

«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.

« ____ » _____ 2026г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на поставку, установку и запуск в эксплуатацию

Изолированной системы для безопасного исполнения файлов
(Песочница/Sandbox) для нужд ООО «UNIVERSAL MOBILE SYSTEMS»

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	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	11
10	Гарантийные обязательства	12
11	Условия сервисной поддержки и техническое сопровождение	12
12	Требования к технической поддержке аппаратного комплекса	13
13	Иные требования к работам, услугам и условиям их оказания	14
14	Используемые термины и сокращения	15
15	Перечень приложений	15

1 Общие сведения

В настоящем техническом задании описаны требования к изолированной системе для безопасного исполнения файлов (Песочница/Sandbox) (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: Изолированной системе для безопасного исполнения файлов (Песочница/Sandbox) (далее по тексту – Система).

Работы проводятся на инфраструктуре и площадке Заказчика.

В рамках данного Технического задания Исполнитель должен предоставить коммерческое предложение на поставку АПК, монтаж, интеграцию и запуск в эксплуатацию аппаратно-программного комплекса Sandbox.

1.2 Цели использования выполняемых работ и оказываемых услуг

Основная цель проекта – внедрение системы динамического анализа вредоносного кода для повышения уровня защищенности информационной инфраструктуры Заказчика.

Основные задачи, решаемые Системой:

- детектирование вредоносного и ранее неизвестного (Zero-day) ПО;
- анализ поведения объектов в эмулируемой операционной среде;
- формирование отчётов о выявленных индикаторах компрометации (IOC);
- интеграцию с существующими средствами защиты (SIEM, EDR/XDR, почтовые шлюзы, NGFW);
- автоматическая передача результатов анализа в системы реагирования;
- повышение общего уровня защищённости ИТ-инфраструктуры ООО «UMS».

Основное назначение Системы – выявление, анализ и предотвращение целевых и неизвестных киберугроз, путём изолированного запуска и поведенческого анализа подозрительных файлов, ссылок, вложений и объектов сетевого трафика в контролируемой виртуальной среде.

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 изолированной системы для безопасного исполнения файлов (Sandbox), 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;
- типы подключаемых интерфейсов;
- зоны ответственности Заказчика и Исполнителя в ходе развёртывания Системы.

3.2 Пуско-наладочные и интеграционные работы

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

- установку и конфигурацию аппаратной 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 соответствие 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 приемочные 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, установку 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 Общие требования

5.1.1 Решение должно относиться к классу Sandbox/Advanced Malware Analysis.

5.1.2 Предназначение Системы – выявление неизвестного вредоносного ПО (zero-day), АРТ-угроз и целевых атак в виде загруженных исполняемых файлов.

5.1.3 Поддержка развертывания:

- On-Premise (программно-аппаратного комплекса с поддержкой установки в стандартную телекоммуникационную стойку),
- возможность интеграции с облачными сервисами Вендора Системы.

5.1.4 Поддержка работы в изолированном сегменте.

5.1.5 Возможность масштабирования по производительности.

5.2 Функциональные требования

5.2.1 Методы анализа

- Возможность идентификации в режиме реального времени фишинговых сайтов нулевого дня, включая спам и сайты, содержащие вредоносное ПО.
- Поддержка обнаружения сетевых угроз в режиме сниффера. Выявление деятельности ботнетов и сетевых атак, посещений вредоносных URL-адресов.
- Обеспечение проверки объектов посредством антивирусного сканирования;
- Поддержка отправки файлов и URL-адресов устройствами в SOC.
- Поддержка интеграции с NGFW, в части протоколов: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM и их эквивалентные версии с SSL-шифрованием.
- Поддержка интеграции с почтовой защитой, в части протоколов: SMTP, POP3, IMAP.
- Поддержка интеграции с решением по защите конечных точек, в части протоколов: HTTP, FTP, SMB.
- Поддержка интеграции с WAF, в части протоколов: HTTP, HTTPS.
- Поддержка режима сниффера. HTTP, FTP, POP3, IMAP, SMTP, SMB.
- Возможность проверки прокси через ICAP.
- Возможность работы в режиме MTA/BCC через SMTP.
- Поддержка режима сканирования сетевых общих хранилищ через FTP, sFTP, CIF, NFS.
- Наличие JSON API для автоматизации загрузки образцов и индикаторов вредоносного ПО для исправления ситуации.
- Удаленное и защищенное хранение логов с помощью серверов CEF и серверов syslog и возможность отправки в SIEM.
- Возможность отправки файлов с интегрированного устройства (устройств).
- Возможность развертывания режима сниффера с поддержкой TCP RST для сброса соединения клиента с подозрительным сервером.
- Возможность сканирования сетевых ресурсов с поддержкой больших файлов (например, ISO-образов, общих сетевых папок, SMB/NFS).

- Поддержка высокой доступности с первичным и вторичным узлами для резервирования.
- Мониторинг портов для обеспечения отказоустойчивости кластера.
- Возможность кластеризации узлов для повышения пропускной способности.
- Поддержка агрегированных интерфейсов для увеличения пропускной способности и резервирования.
- Изоляция административного трафика от трафика образов виртуальных машин.
- Возможность настройки интеллектуального адаптивного профиля сканирования, оптимизирующего ресурсы "песочницы" в зависимости от представленных материалов.
- Поддержка параллельного сканирования для одновременного запуска нескольких различных типов VM.
- Возможность извлечения и сканирование файлов, встроенных в документы.
- Возможность извлечения и сканирования URL-адреса, встроенные в документы и QR-коды.
- Возможность извлечения и сканирования изображений в документах с помощью OCR.
- Поддержка интеграции с правилами сторонних производителей Yara.
- Возможность задавать параметры белого и черного списков контрольных сумм файлов.
- Поддержка сканирования URL-адресов из отправленных писем и файлов.
- Мониторинг коэффициента сканирования VM для эффективного использования VM.
- Обеспечивает проверку объектов посредством эмуляции в виртуальной среде (динамический анализ) с целью выявления поведенческих признаков, характерных для вредоносного ПО.
- Поддержка поведенческого анализа на основе искусственного интеллекта.
- Поддержка одновременных экземпляров песочницы.
- Поддерживаемые типы ОС: Windows 11/10, Linux, MacOS, Android.
- Поддержка настраиваемых виртуальных машин для ОС Windows и Linux.
- Настраиваемый интернет-браузер с поддержкой Internet Explorer, Microsoft Edge, Google Chrome и Mozilla Firefox.
- Поддержка интерактивного режима "песочницы", видеозапись взаимодействия с вредоносным ПО и скриншоты VM.

5.2.2 Необходимые техники обнаружения обходов:

- Обфускация API;
- Обнаружение bare-metal;
- Command and Control;
- Прямые системные вызовы;
- Задержка выполнения;
- Payload только для памяти;
- Инъекции в процессы;
- Шифрование/пакинг во время выполнения;
- Слепки системы;
- Time Bomb;
- Проверка пользовательских файлов;

- Проверка взаимодействия с пользователем;
- Обнаружение виртуальных машин и песочниц;
- Поддержка обнаружения обратных вызовов;
- Посещение вредоносных URL-адресов, связь с C&C ботнета и трафик

злоумышленников от активированного вредоносного ПО.

- Загружаемые перехваченные пакеты, журналы трассировки и скриншоты.
- Наличие сводки угроз на основе искусственного интеллекта с использованием

собранных показателей и результатов.

• Наличие виджетов на панели для подключения и служб, статуса лицензии, производительности сканирования, ресурсы системы.

• Наличие страницы производительности сканирования для отслеживания исторического использования.

• Наличие виджетов мониторинга в режиме реального времени. Статистика результатов сканирования, активность сканирования (за определенное время), топ целевых хостов, топ вредоносных программ, топ зараженных URL, топ доменов обратного вызова.

• Наличие средства просмотра событий с раскрытием. Динамическая таблица, включающая действия, название вредоносной программы, рейтинг, тип, источник, пункт назначения, время обнаружения и путь загрузки.

• Поддержка отчетов и логов. Графический интерфейс, загрузка PDF и необработанный файл журнала.

- Возможность формирование подробного отчета о выполнении задания.

• Возможность создания периодических логов состояния системы, производительности, статистики сканирования и использования системных ресурсов.

- Поддержка MITRE ATT&CK v1.1.

• Возможность загрузки журналы трассировки, PCAP и индикаторов в формате STIX 2.0.

• Возможность отправки уведомлений по электронной почте при обнаружении вредоносного файла.

• Возможность создания еженедельных отчетов для глобальных списков электронной почты и администраторов.

• Возможность создания TAC-отчет для получения полной информации о конфигурации и состоянии системы.

- Возможность конфигурирования через графический интерфейс и CLI.

• Поддержка нескольких учетных записей администратора, поддерживающих полный доступ или доступ только для просмотра.

- Поддержка аутентификации Radius для администраторов.

- Поддержка SAML для единого входа в систему.

- Наличие виджета самопроверки конфигураций, подключений и служб.

• Наличие страницы управления кластером для администрирования НА и узлов кластера.

• Наличие централизованная страница поиска, позволяющая администраторам создавать индивидуальные условия поиска.

- Возможность загрузки любой лицензии с одной удобной страницы.

- Мониторинг состояния виртуальных машин.

- Возможность автоматического обновления движка и сигнатур.

- Возможность автоматической проверки наличия нового образа виртуальной машины.
- Наличие системы оповещения о проверке работоспособности системы.
- Поддержка резервного копирования, восстановления и проверки конфигурации системы.
- Наличие консолидированного CLI для поиска и устранения неисправностей.
- Наличие опции в режиме сканирования сетевых дисков для определения приоритета и пересылки файлов стороннему сканирующему устройству для дальнейшего сканирования.

5.2.3 Поддержка типов файлов

- Исполняемые файлы Windows: .bat, .cab, .cmd, .dll, .exe, .js, .msi, .ps1, .vbs, .vbe, .wsf.
- Microsoft Office: .doc, .docm, .docx, .dot, .dotm, .dotx, .ics, .iqy, .one, .pot, .potm, .potx, .ppt, .pptm, .pptx, .ppam, .pps, .ppsm, .ppsx, .pub, .rtf, .sldm, .sldx, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx.
- Файлы документов и электронной почты: .eml, .pdf, .rl.
- Файлы для Android: .apk.
- Файлы Linux: .elf, .sh, ObjectFiles.
- Файлы MacOS: .app, .dmg, Mach-O.
- Веб-файлы: .asp, .hta, .htm, .html, .lnk, .js, .lnk, .url, WEBLink.
- Сжимайте файлы: .7z, .ace, .arj, .bz2, .gz, .iso, .jar, .kgb, .lzh, .rar, .swf, .tar, .tgz, .udf, .upx, .xz, .z, .zip.
- Определяемые пользователем расширения.

5.2.4 Поддержка ОС для эмуляции

Обязательная поддержка следующих типов ОС:

- Windows (несколько версий, включая актуальные);
- Linux (Redhat, OEL, Ubuntu, CentOS);
- поддержка 32/64-bit;
- возможность кастомизации виртуальных образов.

5.3 Интеграционные требования

5.3.1 Интеграция с сетевой инфраструктурой Заказчика

Система должна поддерживать интеграции с:

- файрволами (NGFW);
- шлюзом электронной почты (Email Gateway);
- системой SIEM (после внедрения Заказчиком).

Обмен данными должен поддерживать:

- REST API;
- стандарт STIX;
- Syslog.

5.4 Производительность Системы

- 5.4.1 Производительность по числу локальных виртуальных машин на устройстве: не менее 14.
- 5.4.2 Эффективная пропускная способность песочницы: не менее 10 000 файлов в час.
- 5.4.3 Производительность проверки объектов посредством предварительной фильтрации (статический анализ): не менее 20 000 файлов в час.

- 5.4.4 Производительность проверки объектов посредством эмуляции в виртуальной среде (динамический анализ): не менее 500 файлов в час.
- 5.4.5 Производительность при интеграции с решением для защиты почты: 100 000 писем в час.
- 5.4.6 Производительность проверки объектов посредством MTA Adapter 25 000 писем в час.
- 5.4.7 Производительность в режиме снифера: не менее 500 Мбит/с.

5.5 Технические характеристики и емкость АПК:

- Общий объем хранимой информации: не менее 960 ГБ;
- Сетевые интерфейсы: не менее 4 портов 1Гбит/с разъем RJ-45;
- Блок питания: 100–240V AC, 60–50 Hz;
- Наличие TPM.

5.6 Управление и администрирование Системы

- WEB-интерфейс управления;
- разграничение ролей (ролевая модель);
- журналирование действий администраторов;
- интеграция с AD/LDAP;
- поддержка двухфакторной аутентификации для администраторов Системы.

5.7 Отчетность Системы

Решение должно предоставлять:

- подробный поведенческий отчет:
 - файловая активность,
 - изменения реестра,
 - сетевые соединения,
 - процессы,
- визуализацию графического отображение этапов кибератаки от начала до цели,
- формирование признаков компрометации (hash, IP, URL, domain),
- экспорт отчетов в PDF.

5.8 Лицензирование Системы

- Срок действия подписки на движок песочницы: не менее 3 лет.
- Количество VM – не менее 4 шт. (с возможностью дальнейшего расширения до

14, путем активации дополнительной лицензии).

- Срок подписки на ПО – 3 года.
- Срок технической поддержки – не менее 3 лет.

5.9 Дополнительные требования

- поддержка собственных исследовательских центров от производителя;
- интеграция с платформами класса XDR.

5.10 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 детонация и анализ подозрительных файлов и объектов;

- автономный режим – при отсутствии связи между компонентами Sandbox или с внешними сетями, для доступа к конфигурационной информации и результатам ранее проведенного анализа.

5.11 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.

5.12 Требования к аудиту, мониторингу и отчетности

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

- Должна быть поддержка аудита в реальном времени с возможностью отправки оповещений при выявлении подозрительной активности или ошибок работы Sandbox.

- Все события должны журналироваться с указанием даты и времени, источника события, типа анализируемого объекта и результата анализа.

- Журналы должны быть защищены от несанкционированного изменения или удаления.

- Отчёты о результатах анализа и состоянии системы 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.

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 допускаются выполнять исключительно в согласованные сроки и временные окна, утвержденные 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 Sandbox:
 - 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.
- б) Интеграция с существующими системами управления и мониторинга Заказчика.
- в) Консультации по масштабированию Системы.
- г) Доступ к portalу производителя ПО (возможность скачивать обновления, доступ к техническому форуму, доступ к документации).
- д) Проведение инструктажа 2-х администраторов Системы в случае обновления Системы.
- е) Подключение специалиста посредством VPN по требованию ООО «UMS» для решения возникших проблем, консультаций, связанных с функционированием Системы.
- ж) 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 аппаратного комплекса

12.1 Исполнитель обязан обеспечить техническую поддержку поставляемого аппаратного комплекса в течение всего срока действия контракта.

12.2 Поддержка должна оказываться производителем оборудования либо авторизованным сервисным партнёром производителя.

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

12.4 Поддержка должна распространяться на:

- аппаратную часть (hardware);
- встроенное ПО (firmware, BIOS, контроллеры).

12.5 Поддержка должна предоставляться в режиме:

- 24×7×365 – для критичных компонентов;
- 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 Замена неисправных компонентов должна осуществляться в рамках ТП, но не более чем за 1 месяц.:

12.9 Все заменяемые компоненты должны быть:

- оригинальными (OEM);
- новыми (не восстановленными).

12.10 Исполнитель должен предоставлен единый канал регистрации заявок на ТП:

- Service Desk (портал);
- 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 АПК, программное обеспечение	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

№	Термин / Сокращение	Расшифровка	Определение
1	Sandbox	—	Система изолированного анализа подозрительных объектов в контролируемой виртуальной среде
2	Вредоносное ПО (ВПО)	—	Программное обеспечение, предназначенное для нанесения ущерба информационным системам
3	Zero-day	—	Уязвимость или вредоносное ПО, ранее неизвестное производителям средств защиты
4	IOC	Indicator of Compromise	Индикатор компрометации — технический признак присутствия вредоносной активности
5	APT	Advanced Persistent Threat	Целевая сложная атака с длительным скрытым присутствием в инфраструктуре
6	SIEM	Security Information and Event Management	Система управления событиями и информационной безопасностью
7	EDR	Endpoint Detection and Response	Система обнаружения и реагирования на инциденты на конечных устройствах
8	XDR	Extended Detection and Response	Расширенная платформа обнаружения и реагирования, объединяющая данные из разных источников
9	NGFW	Next-Generation Firewall	Межсетевой экран нового поколения с функциями DPI и анализа приложений
10	ICAP	Internet Content Adaptation Protocol	Протокол интеграции для анализа и модификации трафика
11	API	Application Programming Interface	Интерфейс программного взаимодействия между системами
12	VM	Virtual Machine	Виртуальная машина, используемая для изолированного анализа
13	Динамический анализ	—	Анализ поведения объекта в процессе его выполнения
14	Статический анализ	—	Анализ файла без его запуска
15	Поведенческий анализ	—	Метод выявления угроз на основе анализа действий программы
16	PCAP	Packet Capture	Файл захвата сетевого трафика
17	SLA	Service Level Agreement	Соглашение об уровне доступности и качества сервиса
18	SOC	Security Operations Center	Центр мониторинга и реагирования на инциденты ИБ
19	TI	Threat Intelligence	Данные о киберугрозах и индикаторах компрометации
20	On-premises	—	Размещение решения в инфраструктуре Заказчика
21	Cloud Sandbox	—	Облачная реализация системы изолированного анализа

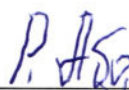
15 Перечень приложений

Приложение №1 – Характеристика объекта информатизации.

Приложение №2 – Форма технического соответствия.

ТЗ разработал:

Начальник отдела информационной безопасности ДИБиР


подпись

Абдулваат 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 серверов и виртуальных машин, откуда будет агрегироваться информация в Sandbox: 200;

Общая пропускная способность сети, связанной с Sandbox: 10 Гбит/с;

Предполагаемый объём трафика или файлов для анализа в Sandbox: 100 файлов в сутки;

Типы источников данных для Sandbox: E-mail, WEB, Endpoints, файлы.

Форма технического соответствия

№ требования	Наименование требования/ технические характеристики
1	Решение должно относиться к классу Sandbox
2	Развертывание Системы: On-Premise (программно-аппаратный комплекс)
3	ПО в составе АПК должно поставляться сроком на 3 года (по типу подписки, включая тех.поддержку)
4	Решение поддерживает следующие методы анализа угрозы: <ul style="list-style-type: none"> • возможность идентификации в режиме реального времени фишинговых сайтов нулевого дня, включая спам и сайты, содержащие вредоносное ПО; • поддержка обнаружения сетевых угроз в режиме сниффера; • выявление деятельности ботнетов и сетевых атак, посещений вредоносных URL-адресов; • обеспечение проверки объектов посредством антивирусного сканирования.
5	Обязательные типы расширения файлов: <ul style="list-style-type: none"> • исполняемые файлы Windows: .bat, .cab, .cmd, .dll, .exe, .js, .msi, .ps1, .vbs, .vbe, .wsf • microsoft Office: .doc, .docm, .docx, .dot, .dotm, .dotx, .ics, .iqy, .one, .pot, .potm, .potx, .ppt, .pptm, .pptx, .ppam, .pps, .ppsm, .ppsx, .pub, .rtf, .sldm, .sldx, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx • файлы документов и электронной почты: .eml, .pdf, .rl • файлы для Android: .apk • файлы Linux: .elf, .sh, ObjectFiles • файлы MacOS: .app, .dmg, Mach-O • веб-файлы: .asp, .hta, .htm, .html, .lnk, .js, .lnk, .url, WEblink • сжимаемые файлы: .7z, .ace, .arj, .bz2, .gz, .iso, .jar, .kgb, .lzh, .rar, .swf, .tar, .tgz, .udf, .upx, .xz, .z, .zip
6	Наличие поддержки следующих типов ОС для эмуляции: <ul style="list-style-type: none"> • Windows (несколько версий, включая актуальные); • Linux (Redhat, OEL, Ubuntu, CentOS); • поддержка 32/64-bit; • возможность кастомизации виртуальных образов.
7	Система должна поддерживать интеграции с: <ul style="list-style-type: none"> • файрволами (NGFW); • шлюзом электронной почты (Email Gateway); • Web Gateway; • антивирусом (Endpoint Protection) • системой EDR / XDR • системой SIEM (в перспективе).
8	Обмен данными должен поддерживать: <ul style="list-style-type: none"> • REST API; • стандарт STIX/; • Syslog.
9	Интеграция Системы с endpoint решениями (антивирусом) <ul style="list-style-type: none"> • возможность автоматической передачи подозрительных файлов с endpoint-агентов антивируса. • возможность автоматического блокирования признаков компрометации на конечных точках. • поддержка автоматической изоляции хоста (при наличии интеграции).

10	<p>Производительность Системы:</p> <ul style="list-style-type: none"> • производительность по числу локальных виртуальных машин на устройстве: не менее 14; • возможность расширения в облако до 80 виртуальных машин; • эффективная пропускная способность песочницы: не менее 10 000 файлов в час; • производительность проверки объектов посредством предварительной фильтрации (статический анализ): не менее 20 000 файлов в час; • производительность проверки объектов посредством эмуляции в виртуальной среде (динамический анализ): не менее 500 файлов в час; • производительность при интеграции с решением для защиты почты: 100 000 писем в час; • производительность проверки объектов посредством MTA Adapter 25 000 писем в час; • производительность в режиме снифера: не менее 500 Мбит/с.
11	<p>Управление и администрирование Системы</p> <ul style="list-style-type: none"> • WEB-интерфейс управления; • разграничение ролей (ролевая модель); • журналирование действий администраторов; • интеграция с AD/LDAP; • поддержка двухфакторной аутентификации для администраторов Системы.
12	<p>Решение предоставляет следующие отчеты:</p> <ul style="list-style-type: none"> • подробный поведенческий отчет: файловая активность, изменения реестра, сетевые соединения, процессы, • визуализацию графического отображение этапов кибератаки от начала до цели, • формирование признаков компрометации (hash, IP, URL, domain), • экспорт отчетов в PDF.
13	<p>Лицензирование Системы</p> <ul style="list-style-type: none"> • лицензия должна покрывать: количество анализируемых объектов, количество интегрируемых устройств, обновления сигнатур и движков. • количество VM – не менее 4 шт. (с возможностью дальнейшего расширения, путем активации дополнительной лицензии); • срок подписки на ПО – 3 года; • срок технической поддержки – не менее 3 лет.
14	<p>Дополнительные требования</p> <ul style="list-style-type: none"> • поддержка собственных исследовательских центров от производителя; • интеграция с платформами класса XDR
15	В проект включены инсталляционные работы
16	В проект включено проектирование
17	В проект включено обучение 2 специалистов Заказчика
18	В проект включена сертификация ПО/АПК в ЦКБ
19	Язык интерфейса - русский/английский
20	Наличие у Исполнителя MAF