РУКОН ЦЕЛЬ
МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ

Программа курса
«Этичный хакинг на Python: надень белую шляпу»

Модуль	Тема	Содержание	Вид учебных занятий	Объем в ак.ч.
Модуль 1. **Основы Python** Данный модуль посвящен изучению специализированных знаний по современному языку программирования Python: основ синтаксиса Python; сущности операторов и выражений; условных выражений и операторов, циклов и структур данных; функций в Python; рекурсии; встроенных функций Python. В качестве практики осваиваются навыки писать простейшие программы; создавать функции таблицы умножения; работать со списками; работать с модулями; создавать модули math_operations.py и	**Тема 1.1** **Введение в Python**	Введение в язык программирования Python: история, особенности, применение. Установка и настройка окружения для работы с Python. Синтаксис Python: переменные, типы данных, операторы, условные выражения, циклы. Ввод и вывод данных: работа с консолью, чтение и запись файлов. Функции и модули в Python: создание и использование функций, импорт и использование модулей. Обработка исключений: обработка ошибок и исключительных ситуаций в Python	теоретические занятия	2
		Написание программы, которая приветствует пользователя и запрашивает его имя. Затем программа выводит приветствие с использованием введенного имени. Написание программы, которая запрашивает у пользователя два числа и выводит их сумму, разность, произведение и частное	практические занятия	5
		Создание функции на Python, которая принимает число в качестве аргумента и выводит таблицу умножения для этого числа до 10	самостоятельная работа	1

string_operations.py; обрабатывать исключения; работать с путями файлов; писать программы для чтения и записи файлов.	**Тема 1.2 Синтаксис и основные конструкции языка**	Операторы и выражения: арифметические операторы, операторы сравнения, логические операторы. Условные выражения и операторы: if-else, elif, вложенные условия. Циклы: цикл while, цикл for, операторы break и continue. Структуры данных: списки, кортежи, словари, множества. Индексация и срезы: доступ к элементам списков, кортежей и строк	теоретические занятия	2
		Написание программы, которая проверяет, является ли введенное пользователем число четным или нечетным. Написание программы, которая выводит все числа от 1 до 10, кроме числа 3. Написание программы, которая запрашивает у пользователя список слов и выводит на экран только те слова, которые начинаются с буквы «а»	практические занятия	5
		Написание программы на Python, которая принимает список чисел и возвращает сумму всех элементов списка. Написание программы, которая запрашивает у пользователя список слов и выводит на экран только те слова, которые начинаются с буквы «о»	самостоятельная работа	1
	Тема 1.3 Функции и модули	Определение функций в Python: синтаксис, аргументы, возвращаемые значения. Локальные и глобальные переменные в функциях. Работа с модулями в Python: импорт модулей, использование функций и	теоретические занятия	2

		переменных из модулей. Создание собственных модулей в Python. Рекурсия: определение рекурсии, примеры рекурсивных функций. Встроенные функции Python: примеры использования встроенных функций.		
		Создание модуля math_operations.py, который содержит функции для выполнения математических операций: сложение, вычитание, умножение и деление. Использование этого модуля в программе для выполнения арифметических операций над двумя числами, введенными пользователем. (работа в парах или группах из 3-х, 4-х человек)	практические занятия	5
		Создание модуля string_operations.py, который содержит функции для работы со строками: подсчет количества символов, поиск подстроки, замена символов и т. д. Написание программы, которая использует функции из этого модуля для выполнения различных операций со строками, введенными пользователем	самостоятельная работа	1
	Тема 1.4 Работа с файлами и обработка исключений	Открытие и закрытие файлов: функция open (), режимы открытия файлов. Чтение данных из файла: методы. read (), .readline(), .readlines(). Запись данных в файл: метод. write (), .writelines(). Обработка исключений: блок try-except, обработка различных видов исключений. Блок finally: использование для выполнения кода в любом случае. Управление	теоретические занятия	2

		ресурсами с помощью менеджера контекста with. Работа с путями файлов: модуль os.path, получение информации о файле или директории		
		Написание программы, которая открывает текстовый файл data.txt, считывает его содержимое и выводит на экран. Создание программы, которая запрашивает у пользователя строку и записывает ее в текстовый файл output.txt. Написание программы, которая открывает текстовый файл data.txt, считывает его содержимое построчно и выводит только те строки, которые содержат определенное ключевое слово, введенное пользователем.	практические занятия	6
		Создание программы, которая копирует содержимое одного текстового файла в другой файл. Имена файлов должны быть заданы пользователем.	самостоятельная работа	2
	Аттестация по итогам модуля	выполнение учебной практической задачи		2
				Объем в ак.ч.	**Объем в %**
ИТОГО ПО 1 МОДУЛЮ:			теоретические занятия	8	22
			практические занятия	21	58

			самостоятельная работа	5	14
			аттестация	2	
			Всего:	**36**	
Модуль 2. **Основы этичного хакинга** В данном модуле осуществляется знакомство с основами этичного хакинга, его отличием от нелегальных действий злоумышленников; с хакерскими атаками; с основными методами и инструментами сбора информации и разведки; с принципами эксплуатации и защиты от атак; с методами обнаружения атак. В рамках модуля осваиваются навыки разработки скриптов для проверки безопасности сети на языке программирования Python; написания программы на Python для	**Тема 2.1 Основные понятия этичного хакинга**	Правовые основы информационной безопасности. Ответственность за противоправные действия. В каких случаях хакинг считается этичным. Международные стандарты, нормы отечественного законодательства (PCI DSS, 149-ФЗ, 187-ФЗ, 152-ФЗ). Как организована деятельность этичного хакера и как тренировать навыки информационной безопасности не нарушая закон. Определение этичного хакинга и его отличие от нелегальных действий. Кодекс этичного хакера и основные принципы. Виды хакерских атак и их классификация. Разрешенные и незаконные действия в рамках этичного хакинга. Сертификации и лицензии в области этичного хакинга	теоретические занятия	2	
		Разработка скрипта для проверки безопасности сети в контексте обеспечения информационной безопасности. Написание скрипта на Python, который будет сканировать указанный IP-адрес или диапазон адресов и проверять открытые порты для принятия решений о методах защиты и обеспечения информационной безопасности.	практические занятия	5	

извлечения информации о домене; проведения поисковых запросов и анализ результатов; разработки программ для эксплуатации и защиты.		Скрипт должен выводить информацию о найденных открытых портах и предлагать рекомендации по устранению уязвимостей.		
		Исследование и сравнение различных сертификаций в области этичного хакинга (например, CEH, OSCP, CISSP). Создание информационного доклада, который описывает каждую сертификацию, ее требования и преимущества, правовые аспекты.	самостоятельная работа	1
	Тема 2.2 Сбор информации и разведка	Информационная безопасности и основные методы сбора информации и разведки. Инструменты для сбора информации: поиск в открытых источниках, использование специализированных программ. Основы сетевого сканирования и анализа уязвимостей. Правовые и этические аспекты сбора информации и разведки.	теоретические занятия	2
		Написание программы на Python для извлечения информации о домене, которая будет принимать доменное имя и извлекать различную информацию о нем, такую как IP-адрес, WHOIS-данные, записи DNS и другие. Использование библиотек, таких как socket, python-whois и dnspython, для взаимодействия с соответствующими сервисами в контексте обеспечения информационной безопасности.	практические занятия	5

		Проведение поисковых запросов и анализ результатов. Составление списка заданных поисковых запросов и анализ результатов поиска. Оценка релевантности результатов, применение фильтров и расширенные операторы поиска для получения более точных и специфических результатов. Составление отчета о найденной информации и ее оценка для дальнейшего использования в деле обеспечения информационной безопасности.	самостоятельная работа	1
	Тема 2.3 Анализ уязвимостей	Принципы и методы анализа уязвимостей в сфере информационной безопасности. Инструменты для обнаружения уязвимостей: сканеры уязвимостей, инструменты анализа кода и т. д. Оценка и классификация уязвимостей. Отчетность и документирование уязвимостей. Правовые аспекты.	теоретические занятия	2
		Написание программы на Python для сканирования уязвимостей сети, которая будет сканировать сеть и идентифицировать уязвимые устройства или службы в контексте информационной безопасности. Использование библиотеки scapy для отправки и получения сетевых пакетов и анализа полученных ответов в деле обеспечения информационной безопасности.	практические занятия	5
		Исследование известных уязвимостей и угроз безопасности (выбор уязвимости или угрозы, например, Spectre или WannaCry, и	самостоятельная работа	1

		подготовка сообщения, в котором должен быть рассмотрен принцип ее работы, возможные последствия и рекомендации по защите от нее).		
	Тема 2.4 Эксплуатация и защита от атак	Основы эксплуатации уязвимостей в контексте информационной безопасности. Инструменты и методы эксплуатации. Защитные меры и техники обнаружения атак. Разработка и внедрение политик безопасности. Правовые аспекты.	теоретические занятия	2
		Освоение основных угроз информационной безопасности через разработку скрипта на Python для взлома слабого пароля, который будет использовать словарь паролей для попыток взлома учетных записей с использованием слабых паролей. (работа в парах или группах из 3-х, 4-х человек)	практические занятия	6
		Исследование и анализ известных уязвимостей и методов эксплуатации в контексте информационной безопасности. Изучение списка известных уязвимостей и методов эксплуатации, таких как буферное переполнение, инъекции кода, отказ в обслуживании (DoS) и другие. Создание отчета, с описанием каждой уязвимости, ее влияние на систему защиты от нее.	самостоятельная работа	2
	Аттестация по итогам модуля	Выполнение учебной практической задачи		2

				Объем в ак.ч.	Объем в %
ИТОГО ПО 2 МОДУЛЮ:			теоретические занятия	8	22
			практические занятия	21	58
			самостоятельная работа	5	14
			аттестация	2	
			Всего:	**36**	
Модуль 3. **Сетевая безопасность** В данном модуле в фокусе внимания - сетевая безопасность. Изучаются основные понятия и протоколы сетевого взаимодействия (IP, TCP, UDP, HTTP, HTTPS); основы анализа сетевого трафика и его роли в обеспечении безопасности; методы защиты сети и техники обнаружения атак;	**Тема 3.1 Основы сетевых протоколов**	Основные понятия и протоколы сетевого взаимодействия: IP, TCP, UDP, HTTP, HTTPS и другие в контексте информационной безопасности. Функции и особенности каждого протокола. Основные принципы маршрутизации и пересылки пакетов в сети. Правовые аспекты	теоретические занятия	2	
		Разработка клиент-серверного приложения на Python с использованием TCP протокола, в которой реализован клиент-серверный обмен данных с использованием TCP протокола для понимания вопросов обеспечения информационной безопасности в Интернет. (работа в парах, один ученик пишет клиентскую часть, а второй - серверную)	практические занятия	5	

принципы работы систем IDS и IPS; методы защиты от DDoS-атак; основные угрозы безопасности Wi-Fi сетей; виды шифрования Wi-Fi. Осваиваются навыки разработки клиент-серверного приложения на Python с использование TCP протокола; разработки программы на Python для сканирования сети и определения активных устройств; работы с инструментами анализа сетевого трафика (Wireshark); написания программы на Python с использованием библиотеки pcapy для анализа сетевого трафика; написания программы на Python для симуляции фаервола; написания программы на Python для сканирования Wi-Fi сетей и проведения аудита безопасности.		Освоение способов обеспечения информационной безопасности в контексте разработки программы на Python, которая будет сканировать сеть и определять активные устройства. Программа должна отправлять ICMP эхо-запросы (ping) на IP адреса в заданном диапазоне и анализировать полученные ответы для определения активных устройств. Выводы о значимости полученных навыков в деле обеспечения информационной безопасности.	самостоятельная работа	1
	Тема 3.2 Анализ сетевого трафика	Основы анализа сетевого трафика и его роли в обеспечении безопасности. Инструменты анализа сетевого трафика, такие как Wireshark. Анализ протоколов на разных уровнях модели OSI (Ethernet, IP, TCP, UDP) и распознавание типичных сетевых пакетов. Идентификация и анализ сетевых атак, таких как атаки отказа в обслуживании (DoS), атаки переполнения буфера и другие. Правовые аспекты использования данных инструментов.	теоретические занятия	2
		Инструмент Wireshark. Установка Wireshark на свой компьютер и проведение анализа сетевого трафика, захват пакетов на сетевых устройствах в контексте обеспечения информационной безопасности. Изучение содержимого пакетов на разных уровнях и анализ данных. Протоколы, адреса отправителей и получателей, порты и другие параметры. Правовые аспекты	практические занятия	5

		Написание программы на Python, которая будет анализировать сетевой трафик, захватываемый с использованием библиотеки pcapy в контексте безопасности. Программа должна просматривать захваченные пакеты и выводить информацию о протоколах, IP адресах отправителей и получателей, портах и других параметрах. Уточнение правовых аспектов.	самостоятельная работа	1
	Тема 3.3 Защита сети и обнаружение атак	Основные методы защиты сети: фаерволы, антивирусные программы, системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS). Техники обнаружения атак: сигнатурный анализ, аномальное поведение, статистический анализ. Принципы работы систем IDS и IPS. Использование сетевых масок для фильтрации трафика. Методы защиты от DDoS-атак.	теоретические занятия	2
		Написание программы на Python, которая симулирует фаервол, принимая сетевой трафик и применяя правила фильтрации для разрешения или блокировки пакетов. Возможна работа в парах или группах из 3-х, 4-х человек. Каждый член команды создает свою функцию или модуль программы, чтобы в дальнейшем объединить их все в общий скрипт на Python.	практические занятия	5
		Методы защиты от DDoS-атак. Разработка плана защиты от DDoS-атак для вымышленной компании, который включает	самостоятельная работа	1

		использование специализированных устройств и программного обеспечения.		
	Тема 3.4 Безопасность Wi-Fi сетей	Основные угрозы безопасности Wi-Fi сетей: перехват трафика, подмена точки доступа, атаки на протоколы аутентификации и шифрования. Методы защиты Wi-Fi сетей: использование безопасных протоколов, настройка сетевых устройств, управление доступом, использование виртуальных частных сетей (VPN). Различные виды шифрования Wi-Fi: WEP, WPA, WPA2, WPA3. Аудит безопасности Wi-Fi сетей и поиск уязвимостей.	теоретические занятия	2
		Написание программы на Python, которая сканирует доступные Wi-Fi сети и выводит информацию о них, включая уровень сигнала, тип шифрования и наличие защищенного пароля в контексте информационной безопасности. Реализация скрипта на Python, который проводит аудит безопасности Wi-Fi сети. Скрипт должен проверять уровень шифрования, наличие уязвимостей и давать рекомендации по улучшению безопасности.	практические занятия	6
		Проведение исследования безопасности Wi-Fi сети в собственном домашнем окружении. Описание проблем и уязвимостей, которые были обнаружены, и предложение меры по улучшению безопасности сети. Написание отчета, в котором детально описаны	самостоятельная работа	2

		найденные уязвимости и предложенные решения для их устранения.		
	Аттестация по итогам модуля	Выполнение учебной практической задачи		2
			Объем в ак.ч.	**Объем в %**
ИТОГО ПО 3 МОДУЛЮ:			теоретические занятия	8	22
			практические занятия	21	58
			самостоятельная работа	5	14
			аттестация	2	
			Всего:	**36**	
Модуль 4. **Веб-безопасность** Этот модуль посвящен освоению основных компонентов веб-приложений; протоколов передачи данных в вебе: HTTP и HTTPS; основных уязвимостей веб-	**Тема 4.1 Основы веб-разработки**	Информационная безопасности и веб-разработка. Основные компоненты веб-приложений: клиентская часть (HTML, CSS, JavaScript) и серверная часть (языки программирования, базы данных). Протоколы передачи данных в вебе: HTTP, HTTPS. Архитектура клиент-сервер и взаимодействие между клиентом и сервером в контексте информационной безопасности. Основные уязвимости веб-приложений: недостаточная валидация ввода,	теоретические занятия	2	

приложений и методов их защиты; кросс-сайтового скриптинга (XSS) и его основных принципов работы; различных типов XSS-атак и их потенциальных последствий; инъекций и уязвимостей баз данных; методов предотвращения XSS-атак и инъекций; методов защиты веб-приложений. В качестве практических навыков осваивается практика разработки веб-приложения с использованием фреймворка Flask на Python; разработки веб-страниц с уязвимостью к XSS-атаке; исследования различных типов XSS-атак и разработки демонстрационных страниц; разработки веб-страниц с уязвимостью к инъекциям; исследования различных типов инъекций баз данных; разработки и осуществления аудита		недостаточная обработка ошибок, уязвимости баз данных		
		Разработка простого веб-приложение с использованием фреймворка Flask на Python в деле обеспечения информационной безопасности. Приложение должно иметь форму для ввода данных от пользователя, а затем выводить их на веб-странице. Возможна работа в парах или группах из 3-х, 4-х человек. Каждый член команды создает свою функцию или модуль программы, чтобы в дальнейшем объединить их все в общий скрипт на Python	практические занятия	5
		Овладение методами защиты веб-приложений, такими как фильтрация ввода, санитизация данных и использование подготовленных запросов. Разработка документа с рекомендациями по обеспечению безопасности веб-приложений, включая примеры кода на Python и объяснения их работы	самостоятельная работа	1
	Тема 4.2 Кросс-сайтовый скриптинг (XSS)	Определение кросс-сайтового скриптинга (XSS) и его роль в обеспечении информационной безопасности. Основные принципы работы. Различие между хранимым (stored), отраженным (reflected) и межсайтовым (DOM-based) XSS. Уязвимые точки веб-приложений, которые могут быть использованы для XSS-атак. Виды XSS-атак	теоретические занятия	2

безопасности веб-приложений.		и их потенциальные последствия. Методы предотвращения XSS-атак		
		Разработка веб-страницы, на которой имеется уязвимость к XSS-атаке. Создание страницу с формой для ввода данных и выводом этих данных на странице используя Python и фреймворк Flask. Демонстрация, как можно провести XSS-атаку, внедрив вредоносный скрипт, и предложение мер по предотвращению такой атаки.	практические занятия	5
		Исследование различные типы XSS-атак (stored, reflected, DOM-based) и разработка набора демонстрационных страниц, которые иллюстрируют каждый из этих типов атак. Уточнение, как можно эксплуатировать уязвимости и предложение методов предотвращения каждого типа атаки	самостоятельная работа	1
	Тема 4.3 Инъекции и уязвимости баз данных	Введение в инъекции и уязвимости баз данных в контексте обеспечения информационной безопасности. Типы инъекций: SQL-инъекции, командные инъекции, NoSQL-инъекции. Уязвимые точки веб-приложений, которые могут быть использованы для инъекций. Потенциальные последствия инъекций баз данных. Методы предотвращения инъекций, включая использование подготовленных запросов, фильтрацию и санитизацию ввода, ограничение привилегий баз данных.	теоретические занятия	2

		Разработка простой веб-страницы с формой для ввода данных, которые будут использоваться для выполнения SQL-запроса к базе данных. Создание страницы, где пользователь может ввести свои данные и получить результат из базы данных используя Python и фреймворк Flask. Правовые аспекты	практические занятия	5
		Исследование различных типов инъекций баз данных (SQL, командные, NoSQL) и разработка демонстрационных приложений, которые иллюстрируют каждый из этих типов инъекций. Демонстрация, как можно эксплуатировать уязвимости и предложите методы предотвращения каждого типа инъекции.	самостоятельная работа	1
	Тема 4.4 Защита веб-приложений	Введение в защиту веб-приложений и ее важность. Основные угрозы и уязвимости веб-приложений, такие как перехват данных, подделка запросов, межсайтовый скриптинг (XSS), инъекции, утечки информации и другие. Методы защиты веб-приложений: валидация и санитизация ввода, использование безопасных архитектурных подходов, контроль доступа, защита от инъекций и уязвимостей баз данных, шифрование данных, управление сеансами и аутентификация, мониторинг и журналирование событий.	теоретические занятия	2

		Разработка простого веб-приложения с использованием фреймворка Flask. Проведение аудита безопасности приложения и выявление потенциальных уязвимостей. Предложения и реализация мер по усилению безопасности приложения, такие как валидация и санитизация ввода, контроль доступа	практические занятия	6
		Исследование различных методов аутентификации и авторизации веб-приложений, таких как многофакторная аутентификация, токены доступа и JSON Web Tokens (JWT).	самостоятельная работа	2
	Аттестация по итогам модуля	Выполнение учебной практической задачи		2
			Объем в ак.ч.	**Объем в %**
ИТОГО ПО 4 МОДУЛЮ:			теоретические занятия	8	22
			практические занятия	21	58
			самостоятельная работа	5	14
			аттестация	2	
			Всего:	**36**	

ИТОГОВАЯ АТТЕСТАЦИЯ (Защита итогового проекта)		**4**	
		Объем в ак.ч.	**Объем в %**
ИТОГО ПО ПРОГРАММЕ:	теоретические занятия	32	22
	практические занятия	84	57
	самостоятельная работа	20	13
	аттестация	12	
	Всего:	148	