ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на выполнение работ по оценке защищенности информационной инфраструктуры ООО АГР

I. Техническое (конкурсное) задание

1. Общие положения

1.1. Термины, используемые в настоящем Техническом задании (также ТЗ) и приведенные с заглавной буквы, имеют значение, приведенное в Условиях проведения внутреннего Конкурса или в ОУЗ, размещенных в сети Интернет по адресу: https://agr.auto/purchase (далее – «Платформа»).

Направляя Коммерческое предложение Участник конкурса подтверждает, что он ознакомлен с содержанием Условий и полностью принимает их положения, а также с Требованиями по охране труда, предъявляемым к Контрагентам, размещенных на Платформе.

Перечень используемых сокращений:

ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
ЛВС	Локально-вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение

1.2.**Контактные данные АГР**

infosec@agr.auto

1.3. **Общая информация о проекте**

Целью работ является оценка Контрагентом (далее Исполнитель) состояния информационной безопасности информационной инфраструктуры АГР (далее Заказчик), анализ выявленных недостатков и разработка рекомендаций, направленных на снижение связанных рисков деятельности Заказчика

2. Описание услуг / работ / товаров

2.1. Решаемые задачи

Для обеспечения достижения поставленных целей при проведении Работ должны быть решены следующие задачи:

- анализ защищенности внешнего периметра сети;
- анализ защищенности web-ресурсов;
- внутреннее тестирование на проникновение;
- тестирование на проникновение беспроводных сетей;
- попытки реализации недопустимых событий Заказчика, в частности:
  - получение доступа к корпоративным финансовым системам и системам управления персоналом (SAP, 1С)
  - получение доступа (шифрование) информации в системах резервного копирования
  - получение административного доступа к MS Active Directory, корпоративной почте MS Exchange
  - получение доступа к конфиденциальной информации (папки с ограниченным доступом) на файловых серверах

2.2. Границы проведения работ

Работы по анализу защищенности внешнего периметра сети Заказчика (по внешнему тестированию на проникновение) должны проводиться из ЛВС Исполнителя или из сегмента ЛВС заранее согласованного с заказчиком. Внешний периметр заказчика состоит из подсети класса С, и нескольких отдельных адресов, в сумме не более 110 активных IP-адресов.

В работы по специализированному тестированию web-ресурсов входят web-ресурсы Заказчика, доступные из сети Интернет, включая диапазон сети класса С, а также 8 вэб-сайтов с относительно несложной логикой.

Детальнее требования к глубине тестирования вэб-ресурсов описаны в разделе требования к составу работ.

Работы по внутреннему тестированию на проникновение планируется проводить в отношении трех площадок Заказчика в городах: Москва, Чехов и Калуга. Тестирование проводится при подключении к ЛВС Заказчика мобильной рабочей станции Исполнителя, также возможно удаленное тестирование с предоставленного Заказчиком хоста.

В границы работ должна входить вся ЛВС Заказчика, при этом Исполнитель сам может определять степень и глубину воздействия на конкретные сетевые сегменты и хосты, исходя из принципа достаточности для достижения цели тестирования на проникновение. Число хостов во внутренней сети – по отдельному запросу по email, указанному в контактах.

В работы по тестированию на проникновение беспроводных сетей входят 6 беспроводных сетей, расположенных на трех площадках Заказчика, помимо Москвы, 1 находятся в Калуге, другая в 60 км от Москвы.

При необходимости границы работ могут быть изменены, если это не ведет к дополнительным затратам Исполнителя.

Планируемое время проведения работ – рабочие дни, с 10-17:00

Исполнитель заранее согласовывает с Заказчиком ограничения на проводимые работы, включая перечень ресурсов, анализ которых необходимо исключить из проведения работ, временные рамки проведения работ, сетевую нагрузку, создаваемую на сеть.

2.3. Сроки выполнения работ

Начало выполнения работ: с момента подписания договора на проведение работ.

Окончание выполнения работ: не позднее 30 рабочих дней с момента проведения повторного тестирования или последнего этапа работ, определенного и письменно указанного Заказчиком. До полного исполнения обязательств по заказу Заказчика в случае дополнительных работ.

2.4. Требования к составу и содержанию Работ

2.4.1. Предварительный этап

Целью данного этапа является разработка плана-графика выполнения работ.

На данном этапе Исполнителем совместно с Заказчиком должны быть определены и уточнены:

- диапазон IP-адресов, подлежащих внешнему анализу защищенности;
- порядок взаимодействия сторон в ходе выполнения работ;
- формат отчетных документов;
- ограничения и пожелания в проведении работ.

На предварительном этапе Исполнителем и Заказчиком должна быть определена степень информирования специалистов (ИТ, ИБ, рядовых пользователей) о проводимых работах.

2.4.2. Внешнее тестирование на проникновение

Анализ защищенности внешнего периметра должен быть направлен на выявление и эксплуатацию уязвимостей ИБ компонентов информационных систем Заказчика, а также вэб-ресурсов, расположенных на периметре корпоративной сети и доступных из сети Интернет.

Также одним из предметов тестирования данного этапа являются сервисы удаленного подключения (VPN), почтовые сервера, сервис онлайн-конференций.

Порядок выполнения и состав этапов внешнего тестирования на проникновение должен соответствовать следующему алгоритму:

- Предварительный сбор информации из общедоступных источников. На данном этапе должен производиться сбор сведений о структуре и компонентах корпоративной сети Заказчика, таких как: доменные имена и зоны, сетевая адресация, компоненты сети, используемые средства защиты. Также должен производиться сбор сведений о сотрудниках Заказчика и другой информации, представляющей интерес для потенциального злоумышленника. В качестве общедоступных источников используются web-сайты в сети Интернет, социальные сети, форумы, новостные ленты, опубликованные интервью с сотрудниками Заказчика, резюме сотрудников Заказчика и т.д.
- Проведение активного внешнего тестирования на проникновение. Для выявления уязвимостей должны использоваться самые эффективные методы (включая «ручные») и специализированное ПО. В состав работ на данном этапе должно входить следующее:
  - Определение типов и версий устройств, ОС, сетевых сервисов и приложений по реакции на внешнее воздействие;
  - Идентификация уязвимостей. Идентификация уязвимостей должна производиться для всех сервисов, входящих в границы работ и доступных (или ставших доступными в ходе работ) из сети Интернет. Также должно производиться выявление как

уязвимостей, связанных с некорректной реализацией, так и уязвимостей, связанных с некорректной конфигурацией сетевых сервисов, ОС, приложений, сетевых устройств и средств защиты.

- Экспертный анализ защищенности (проникновение). Должен представлять собой моделирование атак, с использованием специализированных средств и сведений об известных уязвимостях, в отношении целевых систем. Работы на данном этапе при необходимости должны итеративно повторяться с целью воздействия на связанные информационные системы, вошедшие в границы работ.

Автоматизированные работы, не требующие обязательного присутствия специалиста на рабочем месте (например, сканирования, запускаемые планировщиком задач по расписанию), могут (по согласованию с Заказчиком) проводиться в вечернее и ночное время, а также в выходные дни.

В ходе выполнения работ Исполнитель должен провести тесты на проникновение на сетевом уровне и уровне приложений в ИС Заказчика, используя выявленные уязвимости и небезопасные конфигурации:

- в операционных системах;
- в приложениях;
- в сетевом оборудовании;
- в средствах защиты,
- функционирующих в общедоступных информационных системах Заказчика.

Исполнитель не должен производить преднамеренных атак на отказ в обслуживании.

Результатом выполнения данного этапа должен быть раздел итогового отчета, содержащий сведения о предпринятых попытках проникновения в ИС Заказчика и успешности их реализации.

2.4.2.1. Анализ защищенности web-ресурсов

Анализ защищенности web-ресурсов представляет собой процесс оценки защищенности web-приложений и web-сайтов Заказчика, а также поддерживающих их web-серверов от сетевых атак.

Исполнитель должен провести тестирование методом «черного ящика» в отношении 5 сайтов с простой логикой (либо статичные страницы, либо инофрмамция направить запрос), 1 вэб-ресурс со страницей саморегистрации (тестировать также после прохождения саморегистрации), а также также всех остальных вэб-ресурсов, обнаруженных в диапазоне сети класса С (не более 30 адресов). Методом серого ящика провести тестирование 2 вэб-ресурсов.

В рамках проведения работ специалист Исполнителя не должен осуществлять эксплуатацию уязвимостей, направленных на пользователей web-ресурса, если их эксплуатация предполагает воздействие на узлы сети, не принадлежащие Заказчику (например, домашние ПК пользователей web-ресурса или ПО контрагентов Заказчика).

В ходе тестирования web-ресурсов Исполнителем должны быть выполнены следующие работы:

- анализ структуры web-ресурса. На данном этапе проводится определение окружения, в котором исполняется web-приложение. В частности, производится сбор данных о:
  - исполняемом содержимом на серверах (ОС, ПО web-сервера);
  - технологиях, используемых в web-приложениях (ASP, Java, CGI и т.п.);
  - структуре каталогов web-ресурсов и типах хранящихся файлов;
  - применяемых механизмах аутентификации;
  - средствах управления сессиями;
  - взаимодействии с внешними ресурсами;
  - типах обрабатываемых данных.
- автоматизированный анализ функционирования компонентов web-сайта – сканирование web-ресурсов автоматизированными средствами с целью выявления существующих уязвимостей.
- «ручной» анализ функционирования компонентов web-сайта. На данном этапе работ специалистами Исполнителя с использованием собственных методик и опыта международных организаций, таких как Open Web Application Security Project (OWASP), Web Application Security Consortium (WASC), должна проводиться идентификация следующих классов атак и уязвимостей (включая, но не ограничиваясь) в терминологии OWASP:
  - Injection (SQL Injection, XML Injection, Command Injection);
  - Broken Authentication;
  - Broken Access Control;
  - Client-Side Attack;
  - Cross-Site Scripting (XSS);
  - Cross-Site Request Forgery (CSRF);
  - Sensitive Data Exposure;
  - Security Misconfiguration;
  - Business Logic Attack.
- эксплуатация уязвимостей. По результатам сбора и анализа данных о целевых web-ресурсах выполняется эксплуатация выявленных уязвимостей.

Результатом выполнения данного этапа должен быть раздел итогового отчета, содержащий сведения о предпринятых попытках проникновения в ИС Заказчика и успешности их реализации.

2.4.3. Внутреннее тестирование на проникновение

Внутренним является тестирование на проникновение, выполняемое на площадке Заказчика при организованном доступе в корпоративную сеть и направленное на выявление и эксплуатацию уязвимостей ИБ информационных активов внутри корпоративной сети Заказчика.

Ключевыми задачами внутреннего тестирования на проникновение, в частности, являются:

- Получение доступа к финансовым, логистическим системам и системам управления персоналом.
- Получение возможности выполнения произвольного кода на серверах резервного копирования

- Продемонстрировать возможность вывода из обслуживания почтовый сервер Заказчика (без реализации последнего шага).
- Получение административных привилегий MS Active Directory
- Получение доступа к конфиденциальной информации (папки с ограниченным доступом) на файловых серверах
- Получение контроля над АРМ из одной площадки в другую.
- Получение контроля над АРМ или сервера в производственной сети из офисного сегмента и наоборот
- Выявление недостатков в конфигурировании сетевых зон безопасности

В ходе выполнения работ Исполнитель должен провести тесты на проникновение на сетевом уровне и уровне приложений в ИС Заказчика, используя выявленные уязвимости и небезопасные конфигурации:

- в операционных системах;
- в приложениях;
- в сетевом оборудовании;
- в средствах защиты
- функционирующих на доступных информационных системах Заказчика.

При проведении работ по данному этапу Исполнитель должен реализовать обход СЗИ NAC в рамках следующих сценариев:

- Подключение к свободной сетевой розетке на Площадке Заказчика;
- Использование и попытка развития атаки с оставленного сотрудником Заказчика рабочего устройства (ноутбука).

Независимо от результата обхода NAC для основного состава работ используется сценарий подключения устройства Исполнителя, внесенного в «белый лист» NAC заказчика.

Порядок выполнения и состав этапов внутреннего тестирования на проникновение должен соответствовать следующему алгоритму:

- сбор сведений о ЛВС Заказчика изнутри сети;
- моделирование атак на сетевом уровне;
- определение типов и версий устройств, ОС, сетевых сервисов и приложений по реакции на внешнее воздействие;
- идентификация уязвимостей компонентов информационных систем, сетевого оборудования и сетевых средств защиты;
- моделирование атак на уровне приложений, сетевых сервисов и ОС с использованием специализированных средств, и сведений об известных уязвимостях в отношении выявленных систем.

В ходе работ специалист не должен производить преднамеренных атак на отказ в обслуживании.

Результатом выполнения данного этапа должен быть раздел итогового отчета, содержащий сведения о предпринятых попытках проникновения и поднятия привилегий в ИС Заказчика и достигнутых результатах.

2.4.4. Тестирование на проникновение беспроводных сетей (опциональный этап)

Целью тестирования на проникновение беспроводных сетей является анализ возможности преодоления механизмов защиты беспроводных сетей потенциальным злоумышленником и оценка возможности проникновения в корпоративную сеть Заказчика.

Для этого специалисты Исполнителя должны выполнить следующие работы:

- анализ беспроводного эфира в доступных для потенциального внешнего злоумышленника помещениях Заказчика.
- в зависимости от типов используемых механизмов защиты беспроводных сетей должен быть реализован один или несколько из следующих сценариев:
  - активная атака на точку доступа или клиентские устройства;
  - пассивный перехват процесса подключения клиентского устройства к беспроводной сети с последующим криптографическим анализом перехваченных данных;
  - создание фиктивной точки доступа и пассивный сбор аутентификационных данных.
- подключение к беспроводной сети и определение доступных ресурсов корпоративной сети.
- перехват сетевого трафика других устройств, подключенных к беспроводной сети.

Результатом выполнения данного этапа должен быть раздел итогового отчета, содержащий сведения о предпринятых попытках проникновения в ИС Заказчика и успешности их реализации.

2.4.5. Проведение повторного тестирования (опциональный этап)

На данном этапе, после внесения изменений Заказчиком в свои ИС, специалист Исполнителя должен выполнить проверку корректности этих изменений и устранения ранее выявленных недостатков по следующим этапам работ:

- Внешнего тестирования на проникновение;
- Анализа защищенности web-ресурсов;
- Внутреннего тестирования на проникновение.

Повторное тестирование, содержащее все проверки, не требуется.

Результатом проведения работ является дополнительный раздел Отчета по практическому анализу защищенности, содержащий ранее сформированную сводную таблицу с дополнительной графой «Статус устранения». В сложных случаях информация будет подкреплена дополнительной информацией.

2.5. Разработка отчетных документов

На завершающем этапе выполнения работ должно быть произведено структурирование и анализ полученных данных с целью разработки аналитических выводов о критичности выявленных проблем информационной безопасности.

На данном этапе должны быть разработаны рекомендации по устранению выявленных уязвимостей и недостатков ИБ в целевых системах Заказчика и сформирован итоговый отчет о выполненных работах.

Разрабатываемые рекомендации должны содержать информацию об организационно-технических мероприятиях, которые требуется провести Заказчику для повышения текущего уровня защищенности, предложены приоритеты и порядок реализации.

Отчет о тестировании на проникновение должен включать в себя:

- высокоуровневое резюме для руководства (executive summary);
- структурированное описание полученных данных о целевой инфраструктуре (видение целевой инфраструктуры с позиции потенциального злоумышленника);
- описание выявленных уязвимостей;
- описание предпринятых попыток проникновения и результатов их выполнения;
- аналитические выводы о текущем уровне защищенности целевой информационной инфраструктуры;
- перечень разработанных рекомендаций по повышению уровня защищенности.

Высокоуровневое резюме для руководства должно содержать основные сведения о результатах проведенных работ, экспертные заключения о влияния выявленных проблем в обеспечении информационной безопасности на защищенность корпоративной компьютерной сети, а также сведения о необходимых мероприятиях по повышению текущего уровня защищенности (включая внедрение или замену технических средств обеспечения ИБ или проведение организационных мероприятий).

Результатом работ на данном этапе должен быть отчёт о тестировании на проникновение.

2.6. Требования к отчетной документации

По результатам выполнения работ Заказчику должен быть представлен Отчет о тестировании на проникновение.

Отчетная документация должна быть разработана на русском языке.

2.7. Результаты и плановые сроки выполнения

п/п	Наименование работ	Результат	Срок, рабочие дни с момента подписания Договора
	Подготовительный этап	Уточненные границы работ Согласованный с Заказчиком План-график выполнения работ	5
	Внешнее тестирование на проникновение	Раздел итогового отчета, содержащий результаты анализа	16

п/п	Наименование работ	Результат	Срок, рабочие дни с момента подписания Договора
		защищенности внешнего сетевого периметра	
	Анализ защищенности web-ресурсов	Раздел итогового отчета, содержащий результаты анализа защищенности web-ресурсов	
	Внутреннее тестирование на проникновение	Раздел итогового отчёта, содержащий результаты внутреннего тестирования на проникновение	26
	Тестирование на проникновение беспроводных сетей (опциональный этап)	Раздел итогового отчёта, содержащий результаты тестирования беспроводных сетей	16
	Анализ результатов тестирований на проникновение и разработка Отчета по практическому анализу защищенности	Отчет по практическому анализу защищенности, включающий в себя: • верхнеуровневое резюме для руководства; • структурированное описание полученных данных о целевой инфраструктуре (видение целевой инфраструктуры с позиции потенциального злоумышленника); • описание выявленных уязвимостей; • описание предпринятых попыток проникновения и результатов их выполнения; • аналитические выводы о текущем уровне защищенности целевой информационной инфраструктуры; • перечень разработанных рекомендаций по повышению уровня защищенности	20
	Проведение повторного тестирования (опциональный этап)	Результатом данного этапа является дополнительный раздел отчета, содержащий сводную таблицу с перечнем ранее	16*

п/п	Наименование работ	Результат	Срок, рабочие дни с момента подписания Договора
		обнаруженных недостатков и статуса их устранения.	

*С момента уведомления Исполнителя о готовности Заказчика к проведению повторного тестирования.

2.8. Дополнительные работы

Для выполнения дополнительных работ по заказам Заказчика, не вошедших в описанные границы, Исполнитель организует проведение оценки и длительности работ в срок не позднее 5 рабочих дней с момента письменного запроса.

2.9. Перечень требований к Исполнителю

Квалификация и опыт Исполнителя должны соответствовать задачам, выполняемым в рамках выполнения работ по проекту.

Исполнитель должен иметь опыт выполнения работ по практическому анализу защищенности за последний год не менее 15 проектов.

Исполнитель должен иметь опыт участия в кибер-спортивных соревнованиях.

Исполнитель должен иметь все необходимые действующие лицензии на оказание предлагаемых услуг. В том числе:

Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации (осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации).

Исполнитель должен иметь в структуре компании выделенное подразделение, отвечающее за работы в области информационной безопасности.

Исполнитель должен иметь сертифицированную систему менеджмента ИБ.

Специалисты исполнителя, должны быть штатными сотрудниками Исполнителя и обладать соответствующей квалификацией, а именно:

Иметь не менее 4 сертификатов OSCP (Offensive Security Certified Professional).

Иметь не менее 1 сертификата OSEP (Offensive Security Experienced Penetration Tester).

Иметь не менее 1 сертификата OSCE (Offensive Security Certified Expert).

Иметь не менее 2 сертификатов OSWE (Offensive Security Web Expert).

Иметь не менее 1 сертификата PMP (Project Management Professional).

2.10. Требования к коммерческому предложению

Подаваемое участником предложение должно включать в себя:

1. Информацию об участнике включающая:

– полное наименование Участника (с указанием организационно-правовой формы);

– банковские реквизиты (наименование банка, БИК, ИНН);

– юридический адрес;

– адрес фактического местонахождения;

– ФИО руководителя;

– ФИО, контактный телефон и электронный адрес сотрудника, отвечающего на время проведение конкурса, за взаимодействие с Заказчиком.

2. Технико-коммерческое предложение с обязательным представлением:

– детального плана по работам в разделу 2.7 с указанием ответственных сторон (Исполнитель или Заказчик) и планируемых сроков реализации. В данном плане необходимо в обязательном порядке указать работы, которые должен проводить Заказчик.;

– Стоимости работ по разделу 2.7, а также универсальную ставку специалистов исполнителя (в часах), привлекаемых для выполнения дополнительных работ в рабочие дни с 6:00 до 22:00 и в выходные, праздничные дни и с 22:00 до 6:00 в рабочие дни (цена указывается в рублях РФ без НДС);

– срока действия предложения;

– что в коммерческом предложении учтены все предоставляемые скидки и все расходы участника по проекту.

4. Список сотрудников участника, которые будут привлечены к реализации проекта (с указанием аналогичных проектов в которых они принимали непосредственное участие), информация о квалификации сотрудников

5. Документы, служащие подтверждением соответствия претендента требованиям настоящего задания на выполнение работ.

3. Срок действия Договора

До исполнения обязательств	X
1 год	
2 года	
3 года	X

4. Интеллектуальная собственность

В процессе выполнения работ / оказания услуг от Контрагента ожидается создание/передача следующих объектов интеллектуальной собственности:

• Создание/передача объектов интеллектуальной собственности не ожидается	X

ИЛИ

Типы объектов	
• Фотоматериалы	
• Видеоматериалы	
• Дизайны, макеты	
• Тексты, сценарии	
• Программы для ПК	
• Базы данных	
• Иное	

В случае передачи АГР прав на объекты интеллектуальной собственности, они должны быть переданы АГР в следующем объеме:

Передача прав			
Отчуждение (выкуп) (бессрочно на любую территорию)	☐	**Во временное пользование** Контрагент предоставит АГР права использования указанных объектов (лицензия, сублицензия) на территории всего мира на срок _____ с даты акта приема-передачи в любой форме и всеми способами без ограничений, в том числе способами, указанными в ст. ст. 1270, 1317, 1324 Гражданского кодекса Российской Федерации. При этом, в случае, если исключительны права на Произведения принадлежат Контрагенту в полном объеме, права использования произведений (лицензия) предоставляются АГР без сохранения за Контрагентом права выдачи лицензий другим лицам (исключительная лицензия).	☐

Стоимость прав на объекты интеллектуальной собственности должна быть отдельно указана в коммерческом предложении.

5. Персональные данные

Контрагент не осуществляет сбор и обработку персональных данных, за исключением рабочих контактных данных вовлеченных в проект лиц	X
Контрагент будет осуществлять обработку персональных данных :	
- персональные данные собираются АГР и передаются Контрагенту (в том числе, посредством предоставления доступа к персональным данным в системах АГР)	
- персональные данные собираются Контрагентом и передаются/предоставляются Контрагентом в АГР по требованию	

(поручению) АГР (в том числе посредством предоставления доступа к персональным данных в системах Контрагента)	

Перечень персональных данных	
Рабочие контактные данные (помимо лиц, вовлеченных в проект)	
Личные контактные и идентификационные/ паспортные данные, данные о доходах и т.п.)	
Персональные данные специальной категории (расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни)	
Цель(и) обработки персональных данных	

В случае предполагаемого поручения обработки персональных данных Контрагенту, Участник конкурса заверяет и по запросу АГР должен документально подтвердить соответствие требованиям, приведенным в п. 15.3 ОУЗ.