Техническое задание на разработку электронных курсов для security champions

# **Цель закупки и эффект от закупки**

Цель закупки: подготовка комплексной программы обучения Security Champions, которая напрямую способствуют развитию экспертных знаний и формированию института Security Champions с исходниками в формате SCORM пакетов для публикации в СДО компании и последующего обучения сотрудников. Закупка необходима для углубления знаний и навыков базовых и продвинутых security champions в процессы безопасной разработки систем и сервисов ГК «Иннотех». На текущий момент внутренних ресурсов для развития навыков у security champions недостаточно.

Эффект от закупки: готовые интерактивные тренинги, которые дадут недостающие знания и навыки security champions для работы над проектами.

# **Требования к продукции и квалификации поставщиков**

Требования к содержанию курсов изложены ниже в таблице 1.

Поставщики должны иметь:

- опыт разработки учебных программ под задачи заказчиков, курсов для внутреннего обучения сотрудников в сфере кибербезопасности;

- при разработке курса должны участвовать практикующие эксперты в области кибербезопасности;

- поставщики должны иметь опыт в разработке программ для security champions;

- поставщики должны иметь лицензию на образовательную деятельность

# **Программа обучения**

*Таблица 1: содержание и объем курсов*

|  |  |  |  |
| --- | --- | --- | --- |
| **Курс** | **Объем курса** | **Количество** | **Содержание курса** |
| Основы информационной безопасности для Security Champion  | 3 ак.часа | 1 штука, без ограничения количества пользователей | Темы, которые должен раскрывать курс:* Основные термины и понятия ИБ.
* Три кита ИБ и во что они превращаются в процессах компании.
* Аутентификация, авторизация, аудит.
* Угрозы, уязвимости и риски.
* Основные угрозы безопасности и уязвимости.
* Распространенные уязвимости в ПО.
* Примеры реальных инцидентов.
* Безопасность в процессе разработки и эксплуатации.
* Роль и компетенции Security Champion.

Курс должен включать в себя промежуточное и итоговое тестирования |
| Основы нормативного регулирования информационной безопасности | 2 ак. часа | 1 штука, без ограничения количества пользователей | Темы, которые должен раскрывать курс:* Введение в нормативное регулирование информационной безопасности.
* Обзор нормативного регулирования в области ИБ.
* Виды регуляторов и их требования.
* Нормативные акты по защите ИБ в банковской сфере.
* Государственные стандарты и требования (ГОСТы)

Курс должен включать в себя не менее 1 итогового интерактивного задания на закрепление материала |
| Основы SSDLC | 5 ак.часов | 1 штука, без ограничения количества пользователей | Темы, которые должен раскрывать курс:* Введение в SDLC: что такое SDLC, этапы и инструменты; важность SDLC для разработки ПО
* Введение в SSDLC: что такое SSDLC; важность безопасности на каждом этапе SDLC
* Основы CI/CD и их роль в SSDLC:
* понятия и разница: Continuous Deployment, Continuous Delivery, Continuos Intergation; конвейер разработки CI/CD. Основные компоненты, инструменты; этапы CI/CD конвейера
* Угрозы безопасности и управление ими в CI/CD. Основные типы угроз.
* Инструменты для обнаружения и устранения угроз
* Примеры реальных атак и уязвимостей. Кейсы.

Курс должен включать 2-3 промежуточных и 1 итоговое тестирования |
| Моделирование угроз для разрабатываемых систем и процессов. Модели нарушителя | 3 ак. часа | 1 штука, без ограничения количества пользователей | Темы, которые должен раскрывать курс:* Что такое моделирование угроз и зачем оно нужно?
* Различные подходы моделирования угроз.
* Модели нарушителя. Применение модели нарушителя к процессу моделирования угроз.
* Выбор подхода для конкретного проекта.
* Интеграция моделирования угроз в SDLC.
* Работа с моделями угроз для составления мер митигации.

Курс должен включать не менее 2 кейсов на отработку полученных знаний, промежуточное тестирование. |
| Риск менеджмент в ИБ AppSec | 2 ак. часа | 1 штука, без ограничения количества пользователей | Темы, которые должен раскрывать курс:* Риск менеджмент в контексте ИБ.
* Виды рисков в ИБ, как ими управлять.
* Киберриски и угрозы ИБ.
* Оценка рисков и управление рисками
* Составление списка рисков и основных угроз для активов компании как процесс.
* Уязвимости как реализованные риски. Оценка критичности. Меры митигации и исправления

Курс должен включать не менее 2 кейсов на отработку полученных знаний, промежуточное тестирование. |
| Основы криптографии | 3 ак.часа | 1 штука, без ограничения количества пользователей | Темы, которые должен раскрывать курс:* Что такое криптография.
* Базовые принципы криптографии.
* Алгоритмы шифрования: Симметричные алгоритмы шифрования; ассиметричные алгоритмы шифрования.
* Цифровая подпись.
* Работа с ГОСТ алгоритмами шифрования.
* Выбор корректных алгоритмов исходя из поставленных задач.

Курс должен включать итоговое тестирование. |
| Основы по Identity and Access Management | 4 ак.часа | 1 штука, без ограничения количества пользователей | Темы, которые должен раскрывать курс:* Правила работы с контрагентами и источниками данных (с учетом особенностей написания кода).
* Ограничения сетей - allow list, WAF, SFTP, Firewall.
* Аутентификция клиентов - OIDC, token-based, mTLS, basic + sign.
* Проверка корректности данных - цифровая подпись данных, асинхронная передача с валидацией, двухфакторная проверка по мета - данных.
* Организация передачи данных нестандартными способами - почта, телеграм, SFTP, передача через фиды.
* Аутентификация и авторизация в системах
* Аутентификация различными способами - ADFS, OAuth/OIDC, локальные учетные записи, номер телефона, железные токены.
* Менеджмент пользователей систем - организация IAM, управление пользователями систем согласно принципам безопасности.
* Сессионный менеджмент в системах - cookie-based, HTTP headers, JWT.
* Организация безопасного подключения через второй фактор - OTP, tOTP, push notification, биометрия и др.
* Авторизация для разных целей - DACL, RBAC, ABAC. Проверка доступов централизовано/децентрализовано.

Курс должен включать не менее 2 кейсов на отработку тем курса, итоговое тестирование.  |
| Основы по Communication and Network Security | 3 ак.часа | 1 штука, без ограничения количества пользователей | Темы, которые должен раскрывать курс:* Введение в сетевую безопасность
* Основы сетей и их архитектура
* Сетевые топологии
* Протоколы и модели OSI и TCP/IP
* Типы сетей
* Основные компоненты сети. Сетевые устройства.
* Протоколы и их безопасность
* Инструменты и методы сетевой защиты
* Роль Communication and Network Security в SSDLC

Курс должен включать не менее 2 кейсов на отработку тем курса, также итоговое тестирование |

# **Сроки предоставления услуг**

Конечный срок предоставления электронных курсов - 06.12.2024 года

# **Форма оплаты услуг**

100% пост оплата

Оплата производиться отдельно за каждый курс после приемки курса Заказчиком и принятии всех корректировок.

# **Тесты, интерактивности, диалоговые тренажеры**

Тесты, интерактивности и диалоговые тренажеры должны быть разработаны так, чтобы результаты их прохождения, а также общая статистика прохождения курса слушателями могли быть выгружены отдельно.

# **Этапы разработки электронного курса**

|  |  |
| --- | --- |
| **№** | **Этап разработки**  |
| 1 | Разработка и согласование содержания курса с Заказчиком |
| 2 | Разработка и согласование концепции курса с Заказчиком |
| 3 | Разработка и согласование визуальной концепции курса с Заказчиком  |
| 4 | Разработка и согласование сценария курса с Заказчиком |
| 5 | Верстка курса в формате SCORM |
| 6 | Функциональное тестирование курса и корректорская проверка  |
| 7 | Согласование итоговой версии курса и приемка материалов  |
| 8 | Передача исходных файлов курса и закрывающей документации заказчику |
| 9 | Подписание закрывающих документов |