ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ПРОВЕДЕНИЕ АНАЛИЗА ИСХОДНОГО КОДА ПРИЛОЖЕНИЯ НА БЕЗОПАСНОСТЬ

1 ЦЕЛИ И ЗАДАЧИ ОКАЗАНИЯ УСЛУГ

1.1. Целью работ является независимое обследование, позволяющее оценить текущее состояние информационной безопасности двух мобильных приложений ОАО «Аэроэкспресс» для платформ iOS и Android (далее – Заказчик), выявить существующие уязвимости, оценить угрозы, спланировать дальнейшие шаги по их минимизации и выработать рекомендации по повышению уровня защищенности.

1.2. Задачи, которые должны быть решены в ходе оказания услуг:

– проведение анализа защищенности приложения;

– формирование отчета о найденных уязвимостях, способах их эксплуатации и рекомендациях по их устранению.

2 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ УСЛУГ

2.1. В рамках оказания услуг Исполнитель должен провести:

3.1.1 Анализ безопасности исходного кода приложения

Анализ безопасности исходного кода должен включать в себя:

– анализ архитектуры соответствующих компонентов приложения;

– ручной анализ исходного кода соответствующих компонентов приложения;

– автоматизированный анализ исходного кода соответствующих компонентов приложения.

Исполнитель осуществляет анализ документации на приложения, являющиеся компонентами приложения, а также проводит интервьюирование архитекторов либо других представителей Заказчика с целью получения полной информации о структуре приложения, передаваемой информации, базах данных и т. д.

Исполнителем должны выявляться критические компоненты, подвергаемые в последствии наиболее полному ручному анализу и выделяться основные угрозы веб-приложения.

При анализе архитектуры Исполнитель обязан использовать лучшие мировые практики: методология моделирования угроз STRIDE, Web Application Security Consortium (WASC) Threat Classification и Open Web Application Security Project (OWASP) Testing Guide.

Ручной анализ состоит из трех основных частей: поиск логических ошибок, анализ криптографических механизмов, поиск типовых уязвимостей.

Ручной поиск логических ошибок проводится в следующих компонентах веб-приложения:

– критические компоненты, выявленные на подэтапе анализа архитектуры;

– механизм аутентификации и контроля сессий;

– механизм создания/удаления/изменения пользовательских учетных записей;

– механизм одноразовых паролей (при наличии);

– точки входа в приложение.

Перечень компонентов, подлежащих ручному поиску логических ошибок, может быть расширен в процессе анализа архитектуры или по рекомендации Заказчика.

Исполнителем должен проводиться анализ методов аутентификации, возможных угроз и масштабов последствий их реализации.

При поиске логических ошибок Исполнителем должен проводиться анализ возможности выполнения действий от имени другого пользователя, обхода механизмов защиты или других ограничений, ошибок, связанных с возможностью состояния гонки (race condition) и т. д. Также проводится оценка возможности вызова отказа в обслуживании при выполнении зловредных действий в серверных компонентах веб-приложения.

Исполнителем должен проводиться анализ используемых криптографических механизмов. Оценивается:

- использование криптографии во всех случаях, когда она необходима;
- корректность выбора криптографических протоколов и примитивов, их параметров;
- корректность реализации криптографических протоколов и/или алгоритмов;
- корректность использования генераторов псевдослучайных чисел;
- Выполняется проверка возможности реализации следующих атак:
- дешифрование информации;
- модификация информации без дешифрования;
- взлом ключа шифрования;
- атаки повторения;
- подделки сообщений, созданных легитимным пользователем;
- и других.

При поиске типовых уязвимостей Исполнителем должен проводиться анализ исходного кода на наличие наиболее популярных и известных типов уязвимостей (в соответствии с OWASP Top Ten и CWE/SANS Top 25).

Для каждого вида уязвимостей Исполнитель создает метод или ряд методов поиска исходного кода, потенциально подверженного уязвимости. Далее проводится поиск всех соответствующих участков исходного кода и их изучение на предмет наличия уязвимости.

Методы поиска будут созданы для:

- функций формирования строк SQL-запросов (выявление SQL-injection);
- функции вызова команд операционной системы (выявление Command-injection);
- функции динамического создания кода (рефлексии) (выявление Code-injection);
- функции динамической загрузки кода (выявление Remote/Local file inclusion);
- функции неконтролируемого вывода в HTML и доступа к неотфильтрованным параметрам (выявление межсайтового выполнения сценариев, XSS);
- функции работы с XML (выявление XML external entities и XML injection);
- функции формирования/парсинга JSON (выявление JSON injection);
- функции загрузки/скачивания файлов (выявление Path Traversal уязвимостей);
- функции установки Cookies (проверка корректности параметров);
- функции создания HTML-форм (проверка защиты от атак типа Cross-site request forgery, CSRF).

Также проводится анализ конфигурационных файлов приложения (web.config, .htaccess и др.) на предмет корректности настроек с точки зрения безопасности.

При автоматизированном анализе исходного кода компонентов приложения Исполнителем должен проводиться анализ всех исходных текстов с использованием специализированного сканера безопасности исходного кода. Все результаты, полученные сканером, будут подвергнуты анализу. Будут выделены ложные срабатывания. Для подтвержденных срабатываний будут определены условия эксплуатации уязвимостей и даны рекомендации по их исключению.

3.1.2 Разработка отчетной документации

По результатам исполнения п. 3.1.1 Исполнитель должен разработать отчетную документацию. Требования к отчетной документации указаны в п. 5 данного Технического Задания.

3.1.3 Гарантийные обязательства

По результатам оказания услуг Исполнитель обязуется в течении 1 года оказывать по запросу Заказчика консультации по телефону, электронной почте, а также по запросу Заказчика осуществлять выезд специалиста Исполнителя для оказания технической поддержки по устранению выявленных уязвимостей.

3 ОПИСАНИЕ ГРАНИЦ ОКАЗАНИЯ УСЛУГ

3.1. Услуги оказываются Исполнителем в г. Москва в рабочее время.

3.2. Оказываемые Исполнителем услуги имеют следующие ограничения:

– анализ исходного кода проводится для двух приложений – iOS и Android, общий объём строк исходного кода iOS не более 75 тыс., Android не более 68 тыс.;

– анализу подлежит код, созданный с использованием следующих языков программирования: iOS – Objective-C (IDE XCode), Android - Java (IDE Andriod Studio);

3.3. Исполнитель использует для оказания услуг фиксированные IP-адреса, которые он предоставляет Заказчику до начала проекта.

4 ТРЕБОВАНИЯ К ОТЧЕТНОЙ ДОКУМЕНТАЦИИ

4.1. По итогам оказания услуг Исполнителем должен быть разработан документ «Отчет по результатам анализа безопасности исходного кода приложения», содержащий:

1) краткую информацию об объекте тестирования;
2) описание используемой методики тестирования и применяемой модели нарушителя;
3) обобщенные результаты анализа, резюме для руководства;
4) описание всех выявленных уязвимостей, их степеней риска, ограничений по их эксплуатации, а также рекомендации по их устранению;
5) подробное описание векторов реализованных атак;

4.2. Разработка отчета выполняется на русском языке.

4.3. Отчет должен быть предоставлен Заказчику, как в бумажной форме, так и в электронной форме в формате *.doc(x), *.PDF.

5 КВАЛИФИКАЦИОННЫЕ ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ (КРИТЕРИИ ОТБОРА)

5.1. Исполнитель должен иметь необходимые профессиональные знания и квалификацию, опыт и положительную репутацию, быть надежным поставщиком услуг, обладать необходимыми трудовыми ресурсами для выполнения договора на оказание услуг (см. Таблица 1).

Таблица 1 – Квалификационные требования к Исполнителю

№ п/п	Критерий	Форма подтверждения
1.	Исполнитель должен предоставить для выполнения проекта команду из не менее 2-х специалистов по анализу кода	Перечень проектной команды с указанием роли каждого участника
2.	Один из специалистов по анализу кода должен иметь высшее образование по программам «Информационная безопасность автоматизированных систем» или «Компьютерная безопасность»	Копии дипломов

№ п/п	Критерий	Форма подтверждения
3.	Каждый специалист по анализу кода должен иметь опыт работы в сфере ИБ не менее 3-х лет	Уведомление Исполнителя
4.	Исполнитель должен иметь в штате сотрудников, или иметь срочный/разовый договор с физическим лицом, обладающим одним из следующих сертификатов: - «Offensive Security Certified Professional» - «CREST Registered Penetration Tester» - «ISTQB International Software Qualifications Board»	Уведомление Исполнителя
5.	У Исполнителя должна быть разработана методика статического и динамического анализа приложений (SAST и DAST)	Копия методики или уведомление Исполнителя
6.	Исполнитель должен иметь опыт выполнения проектов в области ИБ – не менее 3 выполненных проектов	Копии благодарственных писем при наличии или уведомление Исполнителя
7.	Исполнитель должен иметь опыт выполнения проектов по анализу безопасности исходного кода – не менее 3 выполненных проектов	Список проектов (наименование заказчика, контактное лицо заказчика)

6 КАЛЕНДАРНЫЙ ПЛАН РАБОТ

6.1. Все виды услуг выполняются в порядке и в сроках, указанных в календарном плане (см. Таблица 2).

Таблица 2 – Календарный план работ

№ п/п	Наименование этапа	Сроки выполнения, рабочих дней	Отчетные документы
1	Анализ исходного кода приложения		Отчет по результатам анализа исходного кода приложения

Директор Департамента информационных технологий В.В. Ремень