ПРОЕКТНО-ИЗЫСКАТЕЛЬСКИЕ РАБОТЫ

ПО ОНБОРДИНГУ КОМАНД В ПРОЦЕССЫ БЕЗОПАСНОЙ РАЗРАБОТКИ И ФОРМИРОВАНИЮ ИНСТИТУТА SECURITY CHAMPIONS

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

от 01.06.2023

1. **ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

|  |  |
| --- | --- |
| **Сокращение/Термин** | **Расшифровка** |
| Безопасная разработка | Методология, включающая в себя набор практик, подходов, рекомендаций и руководящих принципов, направленная на повышение безопасности разрабатываемого и сопровождаемого программного обеспечения |
| Информационная безопасность (ИБ) | Состояние информации, информационных ресурсов и информационных систем, при котором обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации и т. п. |
| Контейнер | Структура, позволяющая инкапсулировать в себе объекты разных типов. |
| Оркестрация | Автоматическое размещение, координация и управление сложными компьютерными системами и службами |
| Платформа безопасной разработки (ПБР) | Набор программного обеспечения (подсистем), автоматизирующего применения практик Безопасной разработки, интегрированного между собой в целях повышения эффективности использования. |
| ПО | Программное обеспечение |
| Практики Безопасной разработки | Практики, входящие в состав методологии Безопасной разработки, применение которых направлено на выявление уязвимостей и повышение безопасности программного обеспечения |
| Программный код | Текст компьютерной программы Заказчика на каком-либо языке программирования или языке разметки. Скомпилированный и запущенный программный код представляет собой программное обеспечение Заказчика, которое Заказчик сам разрабатывает/модифицирует |
| Процесс CI/CD | Единый, бесшовный и циклический процесс непрерывных разработки, сборки, доставки, развертывания и интеграции программного кода, обеспечивающий повышение качества разработки и сопровождения программного обеспечения Заказчика |
| Платформа | Платформа безопасности, обеспечивающая защищённость разрабатываемых приложений, систем и сервисов, внедряемых в производственный цикл (Процессы и инструменты CI/CD). Представляет собой совокупность ПО, настроенного в соответствии с требованиями настоящего Технического задания |
| Сервис | Программный код, который может быть использован другим программным кодом, по заранее декларируемым способам использования. Программное обеспечение Заказчика может быть представлено в виде Сервиса |
| Сканирование кода | Поиск уязвимостей программного обеспечения с помощью базовых алгоритмов (из коробки) или написанных дополнительных правил под конкретное приложение |
| SCORM | (от англ. SCORM - Sharable Content Object Reference Model) - международный стандарт для электронных обучающих курсов. Он задает правила передачи информации из курса до самой системы. Представляет собой сборник спецификаций и стандартов, разработанный для систем дистанционного обучения. Содержит требования к организации учебного материала и всей системе дистанционного обучения. SCORM позволяет обеспечить совместимость компонентов и возможность их многократного использования: учебный материал представлен отдельными небольшими блоками, которые могут включаться в разные учебные курсы и использоваться системой дистанционного обучения независимо от того, кем, где и с помощью каких средств они были созданы. |
| Стейджинг | Механизм централизованного движения артефактов и метаданных процессов по средам (от DEV, TEST, PREPROD к PROD) |
| Уязвимость | Свойство информационных систем, которое можно использовать для нарушения функционирования программного кода или несанкционированного доступа к его ресурсам. Уязвимости обнаруживаются и документируются в результате автоматизированных проверок инструментов ИБ. |
| Дефект | Разобранные уязвимости по результатам анализа, проведенного инженером ИБ. Один дефект может включать в себя несколько уязвимостей.  |
| Application Security  | IT-дисциплина (ISO/IEC 27034), адресующая аспекты безопасности процесса разработки программного кода |
| Application Security Testing | Тестирование компьютерных программ, сервисов и приложений для идентификации уязвимостей. Включает в себя проведение автоматизированного тестирования при помощи инструментов SAST/DAST/CA/SCA |
| ASOC | (от англ. Application Security Orchestration and Correlation) – практика Безопасной разработки, предполагающая применение средств автоматизированного управления, оркестрации и контроля сквозных процессов безопасной разработки программного кода |
| CLI | (от англ. Command Line Interface) – интерфейс командной строки |
| CS | (от англ. Container Security) – практика Безопасной разработки, предполагающая проведение проверки безопасности контейнеров, используемых для развертывания и функционирования программного обеспечения и (или) его компонентов |
| CI | (от англ. Continuous Integration) – процесс непрерывной интеграции |
| DevOps | (от англ. Development Operations) – методология автоматизации технологических процессов сборки, настройки и развертывания программного обеспечения |
| DevSecOps | (от англ. Development Security Operations) – надстройка над методологией DevOps, включающая в себя набор инструментов и практик, нацеленных на активное взаимодействие специалистов по разработке со специалистами по информационной безопасности и взаимную интеграцию их рабочих процессов друг в друга. |
| DevSecOps-конвейер | Непрерывный технологический процесс разработки программного кода Заказчика и проверок на информационную безопасность в ходе разработки программного кода Заказчика |
| Jeopardy/task based CTF | Task-Based (или Jeopardy) — формат, в котором игрокам предоставляется набор заданий (тасков), к которым требуется найти ответ и отправить его. Ответом является флаг в форме набора символов или произвольной фразы. За верное выполнение каждого задания команда получает определенное количество очков. Чем сложнее задание, тем больше очков даётся за правильный ответ. |
| MAST | (от англ. Mobile Application Security Testing) – класс инструментов для проведения динамического тестирования мобильных приложений (тестирования на проникновения), способный выявить уязвимости как на стадии тестирования, так и в ходе эксплуатации имитируя работу пользователя на устройстве |
| OWASP | (от англ. Open Web Application Security Project) – сообщество, поддерживающее и разрабатывающее практики, методики, инициативы, подходы и инструменты в области Application Security |
| Quality Gate | Критерии качества для приемки результатов сканирования. На основе установленных критериев качества, система оркестрации решает успешно ли завершилась работа пайплайна ИБ или нет. |
| SAST | (от англ. Static Analysis Security Testing) – практика Безопасной разработки, подразумевающая применение статических методов анализа кода, для выявления уязвимостей |
| Security Champion | Security Champion — ключевой контакт по всем вопросам ИБ в рамках конкретной производственной инженерной команды и является единым интерфейсом для центра компетенций.Фиксирует идентифицированные уязвимости и дефекты программного обеспечения по результатам проведенного анализа. Вырабатывает рекомендации по исправлению для идентифицированных уязвимостей, консультирует свою проектную команду в рамках компетенции.Проводит регулярный анализ дефектов технического долга ИБ. |
| DAST | (от англ. Dynamic Application Security Testing) – практика Безопасной разработки, подразумевающая проведение динамического тестирования веб приложений (тестирования на проникновения), способная выявить уязвимости как на стадии тестирования, так и в ходе эксплуатации, имитируя работу пользователя в системе. |
| SCA | (от англ. Software Composition Analysis) – практика Безопасной разработки, подразумевающая анализ сторонних компонентов (библиотек, модулей, содержащих открытый исходный код), используемых при разработке программного обеспечения, на предмет наличия известных уязвимостей и (или) несоответствий требованиям лицензий, используемых для распространения этих компонент |
| SSDL | (от англ. Secure Software Development Lifecycle) – жизненный цикл обеспечения безопасности при разработке программного обеспечения, процесс, призванный уменьшить число уязвимостей в программном обеспечении и уровень их серьезности, а также обеспечить безопасность и конфиденциальность на всех этапах процесса разработки |

1. **ОБЩИЕ СВЕДЕНИЯ**

Проект по проведению проектно-изыскательских работ по обучению и онбордингу команд в конвейер безопасной разработки включает в себя подготовку обучающих материалов по использованию инструментов AppSec, проведение комплексного обучения Security Champions, разбор (триаж) срабатываний AppSec инструментов, а также оказание консультационных услуг в части разработки внутреннего медиаплана и концепции внедрения Quality Gates.

1. **ОПИСАНИЕ РАБОТ, ЦЕЛИ И ЗАДАЧИ**

Целью оказания услуги является подготовка комплексной программы обучения Security Champions, а также разработка прикладных материалов и инструкций, которые напрямую способствуют: развитию экспертных знаний, формированию института Security Champions и онбордингу команд разработки в систему оркестрации процессов безопасной разработки (ASOC), а также систему анализа безопасности мобильных приложений (MAST). Проводимые работы по разбору срабатываний инструментов безопасной разработки и приоритезация технического бэклога послужат отправной точкой для работы по уменьшению количества дефектов в разрабатываемых приложениях, а также вовлечению команд в процессы безопасной разработки систем и сервисов ГК «Иннотех».

Проект призван решить следующие задачи:

1. Расширение и поддержание единого контура по тиражированию практик обеспечения безопасной разработки и автоматизации контролей их выполнения с использованием системы оркестрации.
2. Встраивание в процесс разработки и обеспечение контроля качества разрабатываемого программного обеспечения с точки зрения дефектов информационной безопасности.
3. Минимизирование дефектов информационной безопасности в разрабатываемых программных продуктах.
4. Снижение стоимости исправления дефектов информационной безопасности программного обеспечения.
5. Подготовка прикладных материалов и инструкций для Security Champions по использованию инструмента оркестрации и инструмента анализа защищенности мобильных приложений, что позволит производственным командам ГК «Иннотех» покрыть все доступные практики безопасной разработки.
6. Комплексное обучение команд безопасной разработке мобильных приложений, развитие внутренней инженерной культуры.
7. Формирование внутреннего центра компетенций AppSec, аккумулирующего экспертизу в области безопасной разработки.
8. Обучение принципам работы с дефектами на всех стадиях разработки.
9. Руководители команд, которые используют инструмент оркестрации (ASOC) в своих производственных процессах, смогут отслеживать прогресс по ключевым метрикам эффективности процесса DevSecOps.
10. Определение точек роста и развития процессов DevSecOps на основе собираемых метрик Application Security.

В рамках проекта планируется выполнение следующих работ:

* **Актуализация концепции разработки защищенного ПО**: обследование процессов безопасной разработки «ГК Иннотех» и «ПАО ВТБ» в части устройства конвейера разработки и используемого технологического стека. Аудит и оценка должны проводиться на основании принятых в отрасли методологиях (таких как BSIMM и SAMM) и с учетом регуляторных требований российского законодательства. В рамках разрабатываемой «ГК Иннотех» концепции внедрения порогов качества (Quality Gates), Исполнитель проводит экспертное ревью концепции, а также проводит серию рабочих сессий по формированию целевых порогов качества для различных этапов производственного цикла. В дополнение к рабочим сессиям запланировано проведение технического воркшопа с демонстрацией возможности реализации настроек Quality Gates в оркестраторе (ASOC). Комплекс разрабатываемой организационно-распорядительной документации, в рамках данных работ указан в Таблице 1 настоящего Технического задания. Дополнительные условия проведения работ указаны в п. 4 настоящего технического задания.
* **Обучение Security Champions**: Предоставление интерактивных тренингов по безопасной Android и iOS разработке. Проведение онлайн (очных) тренингов по безопасной Android и iOS разработке. Предоставление практических заданий по информационной безопасности в формате соревнований по захвату флага CTF (Capture the Flag) для Android, iOS и веб уязвимостей. Подробное описание программ обучения, указанно в Таблице 2 настоящего Технического задания. Дополнительные условия проведения работ указаны в п. 4 настоящего технического задания.
* **Разработка комплекса вспомогательных материалов**: подготовка серии коротких видеороликов, описывающих на прикладном уровне основные аспекты работы с новыми инструментами безопасной разработки (ASOC, MAST) с позиции роли Security Champion. В дополнение к видеоматериалам, планируется подготовка коротких инструкций, описывающих: процесс создания пайплайна ИБ в оркестраторе (ASOC), а также процесс подключения ASOC в CI/CD. Набор разрабатываемых вспомогательных материалов, указан в Таблице 3 настоящего Технического задания. Дополнительные условия проведения работ указаны в п. 4 настоящего технического задания.
* **Формирование технического долга по информационной безопасности**: после завершения основных работ по подключению команд(ы) и запуску первых сканирований инструментов ИБ класса SAST и MAST с использованием ASOC, Исполнитель разбирает срабатывания инструментов ИБ (PT Application Inspector, Solar AppScreener, Stingray). Дополнительные условия проведения работ указаны в п. 4 настоящего технического задания.
* **Продвижение бренда AppSec и Security Champion в «ГК Иннотех»**: Оказание консультационных услуг по наполнению медиаплана: подготовка списка рекомендуемых статей по информационной безопасности для развития компетенций Security Champion, а также участие в четырех внутренних митапах «ГК Иннотех» по тематике Application Security. Объем и дополнительные условия проведения работ в рамках данного направления указаны в п. 4 настоящего Технического задания.

*Таблица 1. Комплекс организационно-распорядительной документации по результатам проведенного обследования.*

| **№** | **Наименование документа** | **Описание документа** |
| --- | --- | --- |
| 1. | Отчет об обследовании и рекомендации | Описывает результаты обследования процессов разработки ПО, применяемых в «ГК Иннотех» и «ПАО ВТБ», содержит общую информацию об инструментальном стеке информационной безопасности, рекомендуемые решения для внедрения и стратегию повышения уровня зрелости. |
| 2. | Стратегия и дорожная карта | Описывает поэтапный календарный план внедрения и развития практик безопасной разработки ПО на 3 или более лет для «ГК Иннотех» и «ПАО ВТБ», с шагом в месяц/квартал, с описанием необходимых инициатив. При формировании плана учитываются текущее состояние, целевое состояние, а также внешние условия и ограничения, известные на момент проведения обследования. |

*Таблица 2. Программа обучения.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Курс** | **Объем курса** | **Количество** | **Содержание курса** |
| Интерактивный курс по уязвимостям web приложений  | Самостоятельное изучение материала участниками. Ограничение по времени прохождения - 1 календарный месяц. | 1 штука, без ограничения количества пользователей | Данный интерактивный курс знакомит слушателей c основными уязвимостями web приложений. Слушатель узнает об основных классах уязвимостей из категорий OWASP Top 10, причинах возникновения и способах предотвращения. В рамках курса в виде интерактивных примеров демонстрируется эксплуатация уязвимостей web приложений и объясняется причина их возникновения. |
| Интерактивный курс по уязвимостям мобильных приложений на iOS | Самостоятельное изучение материала участниками. Ограничение по времени прохождения - 1 календарный месяц. | 1 штука, без ограничения количества пользователей | Данный интерактивный курс знакомит слушателей c основными уязвимостями мобильных приложений на платформе iOS. Слушатель узнает об основных классах уязвимостей из категорий OWASP Mobile Top 10, причинах возникновения и способах предотвращения. В рамках курса в виде интерактивных примеров демонстрируется эксплуатация iOS уязвимостей и объясняется причина их возникновения. |
| Интерактивный курс по уязвимостям мобильных приложений на Android | Самостоятельное изучение материала участниками. Ограничение по времени прохождения - 1 календарный месяц. | 1 штука, Без ограничения количества пользователей | Данный интерактивный курс знакомит слушателей c основными уязвимостями мобильных приложений на платформе Android. Слушатель узнает об основных классах уязвимостей из категорий OWASP Mobile Top 10, причинах возникновения и способах предотвращения. В рамках курса в виде интерактивных примеров демонстрируется эксплуатация уязвимостей и объясняется причина их возникновения. |
| Online курс по уязвимостям web приложений | 16 ак. часов.(проводится в формате 2 дня по 8 часов, либо 4 дня по 4 часа.) | 2 штуки, до 33 человек в рамках одного курса. Дополнительные проводятся по согласованию. | Обучение слушателей проходит в формате вебинара c возможностью задавать вопросы преподавателю. В рамках вебинара разбираются основные уязвимости веб приложений по классификации OWASP Top 10, причины их возникновения и способы предотвращения. В рамках курса демонстрируется эксплуатация уязвимостей на реальных приложениях и примерах. |
| Online курс по основным уязвимостям мобильных приложений на Android | 16 ак. часов.(проводится в формате 2 дня по 8 часов, либо 4 дня по 4 часа.) | 2 штуки, до 33 человек в рамках одного курса. Дополнительные проводятся по согласованию. | Обучение слушателей проходит в формате вебинара c возможностью задавать вопросы преподавателю. В рамках вебинара разбираются основные уязвимости мобильных приложений на платформе Android по классификации OWASP Mobile Top 10, причины их возникновения и способы предотвращения. В рамках курса демонстрируется эксплуатация уязвимостей на реальных приложениях и примерах. |
| Online курс по основным уязвимостям мобильных приложений на iOS | 16 ак. часов.(проводится в формате 2 дня по 8 часов, либо 4 дня по 4 часа.) | 2 штуки, до 33 человек в рамках одного курса. Дополнительные проводятся по согласованию. | Обучение слушателей проходит в формате вебинара c возможностью задавать вопросы преподавателю. В рамках вебинара разбираются основные уязвимости мобильных приложений на платформе iOS по классификации OWASP Mobile Top 10, причины их возникновения и способы предотвращения. В рамках курса демонстрируется эксплуатация уязвимостей на реальных приложениях и примерах. |
| CTF (англ. Capture the flag) — соревнование по обнаружению уязвимостей web-приложений | 1 календарный месяц | 1 штука, до 100 человек в рамках одного CTF. | Соревнования организуются в формате классического Jeopardy/task-based, когда на каждое задание в рамках соревнования есть собственный флаг. Темы заданий – наиболее часто используемые уязвимости web приложений.Всего в рамках соревнований запланировано порядка 10-20 заданий, покрывающих поверхность атаки потенциального злоумышленника. |
| CTF (англ. Capture the flag) — соревнование по обнаружению уязвимостей мобильных приложений на iOS | 1 календарный месяц | 1 штука, до 100 человек в рамках одного CTF. | Соревнования организуются в формате классического Jeopardy/task-based, когда на каждое задание в рамках соревнования есть собственный флаг. Темы заданий – наиболее часто используемые уязвимости мобильных приложений на iOS платформе.Всего в рамках соревнований запланировано порядка 10-20 заданий, покрывающих поверхность атаки потенциального злоумышленника. |
| CTF (англ. Capture the flag) — соревнование по обнаружению уязвимостей мобильных приложений на Android | 1 календарный месяц | 1 штука, до 100 человек в рамках одного CTF. | Соревнования организуются в формате классического Jeopardy/task-based, когда на каждое задание в рамках соревнования есть собственный флаг. Темы заданий – наиболее часто используемые уязвимости мобильных приложений на Android платформе.Всего в рамках соревнований запланировано порядка 10-20 заданий, покрывающих поверхность атаки потенциального злоумышленника. |
| Воркшоп по ASOC | 2 ак. часа | 1 штука, до 33 человек в рамках одного воркшопа. Дополнительные проводятся по согласованию. | На данном воркшопе слушатели ознакомятся с классом инструментов ASOC, принципами его бесшовной интеграции в рабочие CI/CD пайплайны. В рамках воркшопа на примерах будут продемонстрированы следующие функциональные возможности: добавление пользователей/команд, добавление проектов/ИС в оркестратор, подключение инструментов AppSec, настройка и описание принципов построения Quality Gates, настройка пайплайна для вызова оркестратора, настройка нотификаций, выгрузка дефектов в баг-трекер. Обсуждение и кастомизация ролевых моделей для реализации целевого процесса. |
| Воркшоп по Stingray | 2 ак. часа | 1 штука, до 33 человек в рамках одного воркшопа. Дополнительные проводятся по согласованию. | На данном воркшопе слушатели ознакомятся с классом инструментов MAST, принципами его бесшовной интеграции в рабочие CI/CD пайплайны.В рамках воркшопа на примерах бут продемонстрированы следующие аспекты: добавление и управление проектами, настройка правил проверки и управление сканированием, работа с тест-кейсами, настройка интеграции в CI/CD цикл, интеграция с оркестратором. Разбор наиболее часто встречаемых уязвимостей, описание принципов построения Quality Gates, обсуждение и кастомизация ролевых моделей для реализации целевого процесса. |
| Воркшопы по разбору дефектов (триаж) web и мобильных приложений | 2 ак. часа  | 2 шутки, 2 раза в месяц | На данных воркшопах слушатели смогут обучиться процессу разбора дефектов на реальных примерах. На воркшопах демонстрируются принципы и процесс разбора уязвимостей 5 различных категорий уязвимостей, наиболее часто встречающихся у Заказчика. |

*Таблица 3. Комплекс вспомогательных обучающих материалов.*

| **№** | **Тип материала** | **Наименование** | **Описание** |
| --- | --- | --- | --- |
| 1. | Видео-инструкция | Видео инструкция: добавление и настройка приложений в ASOC | Описывает способ добавления приложения в систему оркестрации и их возможные настройки. |
| 2. | Видео-инструкция | Видео инструкция: добавление объектов сканирования в ASOC | Описывает процесс создания/конфигурирования таких объектов сканирования, как: кодовая база, артефакт, экземпляр приложения, прокси-репозиторий. |
| 3. | Видео-инструкция | Видео-инструкция: создание пайплайна ИБ в ASOC | Описывает процесс создания и настройки пайплайна ИБ для разных объектов сканирования. |
| 4. | Видео-инструкция | Видео-инструкция: Работа со срабатываниями инструментов и формирование дефектов ИБ. | Описывает ключевые аспекты работы со срабатываниями инструментов, такие как: добавление исключений, принятие риска, создание правил обработки срабатываний, создание дефекта. |
| 5. | Видео-инструкция | Видео-инструкция: интеграция ASOC с дефект-трекером Jira | Описывает нюансы настройки синхронизации ASOC с Jira для выгрузки дефектов ИБ производственным командам разработки. |
| 6. | Видео-инструкция | Видео-инструкция: работа с проектами в Стингрей | Содержит основную информацию по работе с проектами в Стингрей, такую как: добавление/редактирование проекта, правила анализа, права доступа, и т.д. |
| 7. | Видео-инструкция | Видео-инструкция: работа с правилами в Стингрей | Содержит основную информацию по правилам анализа уязвимостей, которые применяются для выбранного проекта в Стингрей. |
| 8. | Видео-инструкция | Видео-инструкция: работа с профилями сканирования в Стингрей | Содержит основную информацию по работе с профилями сканирования проектов в Стингрей. |
| 9. | Видео-инструкция | Видео-инструкция: работа с результатами сканирования в Стингрей | Содержит основную информацию по работе с результатами сканирования проектов в Стингрей, такую как: сводные данные по обнаруженным дефектам, рекомендации к устранению, результатам проверки на соответствие стандартам и т.д.  |
| 10. | Видео-инструкция | Видео-инструкция: способы запуска сканирования в Стингрей и настройка автоматического сканирования для магазинов приложений  | Содержит основную информацию по настройке запуска сканирования проектов в Стингрей различными способами, а также возможность автоматического сканирования новых версий приложений, вышедших в магазинах приложений (RuStore, Google Play, AppStore).  |
| 11. | Видео-инструкция | Видео-инструкция: работа с тест-кейсами в MAST | Содержит информацию по созданию тест-кейсов для проектов/приложений.  |
| 12. | Инструкция | Создание пайплайна ИБ в ASOC | Содержит описание необходимых шагов для создания пайплайна ИБ в ASOC. |
| 13. | Инструкция | Подключение ASOC в CI/CD пайплайн | Описывает способ экспорта пайплайна ИБ ASOC для встраивания в производственный цикл CI/CD. |

* 1. **Проведение обследования текущего состояния процессов разработки программного обеспечения**
		1. В рамках данной задачи должны производиться сбор, анализ и документирование информации о процессе разработки ПО в Организации.
		2. Сбор информации должен производиться в рамках интервью-сессий со следующими фокус-группами:
* руководство подразделения ИБ;
* руководство производственных подразделений (команд разработки ПО);
* эксперты команд разработки, отвечающих за реализацию приложений и цифровых сервисов в Организации.

	+ 1. В рамках интервью-сессий должны фиксироваться, анализироваться и документироваться следующие ключевые аспекты и особенности производственного процесса:
* контекст разрабатываемых систем: назначение, основные цели и функциональные задачи, разрабатываемой ИС/приложения /сервиса, используемый технологический стек, размер и динамика роста кодовых баз;
* инфраструктура разработки: использование систем контроля версий, средств автоматического анализа кода, средств автоматической сборки, интеграции изменений и последующего тестирования программного кода, средств автоматического развертывания;
* методологии / Инженерные подходы разработки: скорость разработки (количество релизов/сборок в единицу времени); использование подходов DevOps для непрерывной и ускоренной разработки программного кода и вывода его в промышленную эксплуатацию;
* инженерные практики: разработка юнит-тестов, применение практик код-ревью, использование автоматизированных тестов для проверки функциональности разработанных приложений и сервисов;
* документация процесса: наличие и содержание существующих процедур, политик, руководств, чек-листов применяемых при разработке систем;
* цели по качеству разрабатываемых систем: наличие собираемых метрик качества ПО на уровне отдельных команд, проектов, поставщиков ПО и организации в целом; наличие соответствующих механизмов сбора данных, использование метрик для повышения эффективности процесса разработки и достижения целей качества ПО;
* команда разработки: структура, размер и роли в команде, процессы взаимодействия внутри команды и со смежными подразделениями; показатели динамики роста команды разработки;
* подходы к ИБ разрабатываемого ПО: цели и тактические задачи по обеспечению безопасности программных продуктов, классификация программных продуктов, классификация / категоризация данных, риск-менеджмент и управление угрозами ИБ, текущая техническая инфраструктура ИБ и др.;
* анализа применяемых регламентирующих регуляторных стандартов.
	1. **Проведение обследования используемого технологического стека**
		1. Для определения границ внедрения практик безопасной разработки ПО производится анализ репозиториев исходного кода программного обеспечения на основе заполненных Заказчиком данных в формате опросника.
		2. В рамках данного анализа оцениваются следующие метрики:
* общее количество разработчиков;
* общее количество разрабатываемых проектов;
* количество активных репозиториев;
* объем кода по языкам программирования;
* количество разработчиков в основных разрабатываемых проектах.

	+ 1. По результатам сбора данных должны быть сформированы минимальные и рекомендуемые границы тиражирования практик безопасной разработки ПО.
	1. **Описание целевых процессов безопасной разработки и разработка комплекса организационно-распорядительной документации**
		1. Отчет об обследовании и рекомендации.

Данный документ является результирующим артефактом следующих работ и включает в себя результат их исполнения:

* Проведение обследования и анализа текущего состояния процессов разработки программного обеспечения Заказчика:
	+ Проведение сессий и интервью с фокус-группами;
	+ Анализ текущего состояния процесса разработки;
	+ Проведение обследования и анализа используемого технологического стека.

		1. Стратегия и дорожная карта.

Данный документ является результирующим артефактом следующих работ и включает в себя результат их исполнения:

* Формирование стратегии внедрения практик безопасной разработки ПО;
* Формирование целевого состояния процесса;
* Формирование границ проекта тиражирования практик безопасной разработки ПО;
* Разработка долгосрочного календарного плана внедрения практик и процессов обеспечения безопасной разработки ПО.
	1. **Консультационные услуги по оценке концепции внедрения Quality Gates**
		1. Проведение экспертного ревью и дополнения (при необходимости) концепции внедрения Quality Gates, разрабатываемой «ГК Иннотех».

Данные работы являются результирующим артефактом следующих работ и включают в себя результат их исполнения:

* Предоставление актуальной версии концепции внедрения Quality Gates Заказчиком;
	1. **Обучение Security Champions**
		1. Подготовка и передача интерактивного курса по уязвимостям мобильных приложений на платформе iOS;
		Данные работы являются результирующим артефактом следующих работ и включают в себя результат их исполнения:
* Отправка доступов менеджеру Заказчика, ответственному за прохождение обучения участников со стороны Заказчика (в случае предоставления интерактивного обучения через платформу обучения Исполнителя);
* Самостоятельное прохождение материала участниками (в случае предоставления SCORM пакета Исполнителем).

	+ 1. Подготовка и передача интерактивного курса по уязвимостям мобильных приложений на платформе Android;
		Данные работы являются результирующим артефактом следующих работ и включают в себя результат их исполнения:
* Отправка доступов менеджеру Заказчика, ответственному за прохождение обучения участников со стороны Заказчика (в случае предоставления интерактивного обучения через платформу обучения Исполнителя);
* Самостоятельное прохождение материала участниками (в случае предоставления SCORM пакета Исполнителем).

	+ 1. Проведение онлайн-курса по уязвимостям мобильных приложений на платформе iOS;
		Данные работы являются результирующим артефактом следующих работ и включают в себя результат их исполнения:
* Заказчиком сформирована группа слушателей, прошедших программу интерактивного курса по уязвимостям мобильных приложений на платформе iOS (не более 33 человек в одной группе);
	+ 1. Проведение онлайн-курса по уязвимостям мобильных приложений на платформе Android;
		Данные работы являются результирующим артефактом следующих работ и включают в себя результат их исполнения:
* Заказчиком сформирована группа слушателей, прошедших программу интерактивного курса по уязвимостям мобильных приложений на платформе Android (не более 33 человек в одной группе);

	+ 1. Проведение соревнований по обнаружению уязвимостей (CTF) мобильных приложений на платформе iOS;
		Данные работы являются результирующим артефактом следующих работ и включают в себя результат их исполнения:
* Дата начала проведения соревнований определена Заказчиком таким образом, чтобы наибольшее число участников завершило интерактивное и онлайн обучение уязвимостям мобильных приложений на платформе iOS.

	+ 1. Проведение соревнований по обнаружению уязвимостей (CTF) мобильных приложений на платформе Android;
		Данные работы являются результирующим артефактом следующих работ и включают в себя результат их исполнения:
* Дата начала проведения соревнований определена Заказчиком таким образом, чтобы наибольшее число участников завершило интерактивное и онлайн обучение уязвимостям мобильных приложений на платформе Android.

	+ 1. Проведение соревнований по обнаружению уязвимостей (CTF) веб приложений;
		Данные работы являются результирующим артефактом следующих работ и включают в себя результат их исполнения:
* Определение Заказчиком списка Security Champions, занимающихся веб разработкой;
* Предоставление списка участников для последующей регистрации на платформе проведения CTF.

	+ 1. Проведение воркшопа по работе с инструментом ASOC;
		Данные работы являются результирующим артефактом следующих работ и включают в себя результат их исполнения:
* Сформированный запрос на проведение со стороны Заказчика.

	+ 1. Проведение общего воркшопа по работе с инструментом MAST (Стингрей);
		Данные работы являются результирующим артефактом следующих работ и включают в себя результат их исполнения:
* Прохождение участниками интерактивных тренингов по уязвимостям мобильных приложений (iOS/Android).
* Прохождение участниками онлайн тренингов по уязвимостям мобильных приложений (iOS/Android).

	+ 1. Проведение ежемесячных воркшопов по разбору срабатываний и формированию дефектов (технического долга ИБ).
		Данные работы являются результирующим артефактом следующих работ и включают в себя результат их исполнения:
* Определение даты проведения для каждого воркшопа.
* Предоставление Заказчиком списка основных тематик/категорий уязвимостей, которые требуется разобрать в приоритете на воркшопе (список направляется за 2 недели до проведения планируемого воркшопа);
	1. **Разработка комплекса вспомогательных обучающих материалов.**

Полный набор разрабатываемых материалов содержится в таблице 3 настоящего технического задания и не требует предварительного выполнения работ на стороне Заказчика.

* 1. **Оказание консультационных услуг в части продвижения бренда AppSec и Security Champion.**
		1. Подготовка рекомендуемого списка тематик и рекомендуемого списка статей для медиаплана «ГК Иннотех».
		2. Участие в формате спикера в 4-х внутренних митапах/конференциях «ГК Иннотех» по тематике Application Security.

**ЭТАПЫ ПРОЕКТА И СРОКИ**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование** | **Срок** **выполнения работ** | **Результат работ и документация** |
| **1.** | **Этап 1. Актуализация текущего состояния и концепции разработки защищенного ПО** | 1 месяц | * Проведены интервью-сессии для трех внутренних команд разработки «ГК Иннотех» с участием: руководителей команд разработки, руководителей подразделения ИБ;
* Проведены интервью-сессии для трех внутренних команд разработки «ПАО ВТБ» с участием: руководителей команд разработки, руководителей подразделения ИБ;
* Заполнены технические опросники для обследуемых команд разработки со стороны «ГК Иннотех» и «ПАО ВТБ».
 |
| **2.** | **Этап 2. Разработка документации по результатам проведенного аудита** | 2 месяца | * Документ «Отчет об обследовании и рекомендации»;
* Документ «Стратегия и дорожная карта»;
* Проведено экспертное ревью и (при необходимости) предоставлены комментарии, к концепции внедрения Quality Gates, предоставленной «ГК Иннотех»;
 |
| **3.** | **Этап 3. Обучение Security Champions** | 6 месяцев | * Предоставлены интерактивные курсы по уязвимостям iOS приложений;
* Предоставлены интерактивные курсы по уязвимостям Android приложений;
* Проведены 2 онлайн-тренинга по уязвимостям Android приложений;
* Проведены 2 онлайн-тренинга по уязвимостям iOS приложений;
* Проведены 3 CTF (1 Web, 1 iOS, 1 Android);
 |
| **4.** | **Этап 4. Разработка комплекса вспомогательных материалов по решению mDAST (Стингрей)** | 4 месяца | * Подготовлена видео-инструкция: работа с проектами в Стингрей;
* Подготовлена видео-инструкция: работа с правилами в Стингрей;
* Подготовлена видео-инструкция: работа с профилями сканирования в Стингрей;
* Подготовлена видео-инструкция: работа с результатами сканирования в Стингрей;
* Подготовлена видео-инструкция: способы запуска сканирования и настройка автоматического сканирования для магазинов приложений в Стингрей;
* Подготовлена видео-инструкция: работа с тест-кейсами в Стингрей;
* Проведен воркшоп по работе с инструментом MAST Стингрей;
 |
| **5.** | **Этап 5. Формирование технического бэклога (разбор срабатываний инструментов AppSec)** | 6 месяцев | * Регулярный разбор срабатываний инструментов AppSec (Solar AppScreener, PT AI, Стингрей, Code Scoring и Trivy)
 |
| **6.** | **Этап 6. Оказание консультационных услуг по продвижению бренда AppSec и Security Champion в «ГК Иннотех»** | 3 месяца | * Подготовлен рекомендованный список статей для медиаплана «ГК Иннотех»;
* Факт участия Исполнителя в формате спикера в 4-х митапах, проводимых «ГК Иннотех» на тематику Application Security.
 |
| **7** | **Этап 7. Разработка комплекса вспомогательных материалов по инструменту оркестрации ASOC** | 4 месяца | * Подготовлена видео-инструкция: Работа со срабатываниями инструментов и формирование дефектов ИБ в ASOC;
* Подготовлена видео-инструкция: добавление и настройка приложений в ASOC;
* Подготовлена видео-инструкция: добавление объектов сканирования в ASOC;
* Подготовлена видео-инструкция: интеграция ASOC с дефект-трекером Jira;
* Подготовлена инструкция: Создание пайплайна ИБ в ASOC;
* Подготовлена инструкция: Подключение ASOC в CI/CD пайплайн;
* Проведен технический воркшоп с демонстрацией процесса настройки Quality Gates в ASOC;
* Проведен воркшоп по работе с инструментом оркестрации ASOC для Security Champion;
 |

1. **ОГРАНИЧЕНИЯ И ДОПУЩЕНИЯ**
	1. **Общие**

Работы в рамках настоящего Технического Задания, могут выполняться параллельно.

Старт работ в рамках отдельного этапа может быть отложен по времени и выполняться в рамках заявки на выполнение работ.

До начала оказания услуг по формированию технического долга ИБ, а также возможных работ по установке/настройке/обновления ПО, Заказчиком назначается уполномоченный сотрудник для взаимодействия с Исполнителем в части решения организационных вопросов, в том числе:

* Предоставление сетевого и логического доступа, необходимого для корректной работы ПО и осуществления интеграционного взаимодействия;
* Предоставление физического доступа на объект Заказчика (при необходимости);
* Предоставление материалов и данных, необходимых для проверки работоспособности установленного ПО;
* Прочих вопросов, связанных с оказанием услуг.

В состав работ НЕ входят следующие работы:

* Разработка документации: руководств пользователя/администратора для инструментов ИБ класса SAST, DAST, CS, OSA/SCA.
* Разработка обучающих и вспомогательных материалов по работе с инструментами ИБ класса SAST, DAST, CS, OSA/SCA.
	1. **Актуализация концепции разработки защищенного ПО**
* В рамках проводимого обследования состояния процессов безопасной разработки, Заказчик должен предоставить возможность проведения серий интервью-сессий с тремя командами разработки со стороны «ГК Иннотех», а также с тремя командами разработки со стороны «ПАО ВТБ». В частности, к обследованию будут привлечены владельцы ИЦ «Конвейер DevSecOps» и владельцы «Dreampipe».
* Выбор конкретных команд разработки лежит на стороне Заказчика, однако, выбор должен быть сделан таким образом, чтобы выбранные команды использовали наибольшее количество практик безопасной разработки (таких как OSA/SCA/SAST/DAST/MAST/CS) в своих производственных процессах.
* В случае неполного охвата выбранными командами использующихся практик безопасной разработки, рекомендации, а также разрабатываемая в рамках обследования ОРД будут ограничены только теми данными, которые были предоставлены командами процессе проведения обследования.
* Допускается подготовка общих рекомендаций и общей дорожной карты развития процессов безопасной разработки для «ГК Иннотех» и «ПАО ВТБ» в случае несущественного отличия или схожести процессов и состояния безопасной разработки по результатам обследования.
* Разрабатываемая ОРД по результатам проведенных работ не предполагает наличие требований к оформлению документации со стороны Заказчика.
* Заказчик должен заблаговременно (за 1 месяц до окончания срока этапа) предоставить актуальную версию концепции внедрения Quality Gates, чтобы у Исполнителя было достаточно времени для проведения экспертной оценки и подготовки комментариев/дополнений (при необходимости). В случае несвоевременного предоставления актуальной версии концепции, срок завершения этапа может быть сдвинут.
* Дата и время проведения рабочих сессий по формированию целевых порогов качества для различных этапов производственного цикла обговариваются совместно с руководителем практики со стороны «ГК Иннотех». Обозначенные даты проведения рабочих сессий должны укладываться в срок проведения этапа работ, иначе срок завершения этапа может быть сдвинут.
* В рамках проводимого воркшопа по демонстрации настройки Quality Gates производится запись встречи, для дальнейшего внутреннего использования и изучения Заказчиком.
	1. **Обучение Security Champions**

Общее количество участников программы обучения Security Champions: не более 100 человек.

Количество участников в рамках выбранного онлайн-обучения: не более 33 человек.

Интерактивное обучение предоставляется в формате SCORM пакета, либо в формате предоставления доступа менеджеру Заказчика на онлайн платформу Исполнителя, ответственному за прохождение обучения участниками.

Организация соревнований в формате захвата флага (CTF) проводится единоразово для всех участников с единой датой старта и датой окончания.

Соревнования в формате захвата флага (CTF) для уязвимостей мобильных приложений на платформе Android/iOS должны проходить после того, как основной состав участников уже прошёл интерактивные и онлайн-тренинги по уязвимостям мобильных приложений на платформе Android/iOS.

Соревнования в формате захвата флага (CTF) ограничены по времени, поэтому участникам необходимо иметь возможность спланировать свое время на рабочей неделе, чтобы уделить достаточное для прохождения заданий время.

Проведение воркшопа по ASOC и воркшопа по Стингрей проводятся по запросу в рамках отведенного на этап времени.

* 1. **Формирование технического долга по информационной безопасности**

Для предоставления услуги по триажу (разбору дефектов) и выполнения работ по формированию технического долга ИБ, необходимо выполнение следующих условий:

* Предоставление инженерам Исполнителя удаленного доступа к инструменту оркестрации (ASOC).
* Предоставление инженерам Исполнителя удаленного доступа к инструментам сканирования, установленным в контуре Иннотех.
* Предоставление инженерам Исполнителя удаленного доступа к инструментам сканирования, установленным в контуре ПАО «ВТБ».
* Разбор срабатываний инструментов ИБ производиться из графического интерфейса инструмента оркестрации (ASOC), либо из графического интерфейса инструмента безопасной разработки.

Ограничения по объему выполняемых работ:

* Не более 600 уязвимостей в месяц (или 150 в рабочую неделю) уровня High/Critical.
* Если в результате сканирования уязвимостей уровня High/Critical не обнаружено, разбираются уязвимости уровня Medium/Low (не более 1600 уязвимостей в месяц или 400 в рабочую неделю).
* Разобранные уязвимости формируются в дефекты и могут быть выгружены в рабочее пространство Jira соответствующим командам разработки (при наличии такого пространства).
	1. **Разработка комплекса вспомогательных материалов**

Вспомогательные видеоматериалы предоставляются в виде коротких роликов (записи действий и устного комментария автора материала) длительностью от 5 – 30 минут.

Вспомогательные видеоматериалы не обязаны покрывать полный набор функций, доступный в рамках обозначенной темы.

Объем информации, представленной в вспомогательных видеоматериалах предназначен для быстрого усвоения информации и наглядного пособия для Security Champions.

Инструкции разрабатываются в формате коротких документов от 1-4 страниц, предназначенных для ускорения процесса онбординга команд в инструмент оркестрации ASOC.

* 1. **Продвижение бренда AppSec и Security Champion в «ГК Иннотех»**

Формат предоставления разрабатываемых рекомендаций по наполнению внутреннего информационного портала «ГК Иннотех» по умолчанию определяется Исполнителем, однако, он может быть скорректирован Заказчиком по требованию.

Выбор темы выступления в рамках проводимых внутренних митапов «ГК Иннотех» происходит либо по обоюдной договоренности сторон, учитывая пожелания Заказчика.

Выбранная тема выступления и прочие необходимые детали проводимого митапа должны быть переданы и согласованы с Исполнителем за 1 месяц до проведения мероприятия.

1. **ТРЕБОВАНИЯ К КОНФИДЕНЦИАЛЬНОСТИ**

Все результаты выполненных работ, черновые материалы, анкеты, схемы, статистические материалы, презентации, перечни выявленных дефектов ИБ и т.п., произведенные в результате выполнения работ в рамках настоящего ТЗ являются строго конфиденциальными и должны быть переданы Исполнителем по окончанию выполнения работ Заказчику.