Программа курса
«Этичный хакинг на Python: The Art of Exploitation»

Модуль	Тема	Содержание	Вид учебных занятий	Объем в ак.ч.
Модуль 1. **Программирование на Python** Данный модуль посвящен изучению специализированных знаний по современному языку программирования Python: основных принципов работы с декораторами; принципов множественного наследования; понятия дескрипторов; потоков, однопоточное и многопоточное исполнение; синхронизацию потоков; параллельных вычислений; основ использования GUI в	**Тема 1.1 Обзор продвинутых возможностей Python**	Генераторы: создание и использование генераторов, выражения-генераторы. Декораторы: основные принципы работы с декораторами, использование декораторов функций и классов. Метаклассы: понятие метаклассов, создание и использование метаклассов. Множественное наследование: принципы множественного наследования, разрешение конфликтов. Дескрипторы: понятие дескрипторов, использование дескрипторов для управления доступом к атрибутам класса	теоретические занятия	2
		Реализация декоратора timer, который измеряет время выполнения функции и выводит результат в консоль. Создание генератора, который выводит последовательность чисел Фибоначчи до определенного предела.	практические занятия	5

программах; видов графических библиотек для Python. В качестве практики осваиваются навыки использовать принципы работы с декораторами для изменения поведения функций и классов; создавать и использовать генераторы в Python; работать с файлами (открытие, чтение, запись и закрытие файлов в Python); использовать контекстный менеджер with; создавать базу данных SQLite и таблицы в ней; добавлять новую запись в таблицу; создавать и управлять потоками; разрабатывать графические приложения с использованием выбранной библиотеки.		Создание генератора, который выводит последовательность простых чисел до определенного предела.	самостоятельная работа	1
	Тема 1.2 Работа с файлами и базами данных	Работа с файлами: открытие, чтение, запись и закрытие файлов; использование контекстного менеджера with для автоматического закрытия файла; перемещение указателя файла; чтение и запись текстовых и бинарных данных. Работа с базами данных: введение в базы данных, основные понятия (таблицы, поля, записи); подключение к базе данных; выполнение SQL-запросов (создание таблиц, вставка, обновление, удаление данных); чтение данных из базы данных; закрытие соединения с базой данных.	теоретические занятия	2
		Создание файла data.txt и запись в него строк. Чтение содержимого файла data.txt и вывод его в консоль. Создание базы данных SQLite и таблицу users с полями id, name и email. Добавление новой записи в таблицу users.	практические занятия	5
		Создание таблицы products в базе данных, содержащую поля id, name, price и quantity. Заполнение таблицы несколькими товарами.	самостоятельная работа	1

	Тема 1.3 Многопоточное программирование и параллельные вычисления	Понятие потоков: однопоточное и многопоточное исполнение; преимущества и недостатки многопоточности. Создание и управление потоками: использование модуля threading; создание потоков; запуск и остановка потоков; ожидание завершения потоков. Синхронизация потоков: проблемы совместного доступа к данным; блокировки (Lock); условные переменные (Condition); семафоры (Semaphore); очереди (Queue). Параллельные вычисления: использование модуля multiprocessing; создание и запуск процессов; обмен данными между процессами; пул процессов (Pool); распределенные вычисления.	теоретические занятия	2
		Создание потока, который выводит числа от 1 до 10 с задержкой в 1 секунду между выводом каждого числа. Реализация программы, которая создает 3 потока и каждый поток выводит свое имя 5 раз.	практические занятия	5
		Реализация программы, которая параллельно вычисляет сумму элементов в двух списках и выводит общую сумму. Написание программы, которая создает пул процессов и параллельно считает факториалы чисел от 1 до 10.	самостоятельная работа	1

	Тема 1.4 Разработка интерфейсов с использованием графических библиотек	Основные понятия GUI (графический интерфейс пользователя): окна, виджеты, события. Виды графических библиотек для Python: PyQt, Kivy. Разработка графических приложений с использованием выбранной библиотеки: создание главного окна приложения, размещение виджетов, обработка событий, стилизация интерфейса. Интеграция функциональности: работа с базами данных, файловой системой, сетевыми запросами. Оптимизация и улучшение интерфейса: многопоточность, асинхронные операции, анимация.	теоретические занятия	2
		Разработка приложения с использованием PyQt, которое позволяет пользователю вводить текст в поле ввода и выводит его в метке при нажатии кнопки. Создание интерфейса с использованием Kivy, который отображает список элементов и позволяет пользователю добавлять новые элементы в список.	практические занятия	6
		Разработка графического приложения с использованием выбранной графической библиотеки, которое позволяет пользователю создавать, сохранять и открывать файлы.	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. **Сетевые атаки и защита** В данном модуле осуществляется знакомство с понятием уязвимостей в сетевых протоколах и их классификации; с техникой анализа уязвимостей; с инструментами и программами для анализа уязвимостей; с методами защиты от уязвимостей в сетевых протоколах; с автоматизацией действий на Python; с расширенными методами перехвата и анализа сетевого трафика; с с ролью сниффинга в сетевых атаках; с	**Тема 2.1 Анализ уязвимостей в сетевых протоколах**	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 уязвимости в сетевых протоколах и их классификация. Техники анализа уязвимостей: сканирование портов, перехват и анализ сетевого трафика, исследование уязвимостей конкретных протоколов. Инструменты и программы для анализа уязвимостей: Nmap, Wireshark, Nessus, Metasploit. Понимание основных уязвимостей и способов их эксплуатации:	теоретические занятия	2	

принципами работы протокола ARP; с ARP-атаками; с методами обнаружения и предотвращения сетевых атак. В рамках модуля осваиваются навыки анализировать и фильтровать сетевой трафик; использовать инструменты для сниффинга и проведения ARP-атак; разрабатывать программ для проведения ARP-атак и анализа сетевого трафика; настраивать и управлять брандмауэром; разрабатывать программы для настройки VPN-соединения с использованием протокола IPsec; разрабатывать программы для фильтрации сетевого трафика на основе правил доступа.		отказ в обслуживании (DoS), переполнение буфера, подделка данных, атаки на протоколы аутентификации. Методы защиты от уязвимостей в сетевых протоколах: обновление программного обеспечения, настройка брандмауэра, использование шифрования, применение протоколов безопасности		
		Использование инструмента Nmap, для выполнения сканирования портов в локальной сети и нахождение открытых портов на определенных узлах. Перехват и анализ сетевого трафика для протокола HTTP и извлечение полезной информации, такой как заголовки запросов и ответов. Автоматизация приведенных действий на Python в контексте информационной безопасности. Правовые аспекты использования этих инструментов	практические занятия	5
		Написание программы на Python, которая сканирует указанный диапазон IP-адресов и определяет открытые порты и доступные сервисы на каждом узле	самостоятельная работа	1
	Тема 2.2 Продвинутые методы перехвата и анализа трафика	Обеспечение информационной безопасности и расширенные методы перехвата и анализа сетевого трафика. Использование снифферов для перехвата пакетов на сетевом уровне. Изучение протоколов на прикладном уровне: HTTP, FTP, DNS, SMTP. Анализ и фильтрация	теоретические занятия	2

		сетевого трафика с использованием специализированных инструментов, таких как Wireshark или tcpdump. Распознавание и анализ зашифрованного трафика с применением SSL/TLS. Идентификация и анализ сетевых атак, включая атаки типа Man-in-the-Middle, ARP-отравление, DNS-отравление		
		Реализация программы, которая перехватывает сетевой трафик на локальной машине и ищет подозрительную активность, такую как повышенное количество запросов на определенный порт или аномальный размер пакетов. Перехват зашифрованного сетевого трафика с использованием протокола HTTPS и анализ передаваемых данных в открытом виде, используя инструмент sslstrip, в контексте информационной безопасности. Правовые аспекты	практические занятия	5
		Изучение протокола DNS (Domain Name System) и его уязвимостей. Написание программы, которая перехватывает DNS-запросы и анализирует их содержимое, выявляя подозрительные запросы или изменения DNS-ответов.	самостоятельная работа	1

	Тема 2.3 Сниффинг и ARP-атаки	Сниффинг и обеспечение информационной безопасности. Роль сниффинга в сетевых атаках. Принципы работы ARP (Address Resolution Protocol) и его уязвимости. ARP-атаки, включая ARP-отравление (ARP poisoning) и ARP-перехват (ARP spoofing). Использование инструментов для сниффинга и проведения ARP-атак. Защитные меры от ARP-атак и обнаружение подмененных ARP-записей. Вопросы правомерности и этичности	теоретические занятия	2
		Для понимания сути обеспечения информационной безопасности, разработка программы, которая проводит ARP-отравление в локальной сети, подменяя MAC-адреса между двумя узлами. Вывод информации о перехватываемых пакетах и измененных ARP-записях. Написание программы, которая перехватывает и анализирует сетевой трафик в локальной сети, используя инструмент scapy. Вывод информации о принятых пакетах, идентификация ARP-пакетов и определение изменений в ARP-таблице. Вопросы правомерности и этичности действий	практические занятия	5
		Разработка инструмента для мониторинга ARP-таблицы и обнаружения подмененных записей. Программа должна	самостоятельная работа	1

		регулярно сканировать ARP-таблицу и оповещать администратора о возможной подмене MAC-адресов		
	Тема 2.4 Противодействие атакам и защита сетевых ресурсов	Основные принципы защиты сетевых ресурсов. Методы обнаружения и предотвращения сетевых атак, включая брандмауэры, системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS). Защита от атак типа отказ в обслуживании (DoS) и распределенных атак отказа в обслуживании (DDoS). Использование сетевых политик и фильтров для ограничения доступа к сетевым ресурсам. Протоколы безопасности, такие как IPsec и SSL/TLS, для защиты сетевых коммуникаций	теоретические занятия	2
		Написание программы для настройки и управления брандмауэром на компьютере. Реализация возможности блокировки входящего и исходящего сетевого трафика на основе определенных правил. Создание программы, которая настраивает VPN-соединение с использованием протокола IPsec. Программа должна запрашивать необходимые параметры (адрес сервера VPN, аутентификационные данные и т. д.) и устанавливать защищенное соединение.	практические занятия	6

		Разработка программы для фильтрации сетевого трафика на основе определенных правил. Программа должна позволять настраивать правила доступа для различных IP-адресов, портов и протоколов	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. **Веб-приложения и безопасность** В данном модуле в фокусе внимания - веб-приложения. Изучаются основные уязвимости веб-приложений; инструменты и методы обнаружения и эксплуатации	**Тема 3.1 Уязвимости веб-приложений и их эксплуатация**	Информационная безопасность и уязвимость веб-приложений. Обзор основных уязвимостей веб-приложений, таких как инъекции SQL, кросс-сайтовый скриптинг (XSS), кросс-сайтовая подделка запроса (CSRF). Механизмы эксплуатации уязвимостей, включая получение несанкционированного доступа к данным, выполнение произвольного кода и подмену сеансов. Понятие белого и черного ящиков в контексте анализа уязвимостей.	теоретические занятия	2

уязвимостей веб-приложений; SQL-инъекции; методы защиты от SQL-инъекций; принципы сессий и механизмов аутентификации; виды атак на сессии; методы безопасной аутентификации; стандарты безопасности, связанные с сессиями и аутентификацией; основные методы защиты от атак. Осваиваются навыки разрабатывать скрипты на Python для поиска и эксплуатации уязвимостей; разрабатывать систему фильтрации и санитизации пользовательского ввода; разрабатывать программы на Python для работы с базой данных; анализировать код веб-приложений на предмет уязвимостей SQL-инъекций; разрабатывать системы аутентификации на основе сессий; разрабатывать безопасные веб-приложения с использованием фреймворка Django; исследователь стандарты и формулировать рекомендации по безопасности		Инструменты и методы для обнаружения и эксплуатации уязвимостей веб-приложений, включая сканеры уязвимостей и прокси-серверы для перехвата и изменения трафика. Правовые аспекты.		
		Разработка скрипта на Python для автоматизированного поиска уязвимостей XSS на веб-сайте. Написание программы для эксплуатации уязвимости SQL-инъекции на веб-сайте.	практические занятия	5
		Разработка системы фильтрации и санитизации пользовательского ввода для защиты от уязвимостей XSS. Создание модуля, который будет проверять и очищать входные данные от потенциально опасных символов и скриптов перед их выводом на веб-страницу.	самостоятельная работа	1
	Тема 3.2 SQL-инъекции и защита баз данных	Обзор SQL-инъекций и их принципов работы. Различные типы SQL-инъекций, включая ошибки в SQL-синтаксисе, временные задержки и возвращение ошибок, бандл-инъекции и многое другое. Практические методы защиты от SQL-инъекций, такие как параметризация запросов, использование подготовленных выражений, ограничение прав доступа к базе данных и правильное санитизация и валидация пользовательского ввода.	теоретические занятия	2

веб-приложений; составлять отчет о мерах по защите веб-приложений		Создание простой базы данных с использованием SQLite и разработка программы на Python, которая позволит пользователям выполнять запросы к базе данных. Защита запросов от SQL-инъекций, используя параметризацию и подготовленные выражения	практические занятия	5
		Анализ кода веб-приложения и выявление уязвимости SQL-инъекций. Попытка эксплуатации этих уязвимостей. Предложения по реализации мер по устранению этих уязвимостей	самостоятельная работа	1
	Тема 3.3 Атаки на сессии и механизмы аутентификации	Основные принципы сессий и механизмов аутентификации в веб-приложениях. Сессии используются для установления и поддержания состояния между взаимодействиями клиента и сервера, а механизмы аутентификации проверяют подлинность пользователей. Различные виды атак на сессии, такие как перехват сессионных данных, подмена и подбор идентификаторов сессий, фиксация сессии и многое другое. Принципы безопасной аутентификации, включая использование сильных паролей, двухфакторной аутентификации, ограничение попыток входа и другие меры	теоретические занятия	2
		Разработка простой системы аутентификации на основе сессий веб-приложения с использованием фреймворка	практические занятия	5

		Flask. Защита сессионных данных от перехвата путем использования шифрования и подписи сессионных файлов. Изучение различных методов безопасной аутентификации, такие как двухфакторная аутентификация, включая использование одноразовых паролей или мобильных приложений аутентификации.		
		Изучение стандартов безопасности, связанных с сессиями и аутентификацией в веб-приложениях, таких как OWASP Top 10.	самостоятельная работа	1
	Тема 3.4 Защита веб-приложений и противодействие атакам	Основные методы защиты веб-приложений от атак, включая защиту от инъекций, кросс-сайтового скриптинга (XSS), подделки запросов межсайтовой подделки (CSRF) и других распространенных уязвимостей. Использование валидации данных и фильтрации входных параметров для предотвращения инъекций, таких как SQL-инъекции и командные инъекции. Применение контрмер CSRF, таких как генерация и проверка токенов CSRF при выполнении запросов, а также использование HTTP-заголовков, таких как SameSite и X-Frame-Options. Защита от XSS-атак путем эскейпинга и санитизации пользовательского ввода, а также использование контекстуальной безопасности при вставке данных в HTML-страницы.	теоретические занятия	2

		Разработка веб-приложения с использованием фреймворка Django и применение необходимых меры безопасности для защиты от инъекций и XSS-атак. Включение валидации и фильтрации данных, проверки типов и длины параметров, использование безопасных ORM-запросов и эскейпинг или санитизации пользовательского ввода при отображении на странице.	практические занятия	6
		Изучение стандартов и рекомендаций по безопасности веб-приложений, таких как OWASP Top 10 и CWE/SANS Top 25 Most Dangerous Software Errors. Составление отчета о наиболее важных мероприятиях по защите веб-приложений и противодействию распространенным атакам.	самостоятельная работа	2
	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. Продвинутые методы этичного хакинга Этот модуль посвящен освоению методов и инструментов, правовых и этических аспектов форензики; социальной инженерии и фишинга; типичных сценариев социальной инженерии; видов фишинга; методов анализа и обхода защиты системы; инструментов и программ для проведения анализа и обхода защиты системы; принципов безопасного проектирования систем; основных аспектов разработки безопасных приложений и систем. В качестве практических навыков осваивается практики создавать отчеты об анализе цифровых доказательств; составлять планы действий и процедур в случае инцидентов информационной безопасности; разрабатывать	**Тема 4.1 Форензика и судебная экспертиза**	Определение форензики и судебной экспертизы в контексте информационной безопасности. Роль форензики в обнаружении, сборе и анализе цифровых доказательств, связанных с компьютерными преступлениями. Применение методов и инструментов форензики для извлечения данных, восстановления удаленных файлов, анализа системных журналов и метаданных, а также идентификации следов деятельности злоумышленников. Правовые и этические аспекты форензики и предоставления цифровых доказательств в судебном процессе	теоретические занятия	2
		Создание отчета об анализе цифровых доказательств. Рассмотрение конкретного случая компьютерного преступления и разработка детального отчета, включающего информацию о методах анализа, найденных следах и рекомендации по предотвращению подобных инцидентов.	практические занятия	5
		Составление плана действий и процедур для проведения анализа в случае инцидента информационной безопасности, такого как взлом системы или утечка данных. Описание шагов, которые необходимо выполнить для	самостоятельная работа	1

методы защиты от социальной инженерии и фишинга; разрабатывать методы защиты от атак и повышения безопасности системы; создавать инструмент на Python для автоматического поиска и эксплуатации уязвимостей; проектировать механизмы аутентификации и авторизации		сбора и анализа цифровых доказательств, а также для восстановления нормальной работы системы		
	Тема 4.2 Социальная инженерия и фишинг	Определение социальной инженерии и фишинга в контексте информационной безопасности. Понимание принципов и методов социальной инженерии, которые используются для манипуляции людьми и получения конфиденциальной информации. Анализ типичных сценариев социальной инженерии, включая подборка информации, маскировку под легитимные лица, создание чрезвычайных ситуаций и другие тактики. Изучение различных видов фишинга, включая письма-перехватчики, фишинговые сайты, фишинговые звонки и другие формы атак. Разработка методов защиты от социальной инженерии и фишинга, включая обучение сотрудников, использование технических мер безопасности и мониторинг подозрительной активности	теоретические занятия	2
		С целью понимания механизмов действия злоумышленников для их предотвращения и обеспечения информационной безопасности, написание скрипта на Python для генерации фишингового электронного письма. Включение в письмо элементов	практические занятия	5

		социальной инженерии, например представление от имени известной организации или создание чрезвычайной ситуации, требующей срочных действий от получателя. Сохранение сгенерированного письма в виде HTML-файла и отправка его себе		
		Разработка уроков для сотрудников компании, которые включают презентации и задания для проверки знаний по противодействию атакам социальной инженерии	самостоятельная работа	1
	Тема 4.3 Анализ и обход защиты системы	Обзор методов анализа и обхода защиты системы с целью выявления уязвимостей и повышения безопасности. Изучение различных типов атак, включая брутфорс, словарные атаки, обход аутентификации и другие техники. Ознакомление с инструментами и программами, используемыми для проведения анализа и обхода защиты системы. Разработка методов защиты от атак и повышения безопасности системы	теоретические занятия	2
		Разработка инструмента на Python, используя библиотеку Metasploit, для автоматического поиска и эксплуатации уязвимостей в системе. Создание скрипта для обхода аутентификации на веб-сайте путем перебора пользовательских и паролей, используя библиотеку requests.	практические занятия	5

		Создание собственной уязвимой системы и тестирование ее на безопасность с использованием различных изученных методов и инструментов	самостоятельная работа	1
	Тема 4.4 Проектирование и реализация безопасных систем	Принципы безопасного проектирования систем, включая защиту от атак и уязвимостей. Основные аспекты разработки безопасных приложений и систем. Проектирование механизмов аутентификации и авторизации. Реализация механизмов шифрования и обеспечения конфиденциальности данных	теоретические занятия	2
		Разработка системы управления пользователями, которая обеспечивает безопасность паролей, храня их в хэшированном виде. Создание приложения для обмена зашифрованными сообщениями между пользователями с использованием асимметричного шифрования	практические занятия	6
		Разработка механизм безопасной передачи файлов по сети, используя протокол SSH и симметричное шифрование	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	