Программа курса
«Этичный хакинг на Python: базовая безопасность»

Модуль (описание)	Тема	Содержание	Вид учебных занятий	Объем в ак.ч.
Модуль 1. Основы Python Данный модуль посвящен изучению сущности и преимуществ использования языка Python, выбору и установке интегрированной среды разработки, установке и запуску Python, освоению основных синтаксических конструкций языка; работе с различными типами данных, проведению операций над ними;	**Тема 1.1 Введение в программирование и Python**	Основы языка Python, преимущества использования Python, области применения, обзор синтаксиса Python. Установка Python, выбор и установка интегрированной среды разработки (например, PyCharm, IDLE), запуск Python и выполнения программы в выбранной среде разработки и интегрированной среды разработки. Основные синтаксические конструкции, понятия переменной и присваивания значений, базовые типы данных (числа, строки, списки) и их использование, обзор операций сложения, вычитания, умножения, деления и возведения в степень, примеры использования операций и работа с переменными.	теоретические занятия	2
		Написание программ для простых математических операций: для сложения двух чисел, для вычитания одного числа из другого, для умножения двух чисел, для деления одного числа на другое.	практические занятия	5
		Написание программы на Python, которая решает простую задачу: вычисление среднего значения чисел, процента от числа или простое уравнение.	самостоятельная работа	1

написанию программ на языке программирования Python.	**Тема 1.2 Работа с данными в Python**	Типы данных в Python (целые числа и числа с плавающей точкой), строки, списки и словари. Объявление и использование этих типов данных в программе. Операции над данными: арифметические операции, операции со строками. Условные операторы - принятие решений на основе определенных условий: if, elif, else.	теоретические занятия	2
		Работа с различными типами данных, операции над ними. Написание условных операторов для принятия решений в программе. Конвертер температуры, подсчет суммы чисел в списке.	практические занятия	5
		Создание программ, использующих различные типы данных и условные операторы для решения задач. Вычисление площади прямоугольника, проверка четности числа.	самостоятельная работа	1
	Тема 1.3 Функции и модули в Python	Основы создания функций в Python, передача аргументов в них. Использование ключевого слова "def" для определения функции, указание имени функции и списка аргументов в скобках. Изучение принципов передачи аргументов в функции.	теоретические занятия	2
		Создание и использование собственных функций, импорт модулей и использование стандартных функций Python. Написание генератора паролей. (работа в парах или группах из 3-х, 4-х человек)	практические занятия	5
		Доработка ранее написанных программ с использованием функций и модулей.	самостоятельная работа	1

	Тема 1.4 Работа с файлами и исключениями	Работа с файлами в Python. Чтение и запись данных. Методы открытия файлов, чтения и записи текстовых файлов. Основные операции с файловыми объектами. Концепции обработки исключений, предотвращение сбоев программы при возникновении ошибок, обеспечение гибкого управления ошибками и исключительными ситуациями.	теоретические занятия	2
		Работа с файлами, чтение и запись данных, обработка исключений для предотвращения ошибок в программе. Чтение содержимого файла и вывод на экран. Запись данных в файл. Обработка исключений при делении на ноль.	практические занятия	6
		Создание программ, которые манипулируют данными в файлах и корректно обрабатывают возможные исключения. Подсчет количества строк в файле. Копирование содержимого одного файла в другой.	самостоятельная работа	2
	Аттестация по итогам модуля	Тестирование		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 информационной безопасности и работа с сетями на Python В данном модуле осуществляется первое знакомство с основами информационной безопасности и ее базовыми понятиями, с сущностью этичного хакинга, с базовыми угрозами безопасности, с основными методами защиты. В рамках модуля осваиваются навыки по определению IP-адресов и подсетей с помощью Python; проводятся этичные тесты на проникновение, использование специализированных инструментов;	**Тема 2.1 Основы информационной безопасности**	Основные понятия в информационной безопасности. Конфиденциальность, целостность и доступность информации. 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. Понятие угроз. Виды угроз: вирусы, хакерские атаки и социальная инженерия. Уязвимости.	теоретические занятия	2
		Значение идентификации различных угроз информационной безопасности (вирусов, хакерских атак, фишинга) для обеспечения информационной безопасности. Определение потенциальных последствий. Описание возможности идентификации нескольких угроз и их последствий. (работа в парах или микрогруппах)	практические занятия	5
		Оценка уязвимостей (информационной системы, компьютера или мобильного приложения) в контексте информационной безопасности. Выявление потенциальных уязвимостей, связанных с физической безопасностью, сетевыми настройками, программным обеспечением и человеческим фактором.	самостоятельная работа	1

осуществляется настройка защиты от хакерских атак, создание безопасных паролей, шифрование файлов.	**Тема 2.2 Основы безопасности компьютерных сетей**	Методы защиты: использование паролей, шифрование данных, регулярное обновление программного обеспечения. Основные угрозы безопасности в информационных системах, включая вирусы, трояны, хакерские атаки и социальную инженерию. Брандмауэры и антивирусные программы как основные инструменты защиты.	теоретические занятия	2
		Определение IP-адресов и подсетей с помощью Python. Обнаружение открытых портов на хосте с помощью Python в контексте информационной безопасности.	практические занятия	5
		Обнаружение открытых портов на домашнем ПК с помощью написанного на Python скрипта. Удалось ли найти какие-либо.	самостоятельная работа	1
	Тема 2.3 Основы этичного хакинга	Понятие этичного хакинга. Вопросы этичности в деятельности специалиста по информационной безопасности. Вопросы защиты от хакерских атак. Типы хакерских атак (фишинг, вредоносные программы и перехват данных) и этичные методы тестирования на проникновение, используемые в проектах пентестеров.	теоретические занятия	2
		Проведение этичных тестов на проникновение, использование специализированных инструментов. Установка и настройка виртуальной машины bWAPP. Правовые аспекты работы с этими инструментами	практические занятия	5
		Проведение собственных исследований на предмет обнаружения уязвимостей на виртуальной машине bWAPP.	самостоятельная работа	1

	Тема 2.4 Защита от хакерских атак	Методы защиты от хакерских атак, включая использование брандмауэров, антивирусного программного обеспечения, обновление программ и операционных систем, аутентификацию на основе многофакторной аутентификации , принципы создания безопасных паролей, включая использование длинных и сложных паролей, комбинирование букв, цифр и специальных символов, избегание персональных данных и простых слов, шифрование данных и его роли в обеспечении конфиденциальности информации.	теоретические занятия	2
		Настройка защиты от хакерских атак, создание безопасных паролей, шифрование файлов. Написание программ на Python для определения ненадежных паролей и шифрования файлов.	практические занятия	6
		Проверка собственных паролей в написанной программе по проверке надежности паролей. Попытка шифрования и расшифровки тестовых файлов на домашнем ПК при помощи написанной программы.	самостоятельная работа	2
	Аттестация по итогам модуля	Тестирование		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. Веб-разработка и безопасность В данном модуле в фокусе внимания безопасность веб-сервисов. Изучается клиент-серверная архитектура; протоколы HTTP, HTTPS и их различия; основы HTML для структуры контента; язык стилей CSS; уязвимости веб-приложений; SQL-инъекции; XSS и CSRF-атаки; применение протокола HTTPS для безопасной передачи данных. Осваиваются навыки разработки веб-страниц; работы с HTML- и CSS-кодом; обнаружения и эксплуатации	**Тема 3.1 Основы веб-разработки**	Что такое клиент-серверная архитектура и каково ее место в обеспечении информационной безопасности. Протоколы HTTP, HTTPS и их различия, основы HTML для структуры контента. Язык стилей CSS.	теоретические занятия	2
		Создание простых веб-страниц, работа с HTML- и CSS-кодом. Создание заголовков и параграфов, добавление изображений, оформление текста с помощью CSS, создание простой навигации, создание формы. Поднятие собственного web-сервера на языке Python. Правовые аспекты. (работа в парах или группах из 3-х, 4-х человек).	практические занятия	5
		Разработка собственной веб-страницы с использованием изученных примеров на HTML и CSS.	самостоятельная работа	1
	Тема 3.2 Безопасность веб-приложений	Уязвимости веб-приложений, SQL-инъекции, XSS-атаки, CSRF-атаки в контексте информационной безопасности. Изучение сути возникновения уязвимостей, методы их поиска в тестируемом приложении. Лучшие практики, технические средства и методологии для устранения или минимизации риска от перечисленных уязвимостей в web-приложениях. Правовые аспекты.	теоретические занятия	2
		Обнаружение и эксплуатация уязвимостей на виртуальной машине bWAPP, принципы защиты от атак. Написание собственного приложения, уязвимого к атаке XSS, на Python. Уточнение правовых аспектов.	практические занятия	5

уязвимостей на виртуальной машине bWAPP; написания приложения, уязвимого к атаке XSS, на Python; использования различных алгоритмов хэширования паролей.		Проведение анализа безопасности общедоступных веб-приложений в сети Интернет для практики изученного материала по XSS и SQL-инъекциям (https://xss-game.appspot.com, http://sudo.co.il/xss/, https://sql.training.hackerdom.ru/).	самостоятельная работа	1
	Тема 3.3 Защита данных в веб-приложениях	Обеспечение информационной безопасности посредством паролей. Принципы и методы создания паролей в зашифрованном виде, включая симметричное и асимметричное шифрование. Лучшие практики создания паролей, включая использование длинных и сложных комбинаций символов. Методы хеширования для обеспечения безопасности паролей. Техники и методы безопасного хранения большого объема данных, включая меры, предотвращающие несанкционированный доступ и утечки информации. Применение протокола HTTPS для безопасной передачи данных между клиентом и сервером. Использование сертификатов SSL/TLS для защиты данных во время их транспортировки.	теоретические занятия	2
		Использование различных алгоритмов хэширования паролей для обеспечения информационной безопасности. Пример использования алгоритма хэширования паролей в Python. Применение шифрования данных, методы шифрования. Пример использования протокола HTTPS в Python. Правовые аспекты.	практические занятия	5
		Анализ методов защиты данных в веб-приложениях (с HTTPS и без) и разработка рекомендаций по повышению безопасности.	самостоятельная работа	1

	Тема 3.4 Этические аспекты веб-разработки	Этические принципы веб-разработки. Соблюдение законодательства и этических стандартов. Принципы защиты конфиденциальности информации. Этика использования данных.	теоретические занятия	2
		Разработка стандарта для ранее написанного веб-приложения с учетом изученного материала: этических аспектов, обеспечение конфиденциальности данных. Определение, какие из пунктов стандарта были соблюдены сразу, а какие еще необходимо добавить на сайт, чтобы он соответствовал всем пунктам. (работа в парах или группах из 3-х, 4-х человек)	практические занятия	6
		Анализ существующих веб-сайтов (например, сайт школы или учебного заведения) на предмет соблюдения этических принципов и разработка собственных рекомендаций.	самостоятельная работа	2
	Аттестация по итогам модуля	Тестирование		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. Практическое тестирование на проникновение с использованием Python Этот модуль посвящен освоению основ пентестинга; популярных инструментов для тестирования на проникновение, их возможностей и применения; основ скриптинга на Python, сканирования уязвимостей, эксплуатация уязвимых хостов; инструментов Nmap, Burp Suite, Hydra, Wireshark, dirb, sqlmap, metasploit framework. В качестве практических навыков	**Тема 4.1 Основы пентестинга и ручное тестирование**	Информационная безопасность и пентестинг. Понятие пентестинга. Типы атак: атаки на периметр, приложения, социальная инженерия, физические атаки. Фазы пентеста. Правовые аспекты пентестинга.	теоретические занятия	2
		Обеспечение информационной безопасности с использованием рабочей среды для тестирования на основе виртуальной машины DVWA, подготовка рабочей среды для тестирования на основе виртуальной машины DVWA, сбор информации о целевой системе. Определение и эксплуатация уязвимостей. Правовые аспекты.	практические занятия	5
		Работа по обеспечению информационной безопасности посредством дополнительного изучения виртуальной машины DVWA. Дополнительный сбор информации об используемых сервисах и попытка проведения ручного тестирования на проникновение в данной виртуальной среде.	самостоятельная работа	1
	Тема 4.2 Использование специализированных инструментов	Популярные инструменты для тестирования на проникновение, их возможности и применение. Операционная система Kali Linux и входящие в нее инструменты: Nmap, Burp Suite, Hydra, Wireshark, dirb, sqlmap, metasploit framework. Правовые аспекты использования этих инструментов в целях обеспечения информационной безопасности.	теоретические занятия	2

осваивается практика подготовки рабочей среды для тестирования на основе виртуальной машины DVWA; установки операционной системы Kali Linux на виртуальную машину; разработки скриптов на Python для автоматизации тестирования на проникновение; объединения различных инструментов в один рабочий скрипт с использованием специализированных библиотек для пентестинга.		Обеспечение информационной безопасности через работу с различными специализированными инструментами для тестирования на проникновение. Установка операционной системы Kali Linux на виртуальную машину. Подробное изучение инструментов Nmap, Burp Suite, Hydra, Wireshark, dirb, sqlmap, metasploit framework с применением их функционала на уязвимой виртуальной машине DVWA. Правовые аспекты использования этих инструментов в контексте информационной безопасности.	практические занятия	5
		Поиск уязвимостей на виртуальной машине DVWA, которые не рассматривались на практических занятиях с использованием полученных знаний и попытка их эксплуатации.	самостоятельная работа	1
	Тема 4.3 Автоматизация тестирования на проникновение с использованием Python	Автоматизация задач пентестинга для повышения эффективности обеспечения информационной безопасности. Основы скриптинга на Python. Сканирование уязвимостей или эксплуатация уязвимых хостов. Объединение различных инструментов в один рабочий скрипт с использованием специализированных библиотек для пентестинга, таких как Scapy, для манипуляции сетевыми пакетами или Requests для отправки HTTP-запросов. Правовые аспекты работы с этими инструментами для обеспечения информационной безопасности.	теоретические занятия	2

		Разработка скриптов на Python для автоматизации тестирования на проникновение в контексте информационной безопасности. Сканирование уязвимых хостов. Эксплуатация уязвимых хостов. Объединение инструментов в один рабочий скрипт. (работа в парах или группах из 3-х, 4-х человек)	практические занятия	5
		Создание собственных скриптов для автоматизации задач пентестинга для обеспечения информационной безопасности. Объединение перебора директорий и сбор активных страниц сайта.	самостоятельная работа	1
	Тема 4.4 Отчетность и рекомендации по устранению уязвимостей	Отчетность в сфере информационной безопасности. Цели и задачи. Составление отчетов о тестировании на проникновение, формулирование рекомендаций по устранению уязвимостей. Структура и содержание отчета о тестировании на проникновение. Процесс формулирования рекомендаций для устранения уязвимостей на основе результатов тестирования на проникновение.	теоретические занятия	2
		Создание совместного отчета о проведенных тестах на проникновение по трем выбранным уязвимостям в виртуальной машине DVWA, формулирование рекомендаций, обсуждение получившихся результатов с преподавателем. Правовые аспекты. (работа в парах или группах из 3-х, 4-х человек)	практические занятия	6
		Разработка собственного отчета о проведенном тестировании на проникновение гипотетической компании и предоставление рекомендаций по устранению уязвимостей. Самостоятельно выбрать любые 3 уязвимости и написать отчет.	самостоятельная работа	2
	Аттестация по итогам модуля	Тестирование		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**	