**Запрос информации по Проекту**

**«Внедрение централизованной системы по контролю и управлению**

**мобильными устройствами и приложениями**

**в ПАО АФК «Система»**

**Обзор проекта:**

ПАО АФК «Система» рассматривает возможность реализации проекта **«Внедрение централизованной системы по контролю и управлению мобильными устройствами и приложениями» (далее – «Проект»).**

Требования к составу и содержанию работ указаны в Техническом задании (Приложение 1) к настоящему документу.

**Планируемый график реализации Проекта:**

ПАО АФК «Система» планирует начать работы в январе 2018 года, а завершить их не позднее декабря того же года.

**Предложение и процесс запроса информации:**

Мы ожидаем получить краткое предложение, которое должно включать:

- предлагаемое техническое решение с описанием предполагаемых работ;

- предполагаемый объем работ и график реализации Проекта;

- предложение по цене (в рублях) с учетом применимого НДС;

- данные о ключевых членах команды, предлагаемых для реализации Проекта;

- краткий обзор аналогичных проектов, которые были недавно закончены, с возможностью референса, если применимо.

**ВНИМАНИЕ!!!** Подача документов осуществляется Участником в электронном виде через электронно-торговую площадку (далее - «ЭТП») по адресу <http://utp.sberbank-ast.ru/AFK> в соответствии с регламентом и инструкцией для Участников торговой секции «Закупки» ПАО АФК «Система» универсальной торговой платформы «Сбербанк-АСТ».

Срок окончания подачи документов на участие и коммерческих предложений «10» ноября 2017 г. до 19.00 часов (МСК). **Документы и предложения, поданные после указанного срока, ЭТП не принимаются.**

Вы можете направить интересующие Вас вопросы следующим контактным лицам:

|  |  |
| --- | --- |
| **Георгий Козлов**  ПАО АФК «Система»  Директор по специальным проектам  Тел.: +7 495 228 15 50 доб. 50393  Email: G.Kozlov@sistema.ru  **Владимир Батурин**  ПАО АФК «Система»  Руководитель по мониторингу событий информационной безопасности  Тел.: +7 495 228 15 50 доб. 50394  Email: V.Baturin@sistema.ru |  |

**Важная информация (Disclaimer)**

ПАО АФК «Система» уведомляет, что настоящий запрос информации не должно расцениваться потенциальными исполнителями в качестве публичной оферты ПАО АФК «Система». ПАО АФК «Система» не несет никаких обязательств перед компаниями, принявшими участия в данном запросе информации, и может прекратить проект в любой момент времени.

**Приложения:**

1. **Приложение 1:** Анкета участника и форма ценового предложения.



1. **Приложение 2:**

**Техническое Задание**

**на внедрение централизованной системы по контролю и управлению**

**мобильными устройствами и приложениями в**

**ПАО АФК «Система»**

1. **Цели создания Системы**

Основными целями являются:

* создание централизованной системы защиты корпоративных устройств мобильной связи от несанкционированного доступа к информации в случае взлома, кражи либо утери устройства;
* обеспечение конфиденциальности переговоров между сотрудниками Общества.
* реализация требований политики безопасности на корпоративных мобильных устройствах.
* снижение расходов на корпоративную сотовую связь посредством мониторинга и управления звонками и обменом сообщений абонентов.

1. **Предмет технического задания**

Предметом настоящего технического задания является проведение комплекса работ, направленных на поставку, монтаж и пусконаладку централизованной системы по контролю и управлению мобильными устройствами в ПАО АФК «Система», включая:

* поставка программных и аппаратных средств;
* проведение работ по монтажу оборудования;
* выполнение пусконаладочных работ;
* проведение обучения обслуживающего персонала;
* передача Системы в эксплуатацию.

Комплекс работ, описанных в настоящем техническом задании, должен быть выполнен в срок, не превышающий 10 календарных месяцев.

1. **Область и границы выполнения работ**
   1. Объектом защиты создаваемой Системы являются мобильные устройства сотрудников на базе ОС: iOS, Android, Windows, а также информация, обрабатываемая на данных устройствах в процессе их эксплуатации.
   2. Создаваемая Система не должна быть зависима от используемого провайдера сети передачи данных (операторы сотовой связи, сетей Wi-Fi и т.п.).
2. **Требования к составу Системы**

В состав создаваемой Системы входят следующие средства и подсистемы:

* клиентская часть программного обеспечения на мобильных устройствах;
* центральная консоль управления;
* сервер баз данных;
* сервер управления;
* средства межсетевого экранирования и создания защищенного канала передачи информации между сервером управления и мобильными устройствами;
* подсистема сбора и централизованного хранения истории перемещения мобильных устройств.

1. **Требования к Системе**

|  |  |
| --- | --- |
| * 1. **Общие требования к решению** | |
| 5.1.1. | Сокращение времени работы мобильного устройства при установке средств управления и защиты мобильного устройства не должно превышать 1-2% от заряда аккумулятора. |
| * 1. **Мобильная безопасность** | |
| 5.2.1. | Многофакторная аутентификация для доступа к корпоративной сети и корпоративным приложениям. |
| 5.2.2. | Удаленная блокировка устройства и управление парольной защитой посредством двухфакторной аутентификации на устройстве. |
| 5.2.3. | Удаленный сброс или смена пароля блокировки для восстановления доступа к устройству. |
| 5.2.4. | Дистанционная очистка устройства (затирание всех данных). |
| 5.2.5. | Шифрование данных на устройстве, включая карту памяти, если применимо (если это позволяет мобильная ОС). |
| 5.2.6. | Обнаружение скомпрометированного устройства (rooting). |
| 5.2.7. | Возможность централизованного управления всем функционалом средств защиты информации мобильного устройства в отношении всех имеющихся устройств сразу и каждого в отдельности. |
| 5.2.8. | Возможность обеспечения хранения истории работы средств защиты информации и использования мобильных устройств за период не менее 6 месяцев. |
| 5.2.9. | Удалённая диагностика устройства, получение и обработка событий безопасности на устройстве. |
| 5.2.10. | Централизованное управление всем функционалом подсистемы защиты мобильных устройств из единого интерфейса. |
| 5.2.11. | Возможность ограничения передачи данных по средствам GPRS, 3G, LTE, Wi-Fi, HSDPA на мобильных устройствах. |
| * 1. **Безопасность корпоративных приложений и данных** | |
| 5.3.1. | Организация выделенного и защищённого (с применением средств шифрования) канала связи для доступа к корпоративной сети и информационным системам корпорации. |
| 5.3.2. | Возможность создания изолированного контейнера для корпоративных приложений и данных на личных устройствах. |
| 5.3.3. | Прозрачное шифрование данных в контейнере. |
| 5.3.4. | Выборочная очистка данных и приложений в контейнере. |
| 5.3.5. | Блокировка функций «копировать/вставить» между приложениями в контейнере и вне него. |
| 5.3.6. | Возможность отправки на устройство служебных сообщений и файлов. |
| 5.3.7. | Передача всех событий для хранения серверу баз данных. |
| 5.3.8. | Ограничение приложений для открытия корпоративных файлов (определенные форматы файлов должны открываться в разрешенных в компании приложениях). |
| 5.3.9. | Запрет использования менеджеров паролей для корпоративных учётных записей. |
| 5.3.10. | Запрет доступа к корпоративной электронной почте и корпоративным приложениям при нарушении политик безопасности корпорации. |
| * 1. **Управление мобильными устройствами (MDM)** | |
| 5.4.1. | Возможность централизованного управления настройками устройств на базе iOS, Android, Windows с помощью механизма групповых политик безопасности. |
| 5.4.2. | Настройка подключений к точкам доступа Wi-Fi. |
| 5.4.3. | Настройка прокси для выхода в Интернет через Wi-Fi. |
| * 1. **Управление мобильными приложениями (MAM)** | |
| 5.5.1. | Запрет установки ПО на устройствах. |
| 5.5.2. | Возможность удаленной установки ПО на устройствах. |
| 5.5.3. | Распространение приложений из корпоративного магазина приложений. |
| 5.5.4. | Возможность установки приложений из публичных магазинов (Apple AppStore, Google Play Market и др.). |
| * 1. **Централизованная установка и развертывание** | |
| 5.6.1. | Регистрация устройств и установка агента управления по сети. |
| 5.6.2. | Инвентаризация конфигурации устройств. |
| 5.6.3. | Инвентаризация приложений и сервисов. |
| 5.6.4. | Получение списка зарегистрированных точек доступа Wi-Fi. |
| 5.6.5. | Интеграция с Cisco ISE. |

Применяемое оборудование должно соответствовать следующим требованиям:

* Поставляемое оборудование должно быть новым, с гарантией производителя на детали и качество исполнения не менее 3 лет;
* Должна быть предусмотрена техническая поддержка производителя на срок не менее 3 лет;
* Все применяемое оборудование должно устанавливаться в стандартные серверные стойки 19 дюймов, необходимые принадлежности и запасные части для установки должны быть в комплекте поставки.

1. **Требования к составу и содержанию работ**

Работы должны быть выполнены в 5 этапов, включая:

Этап 1. Техническое проектирование.

Этап 2. Поставка оборудования и лицензий ПО.

Этап 3. Проведение монтажных работ по установке и настройке оборудования.

Этап 4. Внедрение Системы, в том числе настройка поставляемых мобильных устройств для работы в составе Системы.

Этап 5. Проведение обучения обслуживающего персонала.

Работы, осуществляемые в рамках этапов 2-5, должны выполняться на территориальном объекте Заказчика, расположенном по адресу Москва, ул. Моховая, д. 13с1.

1. **Требования к документированию**

Перечень подлежащих разработке комплектов и видов документов должен соответствовать требованиям ГОСТ 34.201-89.

Комплект эксплуатационной документации должен соответствовать требованиям ГОСТ 2.601-2006.

Содержание и оформление документов, входящих в комплект документации, должны соответствовать требованиям РД 50-34.698-90.

Комплект документации предоставляется Заказчику в 2-х экземплярах в печатном виде, а также в электронном виде.

1. **Перспективы развития, модернизации системы**

Система должна предусматривать возможность развития и модернизации в соответствии с нуждами Заказчика, а также должна позволять увеличивать количество:

* мобильных устройств, работающих в составе Системы;
* серверного оборудования, обеспечивающего функционирование Системы.

1. **Требования безопасности**

Система должна отвечать требованиям по обеспечению безопасности при монтаже, наладке, эксплуатации, обслуживании и ремонте технических средств (защита от воздействий электрического тока, электромагнитных полей, акустических шумов и т.п.), по допустимым уровням освещенности, вибрационных и шумовых нагрузок в целом.

Система должна обладать сертификатом соответствия требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей» ФСТЭК России (Гостехкомиссии России) не ниже 4 уровня контроля и технических условий.

1. **Требования к патентной чистоте**

Все программные и технические средства Системы Заказчика должны иметь возможность легального использования на территории Российской Федерации. Помимо этого, все вновь разрабатываемые программные и технические средства Системы Заказчика должны обладать патентной чистотой.

1. **Требования к функциям системы**

Все функции подсистем Системы Заказчика должны быть реализованы в соответствии с требованиями настоящего ТЗ и не противоречить требованиям законодательства Российской Федерации.

1. **Требования к исполнителю работ**

Наличие следующих лицензий и аттестатов:

* Лицензия ФСТЭК РФ на деятельность по разработке и производству средств защиты конфиденциальной информации;
* Лицензия ФСТЭК РФ на деятельность по технической защите конфиденциальной информации.
* Лицензия ФСБ России на осуществление видов деятельности, связанной с шифровальными (криптографическими) средствами.

Опыт оказания услуг в области защиты информации не менее 1 года.

Наличие опыта проведения работ по внедрению предлагаемой системы.

Наличие письма от разработчика программного обеспечения, используемого в рамках работ по внедрению предлагаемой системы.

Желательно наличие положительных отзывов от партнеров по проведению работ в области обеспечения безопасности информации.