Приложение № 4
к образовательной программе среднего профессионального образования – программе подготовки специалистов среднего звена по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (на базе основного общего образования)

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «НАУЧНО-ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «СИРИУС»
(АНОО ВО «УНИВЕРСИТЕТ «СИРИУС»)

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«Тестирование на проникновение в области информационных технологий»

1. Трудоемкость профессионального модуля: 306 ак.ч.

2. Место профессионального модуля в учебном плане:

Профессиональный модуль «Тестирование на проникновение в области информационных технологий» входит в образовательный компонент программы П.00 «Профессиональный цикл» (ПМ.06) и является вариативным. Профессиональный модуль реализуется в 3-5 семестрах.

3. Цель профессионального модуля: сформировать у обучающихся профессиональные компетенции для проведения тестирования на проникновение (пентеста) — выявления и оценки уязвимостей информационных систем, моделирования атак злоумышленников и подготовки рекомендаций по повышению уровня защищённости ИТ-инфраструктуры.

4. Задачи профессионального модуля:

– освоить методологию и стандарты тестирования на проникновение: изучить подходы и этапы пентеста (разведка, сканирование, эксплуатация уязвимостей, постэксплуатация, составление отчёта), ознакомиться с международными стандартами (OSSTMM, PTES, NIST SP 800-115) и этическими нормами проведения тестов;

– приобрести навыки сбора информации и разведки (reconnaissance): научиться использовать инструменты пассивной и активной разведки (WHOIS, DNSenum, Shodan, Google Dorks), выявлять открытые сервисы и потенциальные точки входа в систему;

– овладеть методами сканирования уязвимостей и их эксплуатации: освоить работу с инструментами автоматизированного сканирования (Nmap, Nessus, OpenVAS), научиться выявлять и подтверждать уязвимости (в т.ч. CVE), отрабатывать техники эксплуатации (SQL-инъекции, XSS, RCE) в контролируемой среде;

– изучить техники тестирования веб-приложений и беспроводных сетей: научиться анализировать безопасность веб-интерфейсов (с использованием Burp Suite, OWASP ZAP), выявлять уязвимости аутентификации и авторизации, тестировать защиту Wi-Fi сетей (WPA2/WPA3), выполнять атаки на беспроводные протоколы;

– развить навыки документирования результатов и составления отчётов: освоить структуру отчётов по пентесту, научиться чётко описывать выявленные уязвимости, их риски и способы устранения, формулировать практические рекомендации по укреплению защиты, представлять результаты тестирования заказчику в понятной форме (включая технические детали и резюме для руководства).

5. Перечень разделов (тем) профессионального модуля и их краткое содержание:

Наименования разделов (тем) профессионального модуля	Содержание разделов (тем) профессионального модуля
МДК.06.01 Методы анализа и тестирования информационных систем	
Тема 1. Введение в тестирование на проникновение	Понятие и цели пентеста. Отличие от аудита безопасности и сканирования уязвимостей. Виды тестирования: «черный», «серый», «белый» ящики. Этические и правовые аспекты. Нормативные документы (NIST SP 800-115, PTES, OWASP).
Тема 2. Этапы тестирования на проникновение	Этапы: разведка, сканирование, эксплуатация, постэксплуатация, составление отчета.

Тема 3. Пассивный сбор информации (OSINT)	Источники открытых данных. Поиск информации о доменах, сотрудниках, инфраструктуре. Инструменты: theHarvester, Maltego, Recon-ng, Shodan, Censys.
Тема 4. Активный сбор информации. Сканирование сетей	Принципы работы протоколов TCP/IP. Сканирование портов (TCP SYN, TCP Connect, UDP). Обнаружение хостов. Идентификация ОС и сервисов. Инструменты: Nmap, Masscan, Zmap.
Тема 5. Анализ уязвимостей	Понятие уязвимости, CVE, CVSS. Базы данных уязвимостей (NVD, Exploit-DB). Сканеры уязвимостей: OpenVAS, Nessus, Nikto.
МДК.06.02 Виды и техники тестирования информационных систем	
Тема 1. Эксплуатация уязвимостей веб-приложений	OWASP Top 10. SQL-инъекции (ручные и автоматизированные). XSS (Reflected, Stored, DOM). CSRF, SSRF, Path Traversal. Инструменты: Burp Suite, sqlmap, OWASP ZAP.
Тема 2. Эксплуатация уязвимостей сетевых сервисов и ОС	Типовые уязвимости: SMB (EternalBlue), RDP, SSH, FTP. Подбор паролей (Hydra, Medusa, John the Ripper). Использование Metasploit Framework.
Тема 3. Социальная инженерия и фишинг	Методы сбора информации о сотрудниках. Создание фишинговых писем и поддельных страниц. Инструменты: Gophish, SET (Social-Engineer Toolkit).
Тема 4. Постэксплуатация и закрепление	Повышение привилегий (Linux и Windows). Снятие дампов паролей (Mimikatz, hashdump). Создание бэкдоров. Сокрытие следов.
Тема 5. Анализ трафика и Pivoting	Перехват и анализ сетевого трафика (Wireshark, tcpdump). Использование прокси и туннелей (chisel, ligolo). Перемещение по скомпрометированной сети.
Тема 6. Составление отчета о пентесте	Структура технического отчета. Описание найденных уязвимостей, уровней риска, рекомендаций по устранению.
УП.06.01 Учебная практика (Сетевая инфраструктура и кибербезопасность)	
Выполнение практических заданий по темам, изученным в МДК профессионального модуля. Закрепление освоенных навыков на учебных примерах	

6. Образовательные результаты освоения дисциплины (модуля):

Код и наименование компетенции	Результаты освоения дисциплины
ЛК-02. Использует современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	ИЛК-02.4. Выделяет основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте
	ИЛК-02.8. Знает и применяет информационные технологии (системы счисления, кодирование,

	алгебра логики, теория информации) для представления, преобразования и обработки данных в профессиональной деятельности
ПК-04. Применяет средства автоматизации для администрирования, управления инцидентами и настройки систем информационной безопасности	ИПК-04.1. Разрабатывает скрипты для автоматизации задач администрирования и безопасности
	ИПК-04.2. Осуществляет мониторинг и управление инцидентами в ИТ-системах
	ИПК-04.4. Применяет инструменты автоматизации для настройки средств защиты