Бауманский учебный центр «Специалист»

Программа курса Социальная инженерия и защита от цифрового мошенничества

Код курса: **СОЦИНЖ**

Тема	Ак. часов
Модуль 1. Информационная безопасность и социальная инженерия • Терминология ИБ. • Обзор тактик и техник, используемых злоумышленниками. • Классификация средств защиты и основные инструменты, представленные на рынке. • Законодательство и стандарты обеспечения ИБ. • Понятие социальной инженерии и причины ее эффективности.	**2**
Модуль 2. Разведка и сбор информации • Мотивация и драйверы злоумышленника. • Предварительное обследование цели — способы и инструменты. • Обработка и обогащение полученных данных. • Подготовка к реализации атаки — этапы, очередность, эксплуатация, постэксплуатация. **Практикум 2.1** - Сбор информации с использованием OSINT-подхода (разведка через LinkedIn/Telegram, утечки через GitHub, HavelBeenPwned, DeHashed и т. д.). **Практикум 2.2** - Сбор информации о поддоменах и корпоративных сервисах организации. **Практикум 2.3** - Обогащение информации о выбранных целях атаки.	**4**
Модуль 3. Методы реализации атак и используемые технические средства • Фишинг почты и мессенджеров (классический, целевой, использование ИИ). • Вишинг (корпоративный, личный, сторонний). • Evil Twin Wifi (анализ траффика, перенаправление на фишинговые интерфейсы). • BadUSB (использование USB устройств для похищения информации). • Создание дубликатов аккаунтов мессенджеров и атака «Take over». • Техники QR-фишинга, AI-фишинга, MFA bypass. • Корпоративные коммуникации (Business Email Compromise, атаки через Teams/Slack/Zoom) • Генерация аудио- и видео-дипфейков с использованием ИИ. • Обзор ИИ-инструментов, применяемых злоумышленниками. • Физическое проникновение на объект. **Демонстрация:** Создание дублирующей корпоративной точки доступа и перенаправление на фишинговую страницу. **Практикум 3.1** - Анализ сообщений на наличие «красных флагов», сигнализирующих о фишинге. **Практикум 3.2** – Дипфейки: методы обнаружения, анализ кейсов, инструменты верификации.	**6**
Модуль 4. Методы защиты и реагирования на инциденты • Защита уровня сети (Zero Trust Architecture, Conditional Access). • MFA, устойчивая к атакам социальной инженерии (MFA-resistant phishing). • Защита конечных точек (EDR/XDR). • Защита электронной почты (DMARC/SPF/DKIM).	**2**

Модуль 5. Тестирование на проникновение и повышение осведомленности • Подготовка легитимной атаки (юридические аспекты). • Профайлинг, выбор методологии и критерии оценки. • Подготовка и тестирование инструментов атаки, создание сценария. • Проведение, анализ результатов, подготовка внутреннего отчета. • Подготовка материалов для повышения осведомленности сотрудников. • Методологии MITRE ATT&CK (Enterprise + Social Engineering techniques, Red Team, Purple Team).	**2**
Аудиторная нагрузка в классе с преподавателем	**16 ак.ч. + 16 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru