РУКОН ЦЕЛЬ
МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ

Программа курса
«Этичный хакинг: миг уникальности»

Элементы ДОП (модули и итоговый контроль/аттестация по ДОП)	Элементы модуля (темы, промежуточная аттестация)	Содержание (единицы содержания теоретической подготовки, практической работы, самостоятельной работы, контроля по теме и промежуточной аттестации (вопросы, задания, задачи и пр.)	Виды образовательных мероприятий /деятельности (теоретическая подготовка, практическая работа, самостоятельная работа, аттестация/контроль)	Объем в ак.ч
Модуль 1 Продвинутое программирование на Python с ИИ Описание модуля: Модуль посвящен изучению продвинутых возможностей Python, включая декораторы, множественное наследование, дескрипторы, работу с потоками, параллельные вычисления, основы GUI и графических библиотек. Практические навыки включают использование декораторов, генераторов, работу с файлами, контекстный менеджер, управление базами данных SQLite, многопоточность и разработку графических приложений с помощью ИИ. Цель модуля: Изучение и освоение продвинутых возможностей языка программирования Python с применением технологий искусственного интеллекта. Планируемые результаты: Освоение продвинутых возможностей Python, таких как работа с декораторами, генераторами, метаклассами, множественным наследованием и дескрипторами, приобретение навыков работы с файлами и базами данных SQLite, включая использование контекстного менеджера и выполнение	Инструменты Python для решения сложных задач	Изучение продвинутых возможностей Python: генераторов, декораторов, метаклассов, множественного наследования и дескрипторов, включая их создание, использование и применение для управления данными и атрибутами классов.	Теоретическая подготовка	2
		Реализация декоратора timer для измерения времени выполнения функции и создание генератора, выводящего последовательность чисел Фибоначчи до заданного предела.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Инструменты Python для решения сложных задач".	Текущий контроль	1
	Базы данных и обработка файлов на Python	Работа с файлами (открытие, чтение, запись, использование контекстного менеджера with) и базами данных (подключение, выполнение SQL-запросов, управление данными, закрытие соединения).	Теоретическая подготовка	2
		Создание и работа с файлом (запись и чтение данных) и базой данных SQLite (создание таблицы users, добавление записей).	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Базы данных и	Текущий контроль	1

SQL-запросов, освоение принципов многопоточного и параллельного программирования с использованием модулей threading и multiprocessing, а также получение практических навыков разработки графических интерфейсов с помощью библиотек PyQt и Kivy и применения технологий искусственного интеллекта для создания программного обеспечения. Типы задач/деятельности: Программные решения с использованием продвинутых возможностей Python, включая создание декораторов и генераторов для оптимизации работы функций, реализацию паттернов проектирования через множественное наследование и дескрипторы, решение задач многопоточности и параллельных вычислений для повышения производительности приложений, разработка графических интерфейсов с применением библиотек PyQt и Kivy для создания пользовательских приложений, а также интеграция технологий искусственного интеллекта для автоматизации процессов разработки и тестирования программного обеспечения.		обработка файлов на Python".		
	Основы параллельных вычислений и многопоточного программирования	Изучение многопоточного и параллельного программирования: создание и управление потоками с помощью модуля threading, синхронизации данных (Lock Condition, Semaphore, Queue), а также использование модуля multiprocessing для работы с процессами, обмена данными и распределенных вычислений.	Теоретическая подготовка	2
		Разработка программы для создания потоков: один поток выводит числа от 1 до 10 с задержкой в 1 секунду, а также реализуется программа, где три потока выводят свои имена по 5 раз.	Практические занятия	5
		Реализации программ: параллельное вычисление суммы элементов двух списков и использование пула процессов для параллельного расчета факториалов чисел от 1 до 10.	Самостоятельная работа	1
		Текущий контроль по теме "Основы параллельных вычислений и многопоточного программирования".	Текущий контроль	1
	Создание графических интерфейсов на Python и применению ИИ для разработки программ	Основы GUI (окна, виджеты, события), разработка графических приложений с использованием библиотек (PyQt, Kivy), интеграции функциональности (базы данных, файлы, сети), оптимизация интерфейса (многопоточность, асинхронность). Виды ИИ. GPT-модели. Способы взаимодействия с ИИ. Примеры генерации кода с помощью ИИ. Объяснение кода с помощью ИИ.	Теоретическая подготовка	2
		Основы GUI (окна, виджеты, события), разработка графических приложений с использованием библиотек (PyQt, Kivy), интеграции функциональности (базы данных, файлы, сети), оптимизация интерфейса (многопоточность, асинхронность). Виды ИИ. GPT-модели. Способы взаимодействия с ИИ. Примеры генерации кода с помощью	Практические занятия	6

		ИИ. Объяснение кода с помощью ИИ.		
		Разработка с помощью ИИ графического приложения на выбранной библиотеке, позволяющего пользователю создавать, сохранять и открывать файлы.	Самостоятельная работа	1
		Текущий контроль по теме "Создание графических интерфейсов на Python и применению ИИ для разработки программ".	Текущий контроль	1
	Промежуточная аттестация	Тестирование Форма промежуточной аттестации – зачет, который проводится в форме тестирования, состоящего из 20 вопросов, 15 вопросов – закрытого типа с выбором варианта ответа, где один вариант правильный и 5 вопросов – открытого типа, где необходимо вписать правильный ответ. Перечень вопросов составляется на основе изученного в процессе обучения материала по модулю. Время прохождение тестирования составляет 1 академический час.	Промежуточная аттестация	1
Модуль 2 Защита от сетевых атак с применением ИИ Модуль посвящен изучению уязвимостей сетевых протоколов, методов их анализа и защиты, работы с ARP-атаками, сниффингом и сетевыми атаками, а также освоению навыков анализа трафика, разработки программ для атак и защиты, настройки брандмауэра и управления VPN-соединениями через Ipsec, в том числе с помощью ИИ. Цель модуля: Изучение методов анализа и защиты сетевых протоколов, предотвращения сетевых атак и обеспечения безопасности сетевых ресурсов с использованием технологий искусственного интеллекта. Планируемые результаты: Освоение методов анализа и защиты сетевых протоколов, приобретение навыков работы с инструментами для сканирования портов и анализа трафика (Nmap, Wireshark), умение выявлять и предотвращать сетевые атаки (ARP-атаки,	Уязвимости сетевых протоколов и их анализ с помощью ИИ	Изучение уязвимостей сетевых протоколов, их классификация, методы анализа (сканирование портов, анализ трафика) с использованием инструментов (Nmap, Wireshark, Nessus, Metasploit), способы эксплуатации (DoS, переполнение буфера) и методы защиты (обновления, брандмауэр, шифрование, протоколы безопасности).	Теоретическая подготовка	2
		Использование Nmap для сканирования портов в локальной сети, перехват и анализ HTTP-трафика с извлечением данных (заголовки запросов и ответов) с помощью ИИ, а также автоматизации этих действий на Python.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Уязвимости сетевых протоколов и их анализ с помощью ИИ".	Текущий контроль	1
	Анализ и перехват трафика с применением ИИ	Рассматриваются расширенные методы перехвата и анализа сетевого трафика, использование снифферов, изучение	Теоретическая подготовка	2

сниффинг, DoS/DDoS), разработку программ на Python для мониторинга сетевой безопасности, настройки брандмауэров и управления VPN-соединениями с использованием IPsec, а также применение технологий искусственного интеллекта для автоматизации процессов обнаружения уязвимостей, анализа сетевого трафика и защиты сетевых ресурсов. Типы задач/деятельности: Анализ сетевых уязвимостей и протоколов с использованием инструментов сканирования, задачи на перехват и анализ сетевого трафика, практическое применение методов защиты от сетевых атак (настройка брандмауэров, фильтрация трафика), реализация программ для обнаружения ARP-атак и сниффинга, разработка решений для безопасной передачи данных через VPN и IPsec, а также автоматизация процессов анализа и защиты сетевых ресурсов с применением технологий искусственного интеллекта.		протоколов (HTTP, FTP, DNS, SMTP), фильтрация трафика с помощью Wireshark/tcpdump, анализ зашифрованного трафика (SSL/TLS) и выявление атак (Man-in-the-Middle, ARP-отравление, DNS-отравление).		
		Реализация программы для перехвата сетевого трафика на локальной машине, выявления подозрительной активности (например, аномалий в запросах или размерах пакетов), а также анализа зашифрованного HTTPS-трафика с помощью sslstrip и ИИ для изучения данных в открытом виде.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Анализ и перехват трафика с применением ИИ".	Текущий контроль	1
	ARP-атаки и сниффинг	Рассматриваются сниффинг и его роль в сетевых атаках, принципы работы ARP, уязвимости протокола, методы проведения ARP-атак (отравление, перехват), использование инструментов для сниффинга и защиты, а также способы обнаружения подмененных ARP-записей.	Теоретическая подготовка	2
		Разработка программы для ARP-отравления в локальной сети с подменой MAC-адресов и анализом перехваченных пакетов, а также создание решения с использованием ИИ и scapy для перехвата трафика, идентификации ARP-пакетов и отслеживания изменений в ARP-таблице.	Практические занятия	5
		Разработка инструмента с использованием ИИ для мониторинга ARP-таблицы и обнаружения подмененных записей, который регулярно сканирует таблицу и оповещает администратора о возможной подмене MAC-адресов.	Самостоятельная работа	1
		Текущий контроль по теме "ARP-атаки и сниффинг".	Текущий контроль	1
	Защита сетевых ресурсов	Рассматриваются основы защиты сетевых	Теоретическая	2

	с применением ИИ	ресурсов, включая брандмауэры, IDS/IPS, методы противодействия DoS/DDoS-атакам, использование сетевых политик и фильтров, а также применение протоколов безопасности (IPsec, SSL/TLS) для защиты коммуникаций.	подготовка	
		Разработка программы с помощью ИИ для настройки брандмауэра с возможностью блокировки трафика по заданным правилам, а также для установки VPN-соединения через IPsec с запросом параметров и аутентификационных данных.	Практические занятия	6
		Разработка программы с использованием ИИ для фильтрации сетевого трафика, позволяющую настраивать правила доступа по IP-адресам, портам и протоколам.	Самостоятельная работа	1
		Текущий контроль по теме "Защита сетевых ресурсов с применением ИИ".	Текущий контроль	1
	Промежуточная аттестация	Тестирование Форма промежуточной аттестации – зачет, который проводится в форме тестирования, состоящего из 20 вопросов, 15 вопросов – закрытого типа с выбором варианта ответа, где один вариант правильный и 5 вопросов – открытого типа, где необходимо вписать правильный ответ. Перечень вопросов составляется на основе изученного в процессе обучения материала по модулю. Время прохождение тестирования составляет 1 академический час.	Промежуточная аттестация	1
Модуль 3 Безопасность веб-приложений с применением ИИ В данном модуле в фокусе внимания - веб-приложения. Изучаются основные уязвимости веб-приложений; инструменты и методы обнаружения и эксплуатации уязвимостей веб-приложений; SQL-инъекции; методы защиты от SQL-инъекций; принципы сессий и механизмов аутентификации; виды атак на сессии; методы	Эксплуатация уязвимостей веб-приложений с помощью ИИ	Рассматриваются основные уязвимости веб-приложений (SQL-инъекции, XSS, CSRF), механизмы их эксплуатации, методы анализа (белый и черный ящик), а также инструменты для обнаружения уязвимостей и перехвата трафика (сканеры, прокси-серверы).	Теоретическая подготовка	2
		Разработка скрипта на Python с использованием ИИ для автоматизированного поиска уязвимостей	Практические занятия	5

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 веб-приложений; составлять отчет о мерах по защите веб-приложений. Показываются возможности ИИ для решения таких задач. Цель модуля: Изучение и освоение методов обеспечения безопасности веб-приложений с использованием технологий искусственного интеллекта Планируемые результаты: Освоение методов обнаружения и защиты от основных уязвимостей веб-приложений (SQL-инъекции, XSS, CSRF), приобретение навыков разработки скриптов на Python для поиска и эксплуатации уязвимостей с использованием ИИ, создание систем фильтрации и санитизации пользовательского ввода, разработку защищенных баз данных через параметризацию запросов и подготовленные выражения, проектирование безопасных систем аутентификации и управления сессиями с применением шифрования и подписи, а также освоение стандартов безопасности (OWASP Top 10) и методов противодействия атакам через валидацию данных, фильтрацию входных параметров, использование токенов CSRF и HTTP-заголовков. Типы задач/деятельности: Разработка и анализ веб-приложений на предмет уязвимостей		XSS путем отправки вредоносных данных и анализа ответов, а также программы для эксплуатации SQL-инъекций с целью несанкционированного доступа или изменения данных.		
			Самостоятельная работа	0
		Текущий контроль по теме "Эксплуатация уязвимостей веб-приложений с помощью ИИ".	Текущий контроль	1
	Защита баз данных с применением ИИ	Рассматриваются SQL-инъекции, их принципы работы и типы (синтаксические ошибки, временные задержки, бандлинъекции), а также методы защиты: параметризация запросов, подготовленные выражения, ограничение прав доступа и санитизация ввода.	Теоретическая подготовка	2
		Создание базы данных на SQLite и программы на Python с использованием ИИ для выполнения запросов, защищенных от SQL-инъекций через параметризацию и подготовленные выражения, а также применение sqlmap для автоматизированных атак на SQL-базы.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Защита баз данных с применением ИИ".	Текущий контроль	1
	Аутентификация и атаки на сессии с применением ИИ	Рассматриваются принципы работы сессий и аутентификации в веб-приложениях, виды атак на сессии (перехват, подмена, фиксация) и методы безопасной аутентификации, такие как использование сильных паролей, двухфакторная аутентификация и ограничение попыток входа.	Теоретическая подготовка	2
		Разработка с помощью ИИ системы аутентификации на основе сессий в Flask, обеспечивающей защиту данных через шифрование и подпись сессий, а так-же изучение методов безопасной аутентификации, включая двухфакторную авторизацию с одноразовыми паролями или мобильными	Практические занятия	5

(SQL-инъекции, XSS, CSRF) с использованием инструментов сканирования и эксплуатации, создание систем фильтрации и санитизации пользовательского ввода для защиты от атак, реализация безопасных механизмов работы с базами данных через параметризованные запросы и подготовленные выражения, проектирование защищенных систем аутентификации и управления сессиями с применением шифрования и подписи, а также разработка рекомендаций и отчетов по обеспечению безопасности веб-приложений на основе стандартов OWASP и других		приложениями.		
		Рассмотрение стандартов безопасности сессий и аутентификации в веб-приложениях, включая OWASP Top 10, и применение возможностей ИИ для проведения аудита безопасности.	Самостоятельная работа	1
		Текущий контроль по теме "Аутентификация и атаки на сессии с применением ИИ".	Текущий контроль	1
	Защита и противодействие атакам на веб-приложения с помощью ИИ	Рассматриваются методы защиты веб-приложений от инъекций, XSS, CSRF и других уязвимостей через валидацию данных, фильтрацию входных параметров, использование токенов CSRF, HTTP-заголовков (SameSite, X-Frame-Options), а также эскейпинг и санитизацию для предотвращения XSS-атак.	Теоретическая подготовка	2
		Разработка с помощью ИИ веб-приложение на Django, включая меры защиты от инъекций и XSS-атак через валидацию, фильтрацию данных, ORM-запросы, эскейпинг и санитизацию пользовательского ввода.	Практические занятия	6
		Изучение стандартов безопасности веб-приложений, такие как OWASP Top 10 и CWE/SANS Top 25, и составление с помощью ИИ отчета о ключевых мерах защиты и противодействия распространенным атакам.	Самостоятельная работа	1
		Текущий контроль по теме "Защита и противодействие атакам на веб-приложения с помощью ИИ".	Текущий контроль	1
	Промежуточная аттестация	Тестирование Форма промежуточной аттестации – зачет, который проводится в форме тестирования, состоящего из 20 вопросов, 15 вопросов – закрытого типа с выбором варианта ответа, где один вариант правильный и 5 вопросов – открытого типа, где необходимо вписать правильный ответ. Перечень вопросов составляется на основе изученного в	Промежуточная аттестация	1

		процессе обучения материала по модулю. Время прохождение тестирования составляет 1 академический час.		
Модуль 4 Комплексная безопасность информационных систем с применением ИИ В данном модуле рассматриваются методы и инструменты форензики, правовые и этические аспекты, социальная инженерия, фишинг, анализ и обход защиты систем, безопасное проектирование систем, а также практические навыки: создание отчетов по цифровым доказательствам, разработка инструментов на Python и проектирование механизмов аутентификации. Цель модуля: Формирование комплексного понимания методов обеспечения информационной безопасности и противодействия различным типам атак на информационные системы с использованием технологий искусственного интеллекта. Планируемые результаты: Освоение методов цифровой экспертизы и анализа киберинцидентов, приобретение навыков разработки мер защиты от манипулятивных атак (социальная инженерия, фишинг) с использованием ИИ, умение анализировать и обходить системы защиты для выявления уязвимостей, создание инструментов на Python для тестирования безопасности систем, разработку безопасных механизмов аутентификации и авторизации с применением шифрования данных, а также проектирование защищенных систем с учетом принципов конфиденциальности и целостности данных. Типы задач/деятельности: Анализ и сбор цифровых доказательств для расследования киберинцидентов, разработка мер защиты от атак социальной инженерии и фишинга с использованием ИИ, создание инструментов на Python для тестирования безопасности систем и обхода проектирование защищенных	Цифровая экспертиза с применением ИИ	Рассматриваются определение и отличия форензики и судебной экспертизы, роль форензики в сборе и анализе цифровых доказательств, методы извлечения данных, восстановления файлов и анализа метаданных, а также правовые и этические аспекты использования доказательств в суде.	Теоретическая подготовка	2
		Разработка с помощью ИИ отчета об анализе цифровых доказательств для конкретного случая компьютерного преступления, включающий методы анализа, найденные следы и рекомендации по предотвращению подобных инцидентов.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Цифровая экспертиза с применением ИИ".	Текущий контроль	1
	Манипулятивные атаки с применением ИИ	Рассматриваются социальная инженерия и фишинг, их принципы, методы и типичные сценарии, включая манипуляции и создание чрезвычайных ситуаций, виды фишинга (письма, сайты, звонки) и разрабатываются методы защиты через обучение, технические меры и мониторинг активности.	Теоретическая подготовка	2
		Разработка с помощью ИИ скрипта на Python для создания фишингового письма, включающего элементы социальной инженерии, такие как маскировка под известную организацию или создание срочной ситуации, с последующим сохранением письма в HTML-формате и отправкой его себе или сокурснику.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме	Текущий контроль	1

механизмов аутентификации и авторизации, реализация шифрования данных и обеспечение конфиденциальности, а также составление отчетов по анализу уязвимостей и рекомендаций по повышению уровня защищенности информационных систем.		"Манипулятивные атаки с применением ИИ".		
	Обход системы защиты и противодействие этому с помощью ИИ	Рассматриваются методы анализа и обхода защиты системы для выявления уязвимостей, включая атаки (брутфорс, словарные, обход аутентификации) и инструменты для их проведения, а также рассмотрение мер защиты и повышения безопасности системы.	Теоретическая подготовка	2
		Разработка с помощью ИИ инструмента на Python для автоматического поиска и эксплуатации уязвимостей через библиотеку Metasploit, а также создание скрипта для обхода аутентификации на веб-сайте методом перебора логинов и паролей с использованием библиотеки requests.	Практические занятия	5
		Разработка с помощью ИИ уязвимой системы для тестирования её безопасности с применением изученных методов и инструментов.	Самостоятельная работа	1
		Текущий контроль по теме "Обход системы защиты и противодействие этому с помощью ИИ".	Текущий контроль	1
	Безопасные системы с применением ИИ	Рассматриваются принципы безопасного проектирования систем, включая защиту от атак, разработку безопасных приложений, проектирование механизмов аутентификации и авторизации, а также реализацию шифрования и обеспечения конфиденциальности данных.	Теоретическая подготовка	2
		Разработка с помощью ИИ системы управления пользователями с хранением паролей в хэшированном виде и приложения для обмена зашифрованными сообщениями через асимметричное шифрование.	Практические занятия	6
		Разработка с помощью ИИ механизма безопасной передачи файлов по сети с использованием протокола SSH и симметричного шифрования.	Самостоятельная работа	1
		Текущий контроль по теме "Безопасные	Текущий контроль	1

		системы с применением ИИ".		
	Промежуточная аттестация	Тестирование Форма промежуточной аттестации – зачет, который проводится в форме тестирования, состоящего из 20 вопросов, 15 вопросов – закрытого типа с выбором варианта ответа, где один вариант правильный и 5 вопросов – открытого типа, где необходимо вписать правильный ответ. Перечень вопросов составляется на основе изученного в процессе обучения материала по модулю. Время прохождение тестирования составляет 1 академический час.	Промежуточная аттестация	1
Итоговый контроль/аттестация	Итоговый контроль/аттестация по ДОП	Представление итогового проекта Оценка итогового проекта осуществляется в соответствии с системой критериев. Каждый критерий оценивается по следующим рубрикаторам: • не соответствует критерию (0 баллов) • скорее соответствует, чем не соответствует критерию (1 балл) • скорее соответствует, чем не соответствует критерию (2 балла) полностью соответствует критерию (3 балла).	Итоговый контроль/аттестация	4

		Объем в ак.ч.	***Объем в %***
ИТОГО ПО ПРОГРАММЕ:	Теоретическая подготовка	32,00	21,62
	Практическая работа	84,00	56,76
	Самостоятельная работа	8,00	5,41
	Текущий контроль	16,00	10,81
	Промежуточная аттестация	4,00	2,70
	Итоговый контроль/аттестация	4.00	2,70
	Всего:	***148***	

ИТиСИ	Часы ИТиСИ не входят в общую трудоемкость ДОП, но участие в ИТиСИ обязательно для всех успешно прошедших итоговый контроль/аттестацию по ДОП