РУКОН ЦЕЛЬ
МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ

Программа курса
«Этичный хакинг: первые шаги с 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 Python для кибербезопасности и искусственный интеллект Модуль направлен на изучение основ языка Python, его ключевых особенностей и преимуществ. В рамках курса вы познакомитесь с выбором и настройкой интегрированной среды разработки (IDE), установкой и запуском Python. Вы освоите базовые синтаксические конструкции, научитесь работать с разными типами данных и выполнять операции над ними, а также создавать программы на Python. Цель модуля: Формирование базовых знаний и практических навыков работы с языком программирования Python, необходимых для применения в области кибербезопасности Планируемые результаты: Формирование компетенций в области программирования на Python для кибербезопасности: знания теоретических основ языка, навыки работы с различными типами данных и базовыми операциями, практические умения создания программ на Python, навыки работы с функциями и модулями языка, обработки исключений и работы с файлами, а также	Введение в Python: синтаксис, среды разработки	Введение в язык Python: основные особенности и преимущества его использования, сферы применения. Общее представление о синтаксисе языка. Установка Python на компьютер, выбор и настройка интегрированной среды разработки, а также запуск и выполнение программ в выбранной IDE. Рассмотрение базовых синтаксических конструкций, понятия переменных и присвоения им значений. Изучение простейших типов данных - числа, строки, списки - и операций над ними: сложение, вычитание, умножение, деление, возведение в степень. Практические примеры работы с переменными и использованием арифметических операций.	Теоретическая подготовка	2
		Создание программ для выполнения базовых математических операций: сложение, вычитание, умножение и деление чисел	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Введение в Python: синтаксис, среды разработки"	Текущий контроль	1
	Типы данных в Python и их применение	Основные типы данных в Python: целые числа, числа с плавающей точкой, строки, списки и словари. Объявление и работа с этими типами в программе. Выполнение различных операций: арифметические действия и	Теоретическая подготовка	2

понимание возможностей искусственного интеллекта при разработке программ. Создание программ для выполнения базовых математических операций, разработка простых приложений на Python для решения практических задач, работа с различными типами данных и условными операторами, написание пользовательских функций и использование модулей, выполнение операций с файлами и обработка исключений, а также задачи на применение искусственного интеллекта для генерации и анализа кода.		манипуляции со строками. Использование условных операторов (if, elif, else) для принятия решений в зависимости от заданных условий.		
		Различные типы данных, выполнение операций над ними. Создание условных конструкций для принятия решений в программе. Примеры практических задач: разработка конвертера температуры и вычисление суммы чисел в списке.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Типы данных в Python и их применение"	Текущий контроль	1
	Модули и функции языка Python	Ознакомление с основами создания функций в Python и передачей аргументов в них. Изучение использования ключевого слова def для определения функции, указания её имени и списка параметров. Рассмотрение принципов передачи аргументов при вызове функций	Теоретическая подготовка	2
		Разработка и применение пользовательских функций в Python, подключение модулей и использование встроенных стандартных функций языка. Создание программы-генератора паролей.	Практические занятия	5
		Доработка ранее написанных программ с использованием функций и модулей.	Самостоятельная работа	1
		Текущий контроль по теме "Модули и функции языка Python"	Текущий контроль	1
	Файлы и исключения в Python, использование ИИ при разработке программ на Python	Работа с файлами в языке Python: открытие, чтение и запись данных. Изучение основных методов работы с текстовыми файлами и операций над файловыми объектами. Введение в обработку исключений — защита программы от сбоев при возникновении ошибок и обеспечение гибкого управления исключительными ситуациями. Виды искусственного интеллекта, включая GPT-модели, способы взаимодействия с ИИ, а также практические примеры: использование	Теоретическая подготовка	2

		искусственного интеллекта для генерации программного кода и объяснения его работы.		
		Работа с файлами в Python: чтение данных и вывод их на экран, запись информации в файл. Применение механизма обработки исключений для предотвращения ошибок, включая деление на ноль. Освоение подходов к автоматической генерации кода с помощью ИИ и его сравнение с ручным способом написания программ	Практические занятия	6
		Разработка программ с использованием искусственного интеллекта, выполняющих обработку данных в файлах с корректной обработкой возможных исключений. Подсчёт количества строк в файле и копирование содержимого из одного файла в другой.	Самостоятельная работа	1
		Текущий контроль по теме "Файлы и исключения в Python, использование ИИ при разработке программ на Python"	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 Основы информационной безопасности с элементами ИИ и работа с компьютерными сетями В рамках данного модуля происходит первоначальное ознакомление с основами информационной безопасности: изучаются ключевые понятия, сущность этичного хакинга, базовые угрозы и методы защиты информации; осваиваются навыки	Ключевые концепции кибербезопасности	Введение в основные понятия информационной безопасности: конфиденциальность, целостность и доступность информации. Рассмотрение понятия угроз, их классификация и влияние на безопасность данных. Основные виды угроз — вирусы, хакерские атаки, методы социальной инженерии. Понятие уязвимостей и их роль в обеспечении информационной безопасности.	Теоретическая подготовка	2
		Ознакомление с различными угрозами	Практические занятия	5

определения IP-адресов и подсетей с использованием Python и искусственного интеллекта; способы настройки защиты от хакерских атак, создания надежных паролей, а также шифрования файлов. Цель модуля: Формирование базовых знаний и практических навыков в области информационной безопасности и работы с компьютерными сетями, включая применение технологий искусственного интеллекта. Планируемые результаты: Формирование комплексных компетенций в области информационной безопасности и работы с компьютерными сетями: теоретическое понимание ключевых концепций кибербезопасности, умение выявлять и анализировать различные типы угроз и уязвимостей, практические навыки определения IP-адресов и подсетей с помощью Python, обнаружения активных портов, проведения этичного тестирования на проникновение с использованием специализированных инструментов и виртуальной машины bWAPP, применения методов защиты от хакерских атак, создания надежных паролей и шифрования данных, а также навыки использования технологий искусственного интеллекта для анализа безопасности систем и разработки программных решений. Типы задач/деятельности: Выполнение практических заданий по анализу уязвимостей информационных систем, исследованию методов защиты от вирусов и хакерских атак, задач на определение IP-адресов и подсетей с использованием Python, обнаружение активных портов на удаленных хостах, проведение этического тестирования на проникновение с применением инструментов и технологий		информационной безопасности, такими как вирусы, хакерские атаки и фишинг. Определение возможных последствий воздействия этих угроз. Рассмотрение методов распознавания нескольких типов угроз и анализа их потенциального влияния на безопасность данных и систем.		
			Самостоятельная работа	0
		Текущий контроль по теме "Ключевые концепции кибербезопасности"	Текущий контроль	1
	Угрозы безопасности и инструменты для их обнаружения	Рассмотрение основных угроз безопасности в информационных системах, таких как вирусы, трояны, хакерские атаки и методы социальной инженерии. Изучение базовых способов защиты: применение надёжных паролей, шифрование данных, своевременное обновление программного обеспечения. Ознакомление с ролью брандмауэров и антивирусных программ как ключевых инструментов обеспечения информационной безопасности.	Теоретическая подготовка	2
		Определение IP-адресов и подсетей при помощи программ на Python. Обнаружение активных портов на удалённом хосте с использованием скрипта, написанного на Python и сгенерированного с помощью искусственного интеллекта.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Угрозы безопасности и инструменты для их обнаружения"	Текущий контроль	1
	Этичный хакинг: методы тестирования с помощью ИИ	Этичный хакинг как метод улучшения безопасности систем. Рассмотрение основных типов хакерских атак, таких как фишинг, использование вредоносных программ и перехват данных. Изучение этичных методов тестирования на проникновение, применяемых специалистами по защите информации (пентестерами) в рамках обеспечения	Теоретическая подготовка	2

искусственного интеллекта, реализация мер защиты от атак через создание надежных паролей и шифрование данных.		кибербезопасности.		
		Выполнение этических тестов на проникновение с использованием специализированных инструментов, включая средства на основе искусственного интеллекта. Установка и настройка виртуальной машины bWAPP для практического исследования уязвимостей и отработки навыков тестирования безопасности.	Практические занятия	5
		Выполнение самостоятельных исследований по выявлению уязвимостей на виртуальной машине bWAPP с использованием инструментов и технологий на основе искусственного интеллекта.	Самостоятельная работа	1
		Текущий контроль по теме "Этичный хакинг: методы тестирования с помощью ИИ"	Текущий контроль	1
	Защита от атак с использованием ИИ	Изучение основных методов защиты от хакерских атак: применение брандмауэров и антивирусного программного обеспечения, регулярное обновление операционных систем и приложений, использование многофакторной аутентификации. Рассмотрение принципов создания безопасных паролей — включая формирование сложных, длинных комбинаций с использованием букв, цифр и специальных символов, избегание личных данных и распространённых слов. Ознакомление с ролью шифрования данных в обеспечении конфиденциальности и защите информации.	Теоретическая подготовка	2
		Реализация мер защиты от хакерских атак, включая создание надёжных паролей и шифрование файлов. Разработка программ на языке Python с использованием ИИ для анализа паролей на устойчивость к взлому и выполнения операций шифрования данных.	Практические занятия	6
		Проверка собственных паролей с использованием разработанной программы для оценки их надёжности. Выполнение тестового шифрования и расшифрования	Самостоятельная работа	1

		файлов на домашнем компьютере как с помощью созданной программы, так и при помощи инструментов на основе искусственного интеллекта.		
		Текущий контроль по теме "Защита от атак 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 3 Веб-безопасность и ИИ: обнаружение уязвимостей В рамках данного модуля основное внимание уделяется безопасности веб-сервисов. Изучаются клиент-серверная архитектура, протоколы HTTP и HTTPS, их отличия, а также основы HTML для структурирования веб-контента и язык стилей CSS. Рассматриваются распространённые уязвимости веб-приложений, такие как SQL-инъекции, XSS- и CSRF-атаки, и способы защиты от них, включая использование протокола HTTPS для безопасной передачи данных. Обучающиеся осваивают навыки разработки веб-страниц, работы с HTML и CSS, выявления и анализа уязвимостей на виртуальной машине bWAPP создания простого веб-приложения на Python, уязвимого к XSS-атаке, а также применения различных алгоритмов хэширования паролей. Цель модуля: Формирование знаний и	Основы веб-разработки с применением ИИ	Рассмотрение клиент-серверной архитектуры, основных протоколов передачи данных — HTTP и HTTPS, а также их ключевых различий. Изучение базовых понятий языка HTML для определения структуры веб-контента и каскадных таблиц стилей (CSS) для оформления и форматирования веб-страниц.	Теоретическая подготовка	2
		Разработка простых веб-страниц и работа с HTML- и CSS-кодом: создание заголовков и параграфов, добавление изображений, стилизация текста с помощью CSS, реализация базовой навигации и форм. Настройка и запуск собственного веб-сервера на языке Python. Использование искусственного интеллекта для генерации кода и ускорения разработки.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Основы веб-разработки с применением ИИ"	Текущий контроль	1
	XSS, SQL-инъекции, и другие атаки: как ИИ помогает в защите	Изучение распространённых уязвимостей веб-приложений, таких как SQL-инъекции, XSS- и CSRF-атаки. Рассмотрение причин возникновения данных уязвимостей и методов их обнаружения в тестируемых приложениях. Ознакомление с лучшими практиками,	Теоретическая подготовка	2

практических навыков в области обеспечения безопасности веб-приложений с использованием технологий искусственного интеллекта. Планируемые результаты: Формирование компетенций в области веб-безопасности и применения технологий искусственного интеллекта: теоретическое понимание принципов работы веб-приложений, клиент-серверной архитектуры, протоколов HTTP/HTTPS, основ HTML и CSS, навыки практической разработки веб-страниц, выявления и анализа уязвимостей (SQL-инъекции, XSS, CSRF) с использованием виртуальной машины bWAPP, создания Python, применения различных методов шифрования и хэширования паролей, а также знание этических аспектов веб-безопасности. Типы задач/деятельности: Разработка простых веб-страниц с использованием HTML и CSS, задачи на выявление и анализ уязвимостей (SQL-инъекции, XSS, CSRF) с применением виртуальной машины bWAPP, создание уязвимых веб-приложений на Python для исследования методов атак, реализация алгоритмов хэширования паролей и шифрования данных, задачи на сравнение безопасности передачи данных через HTTP и HTTPS, а также разработка рекомендаций по обеспечению этических стандартов и защиты конфиденциальности в веб-приложениях.		технических средствами и методологиями, направленными на устранение или минимизацию рисков, связанных с указанными типами уязвимостей в веб-приложениях.		
		Выявление и исследование уязвимостей на виртуальной машине bWAPP, изучение методов их эксплуатации и принципов защиты от различных типов атак. Разработка собственного веб-приложения на языке Python, уязвимого к XSS-атаке, с использованием искусственного интеллекта для поддержки в написании кода.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "XSS, SQL-инъекции, и другие атаки: как ИИ помогает в защите"	Текущий контроль	1
	Шифрование и безопасное хранение данных с применением ИИ	Рассматриваются принципы создания паролей с использованием симметричного и асимметричного шифрования, современные методы хеширования для их защиты, а также рекомендации по формированию надежных паролей, включая применение длинных и сложных комбинаций символов; изучаются техники безопасного хранения данных, направленные на предотвращение несанкционированного доступа и утечек, и описываются механизмы обеспечения безопасности при передаче данных через протокол HTTPS и использование SSL/TLS-сертификатов.	Теоретическая подготовка	2
		Рассматривается применение различных алгоритмов хэширования паролей, включая пример реализации такого алгоритма в Python с помощью искусственного интеллекта, а также изучаются методы шифрования данных и приводится пример использования протокола HTTPS в Python для обеспечения безопасной передачи информации.	Практические занятия	5
		Анализ способов защиты данных в веб-приложениях с использованием HTTPS и без	Самостоятельная работа	1

		него, а также разработка ИИ-рекомендаций для улучшения их безопасности.		
		Текущий контроль по теме "Шифрование и безопасное хранение данных с применением ИИ"	Текущий контроль	1
	Этические аспекты веб-безопасности с использованием ИИ	Этические принципы веб-разработки, включая соблюдение законодательства и этических норм, обеспечение защиты конфиденциальности данных и ответственное использование информации.	Теоретическая подготовка	2
		Разработка стандарта для существующего веб-приложения с учетом этических аспектов и конфиденциальности данных, анализ соблюдения требований стандарта и выявление необходимых доработок для полного соответствия. Применение ИИ для проведения аудита безопасности сайта.	Практические занятия	6
		Анализ веб-сайтов учебных заведений на соответствие этическим принципам и разработка рекомендаций по их улучшению с использованием ИИ.	Самостоятельная работа	1
		Текущий контроль по теме "Этические аспекты веб-безопасности 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 Практический пентестинг с Python и ИИ Модуль посвящен основам пентестинга, включая изучение популярных инструментов (Nmap, Burp Suite, Hydra, Wireshark, sqlmap), скриптинга на Python, сканирования уязвимостей и эксплуатации	Основы пентестинга: ручное и автоматизированное тестирование с ИИ	Пентестинг и его фазы. атаки на периметр, приложения, социальная инженерия, физические атаки.	Теоретическая подготовка	2
		Подготовка рабочей среды на базе виртуальной машины DVWA, сбор данных о целевой системе и выявление уязвимостей для их последующей эксплуатации.	Практические занятия	5

хостов. Практические навыки включают настройку рабочей среды на базе DVWA, установку Kali Linux, разработку автоматизированных скриптов с помощью ИИ и объединение инструментов в единый рабочий процесс с использованием специализированных библиотек. Цель модуля: Формирование практических навыков проведения тестирования на проникновение с использованием языка Python, специализированных инструментов и технологий искусственного интеллекта. Планируемые результаты: Формирование комплексных компетенций в области практического пентестинга: теоретическое понимание фаз и типов атак, навыки работы с инструментами в среде Kali Linux, умение настраивать рабочую среду на базе DVWA, автоматизировать задачи пентестинга через скриптинг на Python с использованием библиотек (Scapy, Requests), создавать комплексные решения для тестирования безопасности путем объединения различных инструментов, анализировать результаты тестирования, составлять детальные отчеты и формулировать рекомендации по устранению уязвимостей с применением технологий искусственного интеллекта для оптимизации процессов сбора данных, анализа уязвимостей и генерации отчетов Типы задач/деятельности: Выполнение практических задач по настройке рабочей среды на базе DVWA, сканированию уязвимостей с использованием инструментов Kali Linux, разработке автоматизированных скриптов на Python для тестирования на проникновение, анализу результатов и составлению отчетов с применением технологий искусственного интеллекта для оптимизации процессов сбора данных, выявления уязвимостей и формулирования			Самостоятельная работа	0
		Текущий контроль по теме "Основы пентестинга: ручное и автоматизированное тестирование с ИИ"	Текущий контроль	1
	Инструменты для пентеста, включая ИИ	Обзор популярных инструментов для тестирования на проникновение, их возможностей и применения, включая инструменты операционной системы Kali Linux: Nmap, Burp Suite, Hydra, Wireshark, dirb, sqlmap и Metasploit Framework.	Теоретическая подготовка	2
		Работа со специализированными инструментами для тестирования на проникновение, включая установку Kali Linux на виртуальную машину и детальное изучение инструментов Nmap, Burp Suite, Hydra, Wireshark и sqlmap с их применением на уязвимой виртуальной машине DVWA, при этом ИИ используется как помощник для работы с этими инструментами.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Инструменты для пентеста, включая ИИ"	Текущий контроль	1
	Автоматизация пентестинга на Python с использованием ИИ	Автоматизация пентестинга через скриптинг на Python, включая сканирование уязвимостей и эксплуатацию хостов, с объединением инструментов в единый скрипт с использованием библиотек, таких как Scapy для работы с сетевыми пакетами или Requests для HTTP-запросов.	Теоретическая подготовка	2
		Разработка Python-скриптов с использованием ИИ для автоматизации тестирования на проникновение, включая сканирование и эксплуатацию уязвимых хостов, а также объединение инструментов в единый рабочий скрипт.	Практические занятия	5
		Разработка собственных скриптов с использованием ИИ для автоматизации задач пентестинга, включая перебор директорий и сбор активных страниц сайта.	Самостоятельная работа	1
		Текущий контроль по теме "Автоматизация пентестинга на Python с использованием ИИ"	Текущий контроль	1

рекомендаций по их устранению	Анализ результатов и генерация отчетов с помощью ИИ	Составление отчетов о тестировании на проникновение, включая структуру и содержание документа, предоставленного преподавателем, а также процесс формулирования рекомендаций по устранению выявленных уязвимостей на основе результатов анализа.	Теоретическая подготовка	2
		Создание отчета по трем выбранным уязвимостям в виртуальной машине DVWA, включая описание проведенных тестов на проникновение и формулирование рекомендаций с помощью ИИ.	Практические занятия	6
		Разработка отчета с использованием ИИ о тестировании на проникновение гипотетической компании, включая анализ трех выбранных уязвимостей и предоставление рекомендаций по их устранению.	Самостоятельная работа	1
		Текущий контроль по теме "Анализ результатов и генерация отчетов 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 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)	Итоговый контроль/аттестация	4

		полностью соответствует критерию (3 балла).			
				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			