемещение злоумышленника внутри инфраструктуры после первоначальной компрометации
Prevention	Механизмы предотвращения угроз до их исполнения
Detection	Процесс выявления подозрительной или вредоносной активности
Response	Автоматизированные или ручные действия по локализации и устранению угрозы
Incident	Подтвержденное событие информационной безопасности, оказывающее влияние на активы компании
SLA	Соглашение об уровне сервиса (время реакции, доступность и т.д.)
MTTR	Mean Time To Respond (Среднее время реагирования на инцидент)
MTTD	Mean Time To Detect (Среднее время обнаружения инцидента)
RBAC	Role-Based Access Control (Модель разграничения доступа на основе ролей)
API	Application Programming Interface (Интерфейс программного взаимодействия систем)
Application Programming Interface	Transport Layer Security (Криптографический протокол защиты сетевых соединений)
CVE	Common Vulnerabilities and Exposures (Общепринятый идентификатор уязвимостей информационной безопасности)
VM	Virtual Machine (Виртуальная машина)
Cloud Console	Облачная консоль управления XDR, размещенная в инфраструктуре производителя

Telemetry	Совокупность данных, передаваемых агентами для анализа и корреляции событий
Policy	Набор правил и настроек безопасности, применяемых к endpoint или группе устройств

15 Перечень приложений

Приложение №1 – Характеристика объекта информатизации.

Приложение №2 – Таблица соответствия техническим требованиям.

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 рабочих станций (endpoints) – не более 1500 шт.

Общее количество серверов (Windows, Linux, в т.ч. виртуальных) – не более 500 шт.

Таблица соответствия

№ требования	Наименование требования/ технические характеристики
1	ПО должно поставляться сроком на 3 года (подписка, включая тех.поддержку)
2	Решение должно относиться к классу Extended Detection and Response (XDR)
3	Платформа поддерживает централизованную консоль управления с возможностью работы в режиме 24×7.
4	При поставке SaaS модели должны соблюдаться условия: - изоляции данных Заказчика; - размещения данных в сертифицированных дата-центрах; - использования шифрования данных при передаче и хранении.
5	Архитектура решения обеспечивает горизонтальное масштабирование без остановки сервисов.
6	Обязательно наличие следующих функций: - предотвращение эксплуатации уязвимостей; - защита от файловых и безфайловых атак; - защита от вредоносных скриптов; - детектирование и предотвращение атак типа ransomware
7	Наличие автоматической корреляции телеметрии из различных источников безопасности
8	Система обеспечивает визуализацию цепочки атаки
9	Решение поддерживает нативную интеграцию с сетевыми средствами защиты (межсетевые экраны, системы предотвращения вторжений)
10	Решение поддерживает автоматическую блокировку сетевых соединений, IP-адресов и доменов в рамках сценариев реагирования
11	Интеграция должна быть реализована без использования сторонних брокеров данных.
12	Решение обеспечивает автоматизированные сценарии реагирования на инциденты безопасности с более чем 100 готовыми плейбуками от производителя, включая: - изоляцию конечной точки; - завершение вредоносных процессов; - блокировку файлов по хэшу; - сбор форензик-артефактов.
13	Решение поддерживает возможность создания кастомных сценариев реагирования без написания программного кода.
14	Решение использует глобальные источники киберугроз, обновляемые в режиме, близком к реальному времени.
15	Решение поддерживает автоматическую корреляция инцидентов с актуальными индикаторами компрометации (IoC).
16	Решение поддерживает: - ролевую модель доступа (RBAC); - аудит действий пользователей; - хранение всей собираемой сервисной информации о событиях (телеметрии) не менее 30 дней, хранение истории инцидентов до 12 месяцев

17	<p>Решение поддерживает формирование:</p> <ul style="list-style-type: none"> - оперативных дашбордов; - отчётов для руководства отдела ИБ; - выгрузки данных в внешние SIEM-системы.
18	<p>Решение должно поддерживать возможность контроля уязвимостей и использования сетевого сканера уязвимостей на базе промежуточного (прокси) сервера от производителя для выполнения сканирование сети и активов без установленных агентов.</p> <p>Решение должно поддерживать расширение в рамках единой платформы для контроля уязвимостей:</p> <ul style="list-style-type: none"> - содержать алгоритмы ранжирования критичности, которые учитывают наличие защитных механизмов (активные правила предотвращения платформы обнаружения и реагирования), способных автоматически блокировать эксплуатацию конкретной уязвимости; - обеспечивать автоматический сбор данных об уязвимостях из сторонних сканеров уязвимостей и их интеграцию в единую систему управления уязвимостями; - содержать специальную панель мониторинга для визуализации наиболее критичных рисков, динамики изменения уровня риска во времени и прогресса их устранения; - обеспечивать автоматизированные встроенные плейбуки для устранения уязвимостей, включая поддержку полностью автоматизированных действий для устранения критических уязвимостей без ручного вмешательства; - предоставлять визуализацию «путей атаки», показывающую, какие уязвимости на конкретных узлах могут быть использованы для продвижения злоумышленника внутри сети; - предоставлять механизм оценки риска уязвимостей, учитывающий не только оценку CVSS, но и наличие признаков эксплуатации данной уязвимости EPSS; - возможность добавления дополнительного модуля для контроля внешней поверхности атаки и оценки внешних уязвимостей и векторов атак извне, коррелируемых с другими угрозами в рамках единой платформы; - содержать возможность автоматического сопоставления обнаруженных уязвимостей с активными инцидентами ИБ, зафиксированными на платформе обнаружения и реагирования.
19	<p>Решение поддерживает интеграцию с:</p> <ul style="list-style-type: none"> - Active Directory / LDAP; - с платформы поддерживающие REST API; - с внешними Syslog Receivers для отправки оповещений и логов аудита.
20	Поддерживается автоматическая синхронизация учетных записей без необходимости ручного администрирования
21	В решении доступно REST API
22	<p>В процессе эксплуатации должен выполняться следующий функционал:</p> <ul style="list-style-type: none"> - обновления сигнатур, моделей детектирования и компонентов аналитики должны выполняться автоматически, - решение должно обеспечивать непрерывную защиту при обновлении компонентов, - Вендор должен обеспечивать техническую поддержку не ниже уровня 24×7.
23	Решение должно поддерживать возможность удаленного подключения к конечной точке
24	Решение должно иметь сертификацию ISO 27001
25	<p>Решение должно обладать следующими функциями по контролю устройств:</p> <ul style="list-style-type: none"> - обеспечивать управление шифрованием для ОС Windows и macOS - обеспечивать функции контроля USB-устройств для ОС Windows и macOS. - обладать возможностью блокировки Bluetooth-устройств. - обладать возможностью запрета печати на определенных устройствах.

26	Решение обеспечивает стабильную обработку телеметрии от: - не менее 10 000 конечных точек в рамках одного логического тенанта; - с возможностью последующего масштабирования без изменения архитектуры.
27	Решение должно поддерживать возможность контроля передачи данных в LLM и облачные хранилища и предотвращения утечек данных на конечных точках в рамках единой платформы управления угрозами и единого агента, устанавливаемого на конечные точки.
28	Агент конечной точки не должен потреблять в среднем более: - 5% CPU в штатном режиме; - 500 МБ оперативной памяти; - 1 Гб дискового пространства.
29	Решение должно обеспечивать отказоустойчивость компонентов аналитики и управления без потери данных и телеметрии.
30	Решение должно поддерживать возможность применения специального модуля для выявления и удаления фишинговых писем за счет продвинутого анализа содержимого при помощи AI на предмет намерений, содержащихся в письме
31	Интеграция должна обеспечивать: - получение информации о пользователях, группах и ролях; - корреляцию событий безопасности с учетными записями пользователей; - использование данных каталогов для построения контекста инцидентов.
32	Обеспечивается двустороннюю интеграцию с внешними SIEM-системами, включая: - передачу инцидентов и алертов; - передачу обогащённых событий.
33	Поддержка интеграции через: - REST API; - Syslog; - нативные коннекторы.
34	Решение возможно использовать в качестве: - источника событий для SIEM; - автономной XDR-платформы без обязательного подключения SIEM.
35	Интеграция должна обеспечивать: - получение телеметрии безопасности; - выявление фишинговых атак и компрометации учетных записей.
36	Решение должно предоставлять публичный, документированный REST API для: - получения событий и инцидентов; - управления объектами защиты; - запуска сценариев реагирования.
37	API поддерживает: - аутентификацию по токенам; - разграничение прав доступа; - журналирование обращений.
38	Решение должно поддерживать интеграцию с системами класса ITSM для: - автоматического создания инцидентов; - передачи статусов расследования; - закрытия инцидентов по результатам реагирования.
39	Должна поддерживаться возможность использования интеграций в рамках: - автоматических playbook-ов; - полуавтоматических сценариев реагирования.

40	Лицензирование решения должно осуществляться по количеству защищаемых конечных точек с возможностью гибкого увеличения лицензируемого объема
41	В стоимость лицензии должны быть включены: - функции предотвращения атак на конечных точках; - функции обнаружения и реагирования (EDR/XDR); - централизованная консоль управления; - аналитика на основе машинного обучения и поведенческих моделей; - встроенные сценарии автоматического реагирования.
42	Дополнительная оплата не допускается за следующий функционал: - корреляцию инцидентов; - визуализацию цепочек атак; - автоматическое реагирование; - базовые отчёты и дашборды.
43	Лицензия должна включать право использования решения: - в круглосуточном режиме; - без ограничений на количество инцидентов и событий
44	В рамках лицензии должно предоставляться: - регулярное обновление сигнатур; - обновление аналитических моделей; - обновление функциональных компонентов платформы.
45	Лицензия должна включать: - техническую поддержку уровня 24×7; - доступ к базе знаний и рекомендациям по реагированию.
46	Лицензирование не должно зависеть от: - объема обрабатываемого трафика; - количества аналитических правил; - числа пользователей консоли управления.
47	- 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); автономный режим (в случае отсутствия связи между компонентами системы или с внешними сетями).
48	- Требования к численности и квалификации персонала Исполнителя, для обеспечения поставки программного комплекса и запуска рабочего функционирования системы: в составе персонала 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.
49	- Требования к аудиту, мониторингу и отчетности система должна обеспечивать аудит действий пользователей и администраторов, регистрацию событий безопасности и эксплуатации, а также мониторинг состояния и доступности компонентов; система должна иметь поддержку аудита в реальном времени с возможностью отправки оповещений при выявлении подозрительной активности; все события должны фиксироваться с указанием даты и времени, источника и результата действия; система должна быть обеспечена защита журналов от несанкционированного изменения и удаления; отчёты должны быть доступны по запросу и/или по расписанию, с возможностью экспорта в стандартные форматы (PDF, CSV).

	срок хранения аудиторских и мониторинговых данных (логов) – не менее 12 месяцев
50	Количество защищаемых конечных точек – не менее 2000
51	В проект включены инсталляционные работы и проектирование
52	В проект включено проектирование
53	В проект включено обучение специалистов Заказчика
54	В проект включена сертификация ПО в ЦКБ
55	Наличие у Исполнителя МАФ