**Запрос информации по Проекту**

**«Проведение комплексного технического аудита**

**информационной безопасности Группы компаний АФК «Система»»**

**Обзор проекта:**

ПАО АФК «Система» рассматривает возможность реализации проекта **«Проведение комплексного технического аудита информационной безопасности Группы компаний АФК «Система»» (далее – «Аудит»).**

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

**Планируемый график реализации Проекта:**

Группа компаний АФК «Система» планирует начать работы в апреле 2019 года, а завершить их не позднее 1 полугодия 2020 года.

**Предложение и процесс запроса информации:**

Мы ожидаем получить краткое предложение, которое должно включать:

* порядок проведения и описание работ по проведению Аудита в разрезе выполнения основных требований – в формате презентации/пояснительной записки (на выбор);
* предполагаемый объем необходимых работ с оценкой трудозатрат по каждому из этапов (в чел./час.) за единицу обследования – в формате Приложения 1, лист «Основные этапы и Ценовое предложение»;
* предложение по цене (в рублях) с учетом применимого НДС, с указанием стоимости по каждому из этапов за единицу проведения (внешний узел, сервер, рабочая станция, сотрудник (социальная инженерия) и т.п.), – в формате Приложения 1, лист «Основные этапы и Ценовое предложение»;
* краткий обзор аналогичных/сопоставимых реализованных проектов;
* данные о ключевых членах предполагаемой проектной команды с указанием их профессионального опыта и функциональных ролей в Аудите – в формате Приложения 1, лист «Команда проекта».

**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».

ВНИМАНИЕ!!! Внесены изменения! Срок окончания подачи документов на участие и коммерческих предложений «01» марта 2019г. до 12.00 часов (МСК). **Документы и предложения, поданные после указанного срока, ЭТП не принимаются.**

**Общий объем Аудита:**

Количество компаний (площадок), планируемых к обследованию – 29

Оценочное количество обследуемой инфраструктуры:

* Внешние узлы – более 1700
* Рабочие станции – более 36 тыс.
* Сервера – более 4 тыс.

Вы можете направить интересующие Вас вопросы следующим контактным лицам:

|  |  |
| --- | --- |
| **Зайцев Алексей**  ПАО АФК «Система»  Директор по эксплуатации систем информационной безопасности  Тел.: +7 495 692 10 88, доб. 50390  Email: a.zaytsev@sistema.ru |  |

**Важная информация (Disclaimer)**

ПАО АФК «Система» уведомляет, что настоящий запрос информации не должен 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:**

Приложение 1. Анкета участника и форма ценового предложения



Приложение 2. Требования к проведению технического аудита информационной безопасности Группы компаний АФК «Система».

**Приложение 2**

**Технические требования**

**к проведению комплексного технического аудита информационной безопасности**

**Группы компаний АФК «Система»**

1. **Общие положения**

Настоящие Технические требования (далее – ТТ) является основным документом, определяющим требования и порядок проведения работ по комплексному техническому аудиту информационной безопасности Группы компаний АФК «Система» (далее – Работы).

1. **Цели проведения работ**

Основной целью проведения Работ является получение объективной и независимой оценки текущего уровня защищенности информационных активов Группы компаний АФК «Система».

Работы по выполнению настоящих Технических требований должны предусматривать следующие этапы:

* внешнее тестирование на проникновение;
* внутреннее тестирование на проникновение;
* анализ защищенности беспроводных сетей;
* оценка осведомленности сотрудников в вопросах информационной безопасности;
* оценка устойчивости информационных активов к распределенным атакам типа «отказ в обслуживании».

## **Задачи проведения работ**

Работы должны включать в себя решение следующих задач:

* выявление недостатков в применяемых мерах информационной безопасности и оценка возможности их использования нарушителем;
* практическая демонстрация возможности использования уязвимостей (на примере наиболее опасных);
* оценка текущего уровня осведомленности сотрудников Заказчика в вопросах обеспечения информационной безопасности;
* получение на основе объективных свидетельств комплексной оценки текущего уровня защищенности информационных активов;
* выработка рекомендаций по устранению выявленных недостатков и для повышения уровня защищенности информационных активов.

# Модель нарушителя

Работы необходимо проводить методом черного ящика. Все операции должны выполняться специалистами Исполнителя, находящимися в тех же условиях, что и потенциальный нарушитель. В рамках выполнения работ следует рассматривать следующие типы нарушителя:

* **Высококвалифицированный внешний нарушитель**, действующий со стороны сети Интернет, который не имеет привилегий в информационных активах и реализует атаки, направленные на получение доступа к одному или несколькими узлам ЛВС Заказчика с возможностями, достаточными для организации атак на внутренние компоненты активов. Данная модель нарушителя применяется на этапе «Внешнее тестирование на проникновение».
* **Высококвалифицированный внутренний нарушитель, имеющий санкционированный доступ к определенному сегменту ЛВС Заказчика**, который реализует атаки, направленные на получение доступа к ключевым компонентам и функциям управления информационными активами, обрабатываемой информации, либо на вывод активов из строя. Данная модель нарушителя применяется на этапе «Внутреннее тестирование на проникновение».
* **Высококвалифицированный внешний нарушитель, имеющий доступ к территории Заказчика**, но не имеющий доступа к ЛВС, который не имеет привилегий в информационных активах и реализует атаки, направленные на получение доступа к одному или несколькими узлам ЛВС Заказчика с возможностями, достаточными для организации атак на внутренние компоненты активов. Данная модель нарушителя применяется на этапе: «Анализ защищенности беспроводных сетей».
* **Высококвалифицированный внешний нарушитель**, действующий со стороны сети Интернет, который не имеет привилегий в информационных активах и реализующий атаки, направленные на нарушение работоспособности или полного отказа в обслуживании целевого внешнего ресурса. Данная модель нарушителя применяется на этапе «Оценка устойчивости информационных активов к распределенным атакам типа «Отказ в обслуживании» (DDoS).

# Требования к объему выполняемых работ

## *Внешнее тестирование на проникновение*

Анализ защищенности сетевого периметра должен включать в себя проверки, направленные на поиск и эксплуатацию уязвимостей на сетевом и прикладном уровнях. Порядок выполнения внешнего тестирования должен предусматривать следующие этапы:

1. **Получение предварительной информации о сетевом периметре** на основе источников информации, доступных потенциальному нарушителю (поисковые системы, новости, конференции и т. п.). На этом этапе составляется перечень идентифицированных сетей и доменных имен, принадлежащих Заказчику. Заказчик добавляет или исключает из списка, предоставленного Исполнителем, тестируемые сети и сетевые объекты.
2. **Сканирование узлов сетевого периметра**, определение типов устройств, операционных систем, приложений по реакции на внешнее воздействие. Составляется перечень идентифицированных сервисов на узлах, вошедших в границы проведения работ. При наличии в границах проведения работ значительного количества узлов и сервисов в итоговом отчете указываются только общие данные о типах и количестве обнаруженных сервисов; полная информация (результаты сканирования) предоставляется Заказчику по запросу.
3. **Идентификация уязвимостей сетевых служб.** Осуществляется анализ данных, полученных в результате сканирования узлов сетевого периметра. Выявляются факты использования сетевых служб на сетевом периметре, доступ к которым со стороны внешнего нарушителя может привести к компрометации систем, перехвату чувствительных данных, реализации атак на отказ в обслуживании и других угроз.
4. **Анализ защищенности сервисов сетевой инфраструктуры (DNS, электронной почты и т. п.).** Устанавливается наличие или отсутствие уязвимостей инфраструктурных служб и приложений (при использовании таких служб).
5. **Инструментальное обследование** с использованием инструментальных средств. Выявляются уязвимости сетевых служб и узлов, которые могут быть найдены автоматизированными методами, в границах проведения работ.
6. **Анализ первичных результатов, ручная верификация уязвимостей.** Подтверждается наличие уязвимостей, выявленных в ходе инструментального сканирования, исключаются уязвимости, являющиеся результатом ложного срабатывания автоматизированных средств анализа защищенности (в случае возможности и целесообразности подобной верификации).
7. **Анализ защищенности внешних корпоративных веб-приложений** методом черного ящика, то есть со стороны нарушителя, не обладающего никакими сведениями и логическим доступом к веб-приложениям. Цель анализа защищенности веб-приложений — выявление уязвимостей, которые могут быть использованы для преодоления сетевого периметра и дальнейшего развития атаки во внутреннюю сеть. Анализ защищенности веб-приложений осуществляется в объемах, необходимых для обнаружения наиболее серьезных уязвимостей и для выявления хотя бы одного вектора атаки, позволяющего получить доступ к критически важным ресурсам.
8. **Эксплуатация наиболее опасных уязвимостей** с целью преодоления сетевого периметра. Устанавливается возможность или невозможность преодоления специалистами Исполнителя сетевого периметра. Успешной считается атака, при которой специалисты Исполнителя получают доступ к ресурсам внутренней сети.

## *Внутреннее тестирование на проникновение*

Анализ защищенности ЛВС от атак со стороны внутреннего нарушителя направлен на выявление недостатков, позволяющих практически реализовывать атаки на информационные системы Заказчика. Данный этап работ должен включать в себя следующие мероприятия:

1. **Сбор информации.** Составляется перечень узлов внутренней сети, доступных из определенного Заказчиком для проведения работ сегмента сети (например, из пользовательского сегмента). Проводится анализ механизма получения IP-адреса в сети и возможности подключения сторонних устройств. Осуществляется анализ сегментации сети.
2. **Сканирование узлов, доступных из текущего сегмента ЛВС**, без тестирования на наличие уязвимостей; определение типов устройств, операционных систем, приложений по реакции на внешнее воздействие. Составляется перечень идентифицированных сервисов на узлах, вошедших в границы проведения работ.
3. **Идентификация уязвимостей сетевых служб.** Осуществляется анализ данных, полученных в результате сканирования доступных ресурсов. Выявляется возможность доступа к ресурсам с использованием интерфейсов управления, удаленного доступа или доступа к СУБД, которые не должны быть доступны пользователям сети, из которой осуществляются работы. Выявляются сетевые службы, использование которых позволяет перехватывать сетевой трафик или осуществлять другие атаки со стороны внутреннего нарушителя.
4. **Анализ защищенности инфраструктурных служб и приложений** (DNS, электронная почта и т. п.). Устанавливается наличие или отсутствие уязвимостей инфраструктурных служб и приложений (при использовании и доступности таких служб).
5. **Оценка защищенности сети от атак на канальном уровне.** Устанавливается наличие или отсутствие недостатков в реализации сетевой инфраструктуры, а также в использовании протоколов канального и сетевого уровней, которые могут быть использованы для проведения атак.
6. **Перехват и анализ сетевого трафика.** Выявляются факты использования небезопасных протоколов для передачи данных. Собирается информация об идентификаторах и производных паролей пользователей (при наличии такой возможности).
7. **Выявление явных недостатков в управлении доступом**. Выявляются ресурсы, к которым удалось получить доступ с использованием согласованного вектора атаки.
8. **Подбор паролей**. Подбираются словарные пароли пользователей (при их наличии, выбор словаря осуществляется Исполнителем с учетом требований политики блокировки учетных записей Заказчика).
9. **Эксплуатация наиболее опасных уязвимостей** с целью выхода за границы заданного сегмента. Устанавливается возможность или невозможность получения доступа к критически важным системам специалистами Исполнителя.

## *Анализ защищенности беспроводных сетей*

Анализ защищенности беспроводных сетей должен быть направлен на выявление недостатков в использовании точек доступа и клиентских устройств Wi-Fi для диапазонов 2,4 и 5 ГГц с использованием технологий 802.11a/b/g/n, а также недостатков в архитектуре и организации беспроводного доступа.

В ходе оценки защищенности беспроводных сетей должны применяться инструменты и методики, обеспечивающие:

* обнаружение точек беспроводного доступа, несанкционированно подключенных к локальной вычислительной сети Заказчика;
* обнаружение точек беспроводного доступа, не соответствующих стандартам информационной безопасности (использование методов защиты, для которых есть документированные методы обхода, отсутствие механизмов защиты и т. п.);
* обнаружение несанкционированных подключений к беспроводным сетям;
* обнаружение ошибок в конфигурации клиентских устройств беспроводных сетей;
* выявление уровня осведомленности сотрудников в вопросах информационной безопасности при эксплуатации беспроводных сетей Заказчика.

## *Оценка осведомленности сотрудников в вопросах информационной безопасности*

В рамках данного этапа необходимо оценить эффективность принимаемых Заказчиком мер по повышению осведомленности сотрудников в вопросах информационной безопасности. Для оценки необходимо провести ряд тестов, эмулирующих распространенные сетевые атаки с использованием методов социальной инженерии, в том числе, почтовые рассылки с приложенными файлами, ссылками на сторонние ресурсы с ложной формой аутентификации (имитация фишинговых атак).

Тестирование должно производиться в следующем порядке:

* сбор информации о сотрудниках Заказчика в общедоступных источниках, в том числе — получение списка адресов электронной почты;
* формирование и согласование с Заказчиком перечня проводимых проверок и перечня тестируемых пользователей (фокус-группы, 10-20% от общего количества сотрудников);
* разработка специального программного обеспечения для проведения тестов и его адаптация к особенностям системы обеспечения информационной безопасности Заказчика;
* проведение тестов и обработка их результатов.

## *Оценка устойчивости информационных активов к распределенным атакам типа «Отказ в обслуживании» (DDoS)*

В ходе данного этапа Исполнителем оценивается эффективность принимаемых Заказчиком мер для обеспечения устойчивости ресурсов к распределенным атакам типа «отказ в обслуживании» (Distributed Denial of Service, DDoS). Исполнителю необходимо произвести следующие типы атак:

* атака путем генерации значительного количества трафика с целью исчерпания полосы пропускания сетевых каналов.
* атака на прикладное программное обеспечение с целью исчерпания вычислительных ресурсов.

В зависимости от типа ресурса и условий тестирования Исполнителю необходимо использоваться следующие методики:

* **TCP SYN Flood** - атака заключается в отправке большого количества SYN запросов на установление TCP-соединения с целью исчерпания входящего канала веб-сервера или ресурсов балансировщика;
* **UDP Food** - атака заключается в отправке большого количества UDP пакетов с целью исчерпания полосы пропускания сетевых каналов;
* **ICMP Flood** - атака заключается в отправке большого количества ICMP пакетов с целью исчерпания полосы пропускания сетевых каналов;
* **HTTP Flood** - атака заключается в отправке большого количества GET или POST запросов на получение или отправку тяжелых ресурсов с целью исчерпания полосы пропускания сетевых каналов;
* **Атаки с целью исчерпания ресурсов сервера**. Атаки ориентированы на логику веб-приложения и нацелены на исчерпание ресурсов веб-сервера при обработке "тяжелых" запросов, интенсивных функций обработки или памяти;
* **Атака «Slow read»** заключается в осуществлении медленного чтения заголовков ответа;
* **Атака «Slow post»** заключается в осуществлении медленной отправки данных

Тесты должны проводятся сериями, с постепенно нарастающей нагрузкой (10%, 25%, 50%, 75%, 100%) от согласованного с Заказчиком предельного уровня нагрузки.

1. **Требования к документированию**

По окончании комплексного аудита информационной безопасности специалисты Исполнителя разрабатывают и предоставляют Заказчику следующие документы:

**«Отчет о результатах внешнего и внутреннего тестирования на проникновение».** Отчет должен содержать:

* общие сведения и описание хода работ;
* результаты проведенных проверок (перечень скомпрометированных в рамках работ компонентов);
* выводы (как развернутые технические, так и более краткие для руководства);
* оценку состояния защищенности информационных активов Заказчика как с точки зрения потенциальных векторов проникновения, так и с точки зрения используемых механизмов защиты);
* перечень и описание существующих угроз;
* графическое отображение всех выявленных векторов атак с оценкой сложности их реализации;
* описание хода работ, выявленных уязвимостей, ранжирование их по степени потенциальной опасности, вероятности их использования, описание последствий реализации выявленных уязвимостей;
* рекомендации по устранению выявленных уязвимостей, в том числе рекомендации по изменению конфигурации и настроек оборудования, используемых защитных механизмов и программных средств, принятию дополнительных мер и применению дополнительных средств защиты, по установке необходимых обновлений для используемого программного обеспечения;
* результаты эксплуатации нескольких критически опасных уязвимостей, включая информацию о полученном уровне привилегий в активах на различных этапах тестирования.

«**Отчет о результатах анализа защищенности беспроводных сетей**», который должен содержать:

* общие сведения и описание хода работ;
* результаты проведенных проверок;
* описание методики проведения анализа защищенности (условия проведения, модель нарушителя, границы проведения работ);
* оценку уровня критичности уязвимостей;
* выявленные несанкционированные точки доступа;
* рекомендации по устранению выявленных уязвимостей.

«**Отчет о результатах оценки осведомленности сотрудников в вопросах информационной безопасности**», который должен содержать:

* оценку эффективности программы повышения осведомленности;
* статистику по каждому из типов атаки и действиям пользователей;
* перечень сотрудников, недостаточно осведомленных в вопросах информационной безопасности;
* полученные в рамках работ учетные данные и информацию о версиях используемого ПО.

«**Отчет о результатах оценки устойчивости информационных активов к распределенным атакам типа «Отказ в обслуживании» (DDoS)**», который должен содержать:

* описание методов проведенных DDoS-атак;
* детальное описание хода проведения работ;
* анализ устойчивости прикладных систем и сетевой инфраструктуры к DDoS-атакам;
* рекомендации по повышению защищенности информационных активов Заказчика от DDoS-атак.

1. **Требования к исполнителю работ**

К предполагаемому Исполнителю по выполнению Аудита предъявляются следующие базовые квалификационные требования, которые могут быть уточнены в процессе дальнейшей закупочной процедуры:

* лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации;
* наличие успешного опыта оказания аналогичных услуг для компаний по масштабу бизнеса (выручке, размеру активов) и/ или компаний, входящих в Группу АФК «Система», и/ или компаний финансово-инвестиционного сектора (инвестиционных фондов, банков и компаний, в т.ч. управляющих активами в разных отраслях экономики);
* срок деятельности Исполнителя в области оказания услуг по информационной безопасности - не менее 5 лет.
* профессиональная зрелось (подтвержденная участием в аналогичных проектах, наградами и сертификатами) и полнота проектной команды, которая должна в обязательном порядке включать в себя обладающих соответствующей квалификацией штатных специалистов.