РУКОН ЦЕЛЬ
МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ

Программа курса
«Этичный хакинг: инструменты защиты на Python и ИИ»

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 Основы языка Python с применением ИИ Модуль посвящен изучению основ Python, включая синтаксис, операторы, выражения, циклы, структуры данных, функции и рекурсию, с практическим применением этих знаний для написания простых программ, работы со списками, модулями (например, math_operations.py, string_operations.py), обработки исключений, работы с файлами и и создания программ для чтения/записи данных с использованием ИИ. Цель модуля: Изучение базовых концепций и прикладных аспектов программирования на Python, включая основы синтаксиса, операторы, структуры данных, функции и модули, обработку исключений и работу с файлами, с последующим применением этих знаний для написания практических программ и использования возможностей искусственного интеллекта в программировании. Планируемые результаты: Применять базовые концепции программирования на Python, включая работу с переменными, типами данных, операторами, условиями, циклами, функциями, модулями и структурами данных, для написания	Основы Python	Введение в Python: история, особенности и применение языка, установка окружения, основы синтаксиса (переменные, типы данных, операторы, условия, циклы), работа с консолью и файлами, создание функций и использование модулей, а также обработка исключений для управления ошибками.	Теоретическая подготовка	2
		Написание программы, которая запрашивает имя пользователя и приветствует его, затем предлагает ввести два числа и выводит результаты их сложения, вычитания, умножения и деления.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Основы Python".	Текущий контроль	1
	Основные программные конструкции Python	Рассматриваются операторы и выражения в Python (арифметические, сравнения, логические), условные конструкции (if-else, elif, вложенные условия), циклы (while, for, break, continue), структуры данных (списки, кортежи, словари, множества) и работа с индексацией и срезами для доступа к элементам.	Теоретическая подготовка	2
		Написание программ, которые включают проверку числа на четность/нечетность, вывод чисел от 1 до 10 с пропуском числа 3 и фильтрацию слов, начинающихся на букву	Практические занятия	5

простых программ и скриптов; эффективно обрабатывать ошибки с помощью механизмов файловой системой, создавать собственные модули и использовать возможности искусственного интеллекта для генерации и оптимизации кода, что позволит им заложить прочную основу для дальнейшего изучения более сложных аспектов программирования и этичного хакинга. Типы задач/деятельности: Программы для выполнения базовых операций (арифметических вычислений, обработки строк, работы с файлами), создание функций и модулей для решения практических задач, реализация алгоритмов с использованием условий, циклов и структур данных (списков, словарей, множеств), разработка скриптов для обработки исключений и управления ошибками, а также выполнение задач по анализу и оптимизации кода с применением возможностей искусственного интеллекта.		"a", из списка, введенного пользователем.		
			Самостоятельная работа	0
		Текущий контроль по теме "Основные программные конструкции Python".	Текущий контроль	1
	Модули и функции языка Python	Рассматриваются определение функций в Python (синтаксис, аргументы, возвращаемые значения), локальные и глобальные переменные, работа с модулями (импорт, использование, создание собственных), рекурсия (определение и примеры) и применение встроенных функций.	Теоретическая подготовка	2
		Создание модуля math_operations.py с функциями для сложения, вычитания, умножения и деления, и использование его в программе для выполнения арифметических операций над числами, введенными пользователем.	Практические занятия	5
		Создание модуля string_operations.py с функциями для работы со строками (подсчет символов, поиск подстроки, замена) и программы, использующую этот модуль для выполнения операций над строками, введенными пользователем.	Самостоятельная работа	1
		Текущий контроль по теме "Модули и функции в Python".	Текущий контроль	1
	Обработка исключений и работа с файлами в Python, использование ИИ в программировании	Рассматриваются основы работы с файлами в Python (функция open(), режимы, методы чтения и записи), обработка исключений (try-except, finally), управление ресурсами через with, работа с путями (os.path), а также виды ИИ, GPT-модели, способы взаимодействия с ИИ и примеры его применения для генерации и объяснения кода.	Теоретическая подготовка	2
		Написание программы чтения файла data.txt и вывода его содержимого, записи пользовательской строки в файл output.txt, фильтрации строк из data.txt по ключевому слову, а также генерация кода вручную и с помощью ИИ с	Практические занятия	6

		последующим сравнительным анализом		
		Создание программы с помощью ИИ, которая копирует содержимое одного текстового файла в другой, используя имена файлов, заданные пользователем.	Самостоятельная работа	1
		Текущий контроль по теме "Обработка исключений и работа с файлами в Python, использование ИИ в программировании".	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 Базовые основы этичного хакинга и возможности ИИ для рутинных задач Модуль знакомит с основами этичного хакинга, включая отличия от нелегальных действий, методы сбора информации, принципы атак и защиты, а также обнаружение угроз, и развивает навыки написания Python-скриптов для проверки безопасности сети, анализа доменов, проведения запросов и разработки программ для эксплуатации и защиты, в том числе с применением ИИ. Цель модуля: Знакомство с основами этичного хакинга, включая его отличия от нелегальных действий, методы сбора информации, принципы атак и защиты, а также развитие навыков написания Python-скриптов для проверки безопасности сети, анализа доменов, проведения запросов и разработки программ для эксплуатации и защиты, с применением возможностей искусственного интеллекта для	Этичный хакинг с помощью ИИ	Понятие этичного хакинга, его отличие от нелегальных действий, ключевые принципы и кодекс хакера, классификация атак, разрешенные действия, а также сертификация и лицензии в данной области.	Теоретическая подготовка	2
		Разработка с помощью ИИ Python-скрипта для проверки безопасности сети, который сканирует указанный IP-адрес или диапазон, выявляет открытые порты и предоставляет рекомендации по устранению уязвимостей.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Этичный хакинг с помощью ИИ".	Текущий контроль	1
	Разведка и сбор информации с помощью ИИ	Рассматриваются методы и инструменты сбора информации (поиск в открытых источниках, специализированные программы), основы сетевого сканирования и анализа уязвимостей, а также правовые и этические аспекты разведки.	Теоретическая подготовка	2
		Создание с помощью ИИ Python-программы, которая извлекает информацию о домене (IP-адрес, WHOIS-	Практические занятия	5

автоматизации рутинных задач. Планируемые результаты: Знать различия этичного хакинга и нелегальных действий, понимать ключевые принципы и кодекс этичного хакера, классифицировать атаки и разрешенные действия, использовать Python-скрипты для проверки безопасности сети, анализа доменов, проведения запросов и разработки программ для эксплуатации и защиты, а также смогут применять мето-ды сбора информации, анализировать уязвимости с помощью инструментов и сканеров, разрабатывать защитные меры против распространенных уязвимостей (буферное переполнение, инъекции кода, DoS) и создавать детальные отчеты об уязвимо-стях и рекомендациях по защите с использованием возможностей искусственного интеллекта для автоматизации рутинных задач. Типы задач/деятельности: Задачи по анализу сетевой безопасности, включая сканирование IP-адресов и портов, выявление уязвимостей с использованием Python-скриптов и инструментов, сбор информации о доменах и DNS-записях, проведение исследований известных уязвимостей (буферное переполнение, SQL-инъекции, DoS), разработка программ для эксплуатации слабых паролей, создание отчетов об угрозах и рекомендациях по за-щите, а также применение искусственного интеллекта для автоматизации анализа данных и генерации кода.		данные, DNS-записи) с использованием библиотек socket, python-whois и dnspython для взаимодействия с сервисами.		
			Самостоятельная работа	0
		Текущий контроль по теме "Разведка и сбор информации с помощью ИИ".	Текущий контроль	1
	Уязвимости и их анализ с применением ИИ	Рассматриваются принципы и методы анализа уязвимостей, инструменты для их обнаружения (сканеры, анализаторы кода), оценка и классификация, а также отчетность и документирование выявленных проблем.	Теоретическая подготовка	2
		Создание с помощью ИИ Python-программы для сканирования уязвимостей сети, используя библиотеку scapy для отправки, получения и анализа сетевых пакетов с целью выявления уязвимых устройств или служб.	Практические занятия	5
		Исследование известных уязвимостей или угроз (например, Spectre, WannaCry), подготовка с помо-щью ИИ сообщения о принципе их работы, послед-ствиях и рекомендациях по защите.	Самостоятельная работа	1
		Текущий контроль по теме "Уязвимости и их анализ с применением ИИ".	Текущий контроль	1
	Защита от атак и эксплуатация уязвимостей с применением ИИ	Рассматриваются основы эксплуатации уязвимостей, инструменты и методы атак, защитные меры, техники обнаружения атак, а также разработка и внедрение политик безопасности.	Теоретическая подготовка	2
		Создание с помощью ИИ Python-скрипта для взлома слабых паролей, используя словарь для попыток авторизации в учетных записях с ненадежными паролями.	Практические занятия	6
		Исследование и анализ известных уязвимостей (буферное переполнение, инъекции кода, DoS и др.), создание с помощью ИИ детального отчета с описанием каждой уязвимости, её влияния на систему и способов защиты.	Самостоятельная работа	1
		Текущий контроль по теме "Защита от атак и эксплуатация уязвимостей с применением ИИ".	Текущий контроль	1
	Промежуточная	Тестирование	Промежуточная	1

	аттестация	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.	аттестация	
Модуль 3 Компьютерные сети и их безопасность с использованием ИИ Модуль посвящен сетевой безопасности: изучению протоколов (IP, TCP, UDP, HTTP, HTTPS), анализа трафика, методов защиты сети, систем IDS/IPS, противодействия DDoS и угроз Wi-Fi. Осваиваются навыки разработки клиент-серверных приложений, сканирования сети, анализа трафика с помощью Wireshark и библиотеки pcapy, симуляции фаервола, а также программ для аудита Wi-Fi сетей на Python, использование ИИ для анализа и усиления сетевой безопасности. Цель модуля: Изучение основ сетевой безопасности, включая протоколы IP, TCP, UDP, HTTP, HTTPS, принципы анализа трафика, методы защиты сети, системы IDS/IPS, противодействие DDoS и угрозам Wi-Fi, а также развитие навыков разработки клиентсерверных приложений, сканирования сети, анализа трафика с помощью Wireshark и библиотеки pcapy, симуляции фаервола и программ для аудита Wi-Fi сетей на Python с применением ИИ для анализа и усиления сетевой безопасности. Планируемые результаты: Понимать принципы работы основных сетевых протоколов (IP, TCP, UDP, HTTP, HTTPS), анализировать сетевой трафик с помощью инструментов типа Wireshark и библиотеки	Сетевые протоколы и применение ИИ для работы с ними	Рассматриваются основные протоколы сетевого взаимодействия (IP, TCP, UDP, HTTP, HTTPS), их функции и особенности, а также принципы маршрутизации и пересылки пакетов в сети.	Теоретическая подготовка	2
		Разработка с помощью ИИ клиент-серверного приложения на Python, реализующего обмен данными через TCP протокол.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Сетевые протоколы и применение ИИ для работы с ними".	Текущий контроль	1
	Инструменты анализа сетевого трафика, в том числе с ИИ	Рассматриваются основы анализа сетевого трафика для обеспечения безопасности, программа Wireshark, анализ протоколов на уровнях модели OSI, а также методы идентификации сетевых атак, таких как DoS и переполнение буфера.	Теоретическая подготовка	2
		Изучение инструмента Wireshark: установка, захват и анализ сетевого трафика, исследование содержимого пакетов на разных уровнях модели OSI, включая протоколы, адреса, порты и другие параметры.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Инструменты анализа сетевого трафика, в том числе с ИИ".	Текущий контроль	1
	Обнаружение сетевых атак и защита сети с помощью ИИ	Рассматриваются методы защиты сети, включая фаерволы, антивирусы, IDS и IPS, техники обнаружения атак	Теоретическая подготовка	2

pcapy, разрабатывать клиент-серверные приложения на Python, создавать программы для сканирования сети и анализа активных устройств, симулировать работу фаервола с правилами фильтрации трафика, применять методы защиты от DDoS-атак, проводить аудит безопасности Wi-Fi сетей, выявлять уязвимости в беспроводных соединениях и предлагать меры по их устранению, а также использовать возможности искусственного интеллекта для анализа сетевой безопасности, автоматизации процессов мониторинга и усиления защитных механизмов. Типы задач/деятельности: Задачи по анализу сетевого трафика с использованием инструментов типа Wireshark и библиотеки pcapy, разработка клиент-серверных приложений на Python для обмена данными через TCP/UDP протоколы, создание программ для сканирования сети и выявления активных устройств, симуляция работы фаервола с правилами фильтрации трафика, исследование методов защиты от DDoS-атак, проведение аудита безопасности Wi-Fi сетей, анализ уязвимостей в беспроводных соединениях и разработка рекомендаций по их устранению с применением искусственного интеллекта для автоматизации анализа и усиления сетевой безопасности.		(сигнатурный анализ, аномалии, статистика), принципы работы IDS/IPS, использование сетевых масок для фильтрации трафика и методы противодействия DDoS-атакам.		
		Создание с помощью ИИ программы на Python симуляции фаервола, которая обрабатывает сетевой трафик и применяет правила фильтрации для разрешения или блокировки пакетов.	Практические занятия	5
		Рассмотрение методов защиты от DDoS-атак и разработка с помощью ИИ плана для вымышленной компании, включающий использование специализированных устройств и программного обеспечения.	Самостоятельная работа	1
		Текущий контроль по теме "Обнаружение сетевых атак и защита сети с помощью ИИ".	Текущий контроль	1
	Wi-Fi сети и их безопасность с использованием ИИ	Рассматриваются угрозы безопасности Wi-Fi (перехват трафика, подмена точек доступа, атаки на протоколы), методы защиты (безопасные протоколы, настройка устройств, VPN), виды шифрования (WEP, WPA, WPA2, WPA3) и проведение аудита для выявления уязвимостей.	Теоретическая подготовка	2
		Создание с помощью ИИ программы на Python, которая сканирует Wi-Fi сети, выводит данные об уровне сигнала, типе шифрования и защите, а также реализация скрипта для аудита безопасности, проверяющего шифрование, выявляющего уязвимости и дающего рекомендации по их устранению.	Практические занятия	6
		Проведение исследования безопасности домашней Wi-Fi сети, выявление уязвимостей и предложение мер для их устранения, а затем составление с помощью ИИ отчета, детально описывающего найденные проблемы и рекомендации по улучшению защиты.	Самостоятельная работа	1
		Текущий контроль по теме "Wi-Fi сети и их безопасность с использованием 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 4 Безопасность Веб-приложений с применением ИИ Модуль посвящен изучению компонентов веб-приложений, протоколов HTTP/HTTPS, уязвимостей (XSS, инъекции баз данных) и методов защиты, а также освоению практических навыков: разработки веб-приложений на Flask, создания страниц с уязвимостями для исследования атак и проведения аудита безопасности с применением ИИ. Цель модуля: Изучение основных компонентов и уязвимостей веб-приложений, включая протоколы HTTP/HTTPS, архитектуры клиент-сервер, типов атак (XSS, SQL-инъекции и другие), методов защиты (валидация ввода, подготовленные запросы, фильтрация данных), а также развитие навыков разработки безопасных веб-приложений на Flask, создания демонстрационных страниц для исследования атак и проведения аудита безопасности с использованием возможностей искусственного интеллекта для анализа и усиления защиты веб-систем. Планируемые результаты: Понимать архитектуру веб-приложений, протоколы HTTP/HTTPS, основные уязвимости (XSS, SQL-инъекции и другие), методы их эксплуатации и защиты, разрабатывать безопасные веб-приложения на	Разработка веб-приложений с использованием ИИ	Рассматриваются основные компоненты веб-приложений (HTML, CSS, JavaScript) для клиента и для сервера, протоколы HTTP/HTTPS, архитектура клиент-сервер, а также ключевые уязвимости, такие как недостаточная валидация ввода, обработка ошибок и уязвимости баз данных.	Теоретическая подготовка	2
		Разработка простого веб-приложения на фреймворке Flask с формой для ввода данных пользователем и выводом этих данных на странице.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Разработка веб-приложений с использованием ИИ".	Текущий контроль	1
	Основы кросс-сайтового скриптинга (XSS) с применением ИИ	Рассматриваются основы кросс-сайтового скриптинга (XSS), включая его принципы работы, типы атак (stored, reflected, DOM-based), уязвимые места веб-приложений, возможные последствия и методы защиты от XSS.	Теоретическая подготовка	2
		Разработка веб-страницы с уязвимостью к XSS-атакам на Flask, демонстрация внедрения вредоносного скрипта через форму ввода данных и выбор методов защиты от таких атак.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Основы кросс-сайтового скриптинга (XSS) с применением ИИ".	Текущий контроль	1

Flask, создавать демонстрационные страницы для исследования атак, анализировать уязвимости баз данных, применять методы валидации ввода, подготовленных запросов и фильтрации данных, проводить аудит безопасности веб-приложений, использовать искусственный интеллект для анализа кода, выявления угроз и усиления защитных механизмов, а также разрабатывать рекомендации по защите от кибератак и внедрению современных методов аутентификации и авторизации. Типы задач/деятельности: Разработка веб-приложений на Flask с реализацией форм для ввода данных и вывода результатов, создание страниц с уязвимостями (XSS, SQL-инъекции) для исследования атак и методов защиты, анализ типов XSS-атак (stored, reflected, DOM-based) и разработка демонстрационных примеров для их иллюстрации, исследование различных видов инъекций (SQL, командные, NoSQL) с созданием программ для их выявления и предотвращения, проведение аудита безопасности веб-приложений с использованием ИИ для анализа угроз и внедрения защитных мер, таких как валидация ввода, подготовленные запросы и многофакторная аутентификация.	Базы данных и их уязвимости, защита от инъекций с помощью ИИ	Изучение инъекций и уязвимостей баз данных, включая SQL, командные и NoSQL-инъекции, их последствия, а также методы защиты с использованием подготовленных запросов, фильтрации ввода и ограничения привилегий.	Теоретическая подготовка	2
		Разработка веб-страницы с формой для ввода данных, которые используются для выполнения SQL-запросов к базе данных, с применением Python и ИИ для обработки данных и получения результатов.	Практические занятия	5
		Исследование типов инъекций (SQL, командные, NoSQL) и разработка с помощью ИИ демонстрационных приложений для их иллюстрации, анализа способов эксплуатации уязвимостей и методов их предотвращения.	Самостоятельная работа	1
		Текущий контроль по теме "Базы данных и их уязвимости, защита от инъекций с помощью ИИ".	Текущий контроль	1
	Веб-приложения и их защита с помощью ИИ	Основы защиты веб-приложений, включая анализ угроз (XSS, инъекции, перехват данных и др.) и методы защиты: валидация ввода, безопасные архитектурные подходы, контроль доступа, шифрование, управление сеансами и мониторинг событий.	Теоретическая подготовка	2
		Разработка веб-приложения на Flask, проведение аудита безопасности с помощью ИИ для выявления уязвимостей и реализации мер защиты, включая валидацию ввода и контроль доступа.	Практические занятия	6
		Исследование методов аутентификации и авторизации веб-приложений, включая многофакторную аутентификацию, токены доступа и JWT, с использованием ИИ для анализа их особенностей.	Самостоятельная работа	1
		Текущий контроль по теме "Веб-приложения и их защита с помощью ИИ".	Текущий контроль	1
	Промежуточная аттестация	Тестирование Форма промежуточной аттестации – зачет,	Промежуточная аттестация	1

		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.		
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