

Приложение 2.1
к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа дисциплины

«ОПЦ.10 Основы применения искусственного интеллекта и нейронных сетей в профессиональной деятельности»

СОДЕРЖАНИЕ ПРОГРАММЫ

1. Общая характеристика РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	3
1.1. Цель и место дисциплины в структуре образовательной программы.....	3
1.2. Планируемые результаты освоения дисциплины	3
2. Структура и содержание ДИСЦИПЛИНЫ	4
2.1. Трудоемкость освоения дисциплины	4
2.2. Содержание дисциплины.....	5
3. Условия реализации ДИСЦИПЛИНЫ	8
3.1. Материально-техническое обеспечение.....	8
3.2. Учебно-методическое обеспечение	8
4. Контроль и оценка результатов освоения ДИСЦИПЛИНЫ	9

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОПЦ.10 Основы применения искусственного интеллекта и нейронных сетей в профессиональной деятельности»

1.1. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины «ОПЦ.10 Основы применения искусственного интеллекта и нейронных сетей в профессиональной деятельности»: формирование у обучающихся знаний и практических навыков применения технологий искусственного интеллекта и нейронных сетей для решения задач профессиональной деятельности в области обеспечения информационной безопасности автоматизированных систем, включая обнаружение компьютерных атак, анализ защищённости, тестирование средств защиты информации, автоматизацию обработки событий безопасности и генерацию технической документации.

Дисциплина «ОПЦ.10 Основы применения искусственного интеллекта и нейронных сетей в профессиональной деятельности» включена в вариативную часть Общепрофессионального цикла образовательной программы.

1.2. Планируемые результаты освоения дисциплины

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ОПОП-П).

В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	Уметь	Знать	Владеть навыками
ОК.01	– формулировать эффективные промпты для генерации кода, тестов, документации, политик безопасности;	– номенклатуру современных ИИ-инструментов для специалиста по защите информации;	-
ОК.02	– оценивать качество и достоверность сгенерированного ИИ контента; – применять ИИ-инструменты для поиска, анализа и интерпретации информации в профессиональной деятельности по защите информации;	– принципы построения промптов для решения задач информационной безопасности; – возможности и ограничения генеративных нейросетей применительно к анализу логов, выявлению атак, генерации тестов;	-
ОК.09	– использовать нейросети для перевода и адаптации профессиональной документации на иностранном языке.	– этические и правовые аспекты использования ИИ в области защиты информации.	-
ПК 2.2	– использовать ИИ-ассистенты для анализа защищённости автоматизированных систем и выявления потенциальных уязвимостей; – применять нейросети для генерации тестовых воздействий и сценариев проверки программных и	– методы использования нейросетей для обнаружения вторжений (IDS/IPS), анализа сетевого трафика и выявления аномалий; – способы интеграции ИИ-инструментов в процессы мониторинга и реагирования на инциденты (SOAR);	– основами работы с ИИ-ассистентами для анализа логов безопасности и выявления аномалий; – приёмами автоматической генерации отчётов, политик безопасности и технической документации с помощью нейросетей.

	программно-аппаратных средств защиты информации;		
ПК 2.3	– анализировать логи событий информационной безопасности с помощью больших языковых моделей (LLM), выявлять признаки компьютерных атак;	– основные техники верификации и постобработки контента, сгенерированного ИИ;	– методами генерации тестовых сценариев для проверки эффективности СЗИ с помощью нейросетей; – приёмами автоматизированного анализа логов событий безопасности с использованием LLM;
ПК 2.6	– генерировать с помощью ИИ шаблоны политик безопасности, инструкции по настройке средств защиты информации (СЗИ), отчёты об инцидентах.	– стандарты оформления технической документации в области информационной безопасности, поддерживаемые ИИ-инструментами.	– навыками создания шаблонов политик безопасности и эксплуатационной документации с применением генеративных нейросетей.

1.3.Обоснование часов вариативной части ОПОП-П

№№ п/п	Дополнительные знания, умения, навыки	№, наименование темы	Объем часов	Обоснование включения в рабочую программу
1	ПК 2.2, ПК 2.6 – применение ИИ для обнаружения атак, анализа логов, реагирования на инциденты.	Раздел 2, темы 2.1, 2.3	24	Дисциплина формирует востребованные на рынке труда навыки использования ИИ для мониторинга информационной безопасности, выявления компьютерных атак и автоматизации реагирования, что соответствует требованиям работодателей к специалистам по защите информации.
2	ПК 2.3 – использование ИИ для тестирования программных и программно-аппаратных средств защиты информации, генерации тестовых воздействий.	Раздел 2, тема 2.2	24	Дисциплина расширяет компетенции в области тестирования СЗИ за счёт освоения методов генерации тестовых сценариев и анализа результатов с помощью нейросетей, что повышает качество и скорость проверки защищённости автоматизированных систем.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Трудоемкость освоения дисциплины

Наименование составных частей дисциплины	Объем в часах	В т.ч. в форме практ. подготовки
Учебные занятия	44	26
Самостоятельная работа	2	-
Промежуточная аттестация в форме ДФА	2	-
Всего	48	26

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятий	Объем, ак. ч. / в том числе в форме практической подготовки, ак. ч.	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Введение в искусственный интеллект и нейронные сети		8 / 4	
Тема 1.1. Основы ИИ и нейросетей	Содержание	4 / 2	ОК 01, ОК 02, ОК 09, ПК 2.2
	Понятие ИИ, машинного и глубокого обучения. История развития. Генеративные и дискриминативные модели. Архитектуры: GAN, VAE, Transformer, Diffusion models. Классификация нейросетей по решаемым задачам (обработка текста, изображений, аудио, генерация контента).		
	В том числе практических и лабораторных занятий	2	
	Знакомство с интерфейсами и функционалом отечественных нейросетей (YandexGPT, GigaChat, Kandinsky, Шедеврум). Регистрация, настройка, выполнение простых запросов.		
Тема 1.2. Промптинг и этика использования ИИ	Содержание	4 / 2	ОК 01, ОК 02, ОК 09, ПК 2.2
	Основы промптинга: структура запроса, ключевые слова, контекст, стилизация. Сайты-конструкторы промптов. Этические и правовые аспекты генерации контента: авторские права, плагиат, маркировка контента, созданного ИИ, ответственность за использование ИИ в системах обработки информации ограниченного доступа.		
	В том числе практических и лабораторных занятий	2	
	Составление промптов для генерации текстов и изображений. Анализ результатов. Разработка промптов для задач информационной безопасности.		
Раздел 2. Применение ИИ в профессиональной деятельности специалиста по защите информации		20 / 10	
Тема 2.1. ИИ для обнаружения компьютерных атак и анализа уязвимостей	Содержание	8 / 4	ОК 01, ОК 02, ОК 09, ПК 2.2, ПК 2.3, ПК 2.6
	Обзор ИИ-систем обнаружения вторжений (IDS/IPS) на основе машинного обучения. Анализ сетевого трафика с помощью ML-алгоритмов. Использование больших языковых моделей (LLM) для анализа логов безопасности и выявления подозрительных событий. Автоматическое выявление аномалий в поведении пользователей (UEBA).		

	В том числе практических и лабораторных занятий	6	
	Анализ логов событий безопасности (например, журналов Windows, syslog) с помощью YandexGPT/GigaChat – выявление атак перебора, несанкционированного доступа. Генерация сводки и возможных причин.		
Тема 2.2. Использование ИИ для тестирования программных и программно-аппаратных средств защиты информации	Содержание	6 / 2	ОК 01, ОК 02, ОК 09, ПК 2.2, ПК 2.3, ПК 2.6
	Генерация тестовых воздействий для проверки межсетевых экранов, антивирусов, систем контроля доступа. Автоматизация пентеста с помощью ИИ (генерация эксплойтов, подбор паролей). Генерация скриптов для проверки политик безопасности. Оценка эффективности СЗИ с использованием нейросетей.		
	В том числе практических и лабораторных занятий	4	
	Генерация модульных тестов (unit tests) для функций проверки прав доступа. Создание набора тестовых сетевых запросов для проверки правил межсетевого экрана.		
Тема 2.3. Применение ИИ для автоматизации задач защиты информации	Содержание	6 / 4	ОК 01, ОК 02, ОК 09, ПК 2.2, ПК 2.3, ПК 2.6
	ИИ для генерации политик безопасности, конфигураций средств защиты. Автоматическое реагирование на инциденты (SOAR) с элементами ИИ. Генерация отчетов о защищенности, инструкций по настройке СЗИ. Применение нейросетей для создания схем сетей и графических элементов документации по информационной безопасности.		
	В том числе практических и лабораторных занятий	4	
	Создание шаблона политики безопасности (например, политика парольной защиты) с помощью нейросети. Генерация инструкции по настройке антивирусного ПО. Создание схемы защищенной сети с использованием ИИ-генерации изображений.		
Раздел 3. Безопасность и перспективы использования ИИ		16 / 12	
Тема 3.1. Угрозы, связанные с использованием ИИ, и методы защиты	Содержание	8 / 6	ОК 01, ОК 02, ОК 09, ПК 2.2, ПК 2.6
	Фальсификация биометрии, утечка данных при работе с облачными ИИ-сервисами, deerfake как угроза информационной безопасности. Методы разоблачения deerfake. Защита персональных данных и информации ограниченного доступа при использовании генеративных нейросетей. Проверка авторства цифрового контента.		
	В том числе практических и лабораторных занятий	4	
	Анализ кейсов использования deerfake и методов их обнаружения. Разработка рекомендаций по безопасному использованию ИИ в		

	профессиональной деятельности специалиста по защите информации.		
Тема 3.2. Современные тренды и будущее ИИ в информационной безопасности	Содержание	8 / 6	ОК 01, ОК 02, ОК 09, ПК 2.2, ПК 2.6
	Мультимодальные модели. ИИ в SOC (Security Operations Center): автоматизация triage инцидентов, анализ вредоносного кода. Перспективы развития нейросетей для автономного реагирования на атаки. Этические дилеммы и регулирование ИИ в сфере безопасности.		
	В том числе практических и лабораторных занятий	4	
	Итоговая работа: создание комплекта материалов для вымышленного проекта по защите информации с использованием ИИ (политика безопасности, отчёт об анализе логов, тестовые сценарии, графические схемы).		
В том числе самостоятельная работа обучающихся		2	
Подготовка сравнительного обзора отечественных и зарубежных ИИ-инструментов для задач информационной безопасности (обнаружение атак, тестирование, генерация документации) с обоснованием применимости.			
Промежуточная аттестация: ДФА			
Всего		48	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Кабинет(ы) информатики, вычислительной техники, информационных технологий, оснащённый(е) в соответствии с приложением 3 ОПОП-П.

Лаборатория(и):

– лаборатория информационных технологий, сетей и систем передачи информации, программирования и баз данных, оснащённая рабочими местами на базе вычислительной техники, подключёнными к локальной вычислительной сети и сети «Интернет»;

– лаборатория программных и программно-аппаратных средств защиты информации, оснащённая антивирусными программными комплексами, средствами защиты от НСД, средствами обнаружения вторжений, криптографическими средствами;

– лаборатория технических средств защиты информации, оснащённая аппаратными средствами аутентификации, измерителями ПЭМИН, средствами акустической защиты, стендами физической защиты объектов информатизации.

Все лаборатории оснащены в соответствии с приложением 3 ОПОП-П.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Митяков, Е. С. Искусственный интеллект и машинное обучение: учебное пособие для СПО / Е. С. Митяков, А. Г. Шмелева, А. И. Ладынин. – Санкт-Петербург: Лань, 2025. – 252 с. – ISBN 978-5-507-51466-3. – Текст: электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/book/450830>

2. Гудфеллоу, Я. Глубокое обучение / Я. Гудфеллоу, И. Бенджио, А. Курвиль ; перевод с английского А. А. Слинкина. – 2-е изд. – Москва: ДМК Пресс, 2025. – 652 с. – ISBN 978-5-97060-618-6. – Текст: электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/book/107901>

3. Нейросети ChatGPT, Midjourney. Инструкция для начинающих. – Москва: АСТ, 2024. – 128 с. – ISBN 978-5-17-161267-4. – Текст: электронный // ЭБС «Лань».

3.2.2. Дополнительные источники

1. Конструктор промтов (запросов) для нейронных сетей. – URL: <https://gpt-prompt.ru>

2. Инструкция: как формулировать запросы к GigaChat. – URL: <https://developers.sber.ru/help/gigachat/prompt-guide>

3. Каталог промтов для GigaChat. – URL: <https://developers.sber.ru/help/gigachat/catalog/text>

4. Работа с нейронной сетью Yandex GPT для получения краткого содержания видеозаписей. – URL: <https://300.ya.ru/>.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоённости компетенций	Методы оценки
<i>Знает:</i> - номенклатуру современных ИИ-инструментов для ИБ; - принципы построения промптов; - методы использования нейросетей для обнаружения атак и тестирования СЗИ; - возможности и ограничения генеративных нейросетей.	– Правильно классифицирует ИИ-инструменты по их функционалу в области защиты информации. – Грамотно формулирует промпты для анализа логов, генерации тестов, создания документации. – Приводит примеры эффективного и неэффективного использования ИИ в задачах информационной безопасности. – Обосновывает выбор ИИ-инструмента для конкретной профессиональной задачи.	Экспертное наблюдение на практических занятиях. Диагностика (тестирование, устный опрос).
<i>Умеет:</i> - формулировать промпты для генерации тестов, политик безопасности, отчётов; - использовать ИИ-ассистенты для анализа логов и выявления атак; - применять нейросети для генерации тестовых воздействий и сценариев проверки СЗИ; - анализировать сгенерированный контент на соответствие требованиям информационной безопасности.	– Самостоятельно создаёт и корректирует промпты для получения качественного результата. – Демонстрирует способность генерировать с помощью ИИ сценарии проверки политик доступа, выявлять аномалии в логах. – Создаёт шаблоны политик безопасности и инструкции по настройке СЗИ с помощью нейросетей. – Проводит постобработку и верификацию сгенерированного материала.	Экспертное наблюдение выполнения практических работ. Оценка итоговой практической работы (комплекта материалов для вымышленного проекта по защите информации). ДФА.