Аннотация рабочей программы дисциплины

Б1.В.02 «Основы информационной безопасности»

Направление подготовки/специальность 02.03.02 **Фундаментальная информатика и информационные технологии**

(код и наименование направления подготовки/специальности)

Курс 4 Семестр 8 Количество з.е. 3

Объем трудоемкости: 3 зачетных единиц (108 ч., из них – 42 час. аудиторной нагрузки: лекционных 28 ч., лабораторных работ – 14 ч., 8 часов самостоятельной работы, 4часов КСР, 0,3 часа ИКР.), форма контроля – экзамен.

Цель дисциплины: сформировать у обучающихся системное понимание принципов информационной безопасности (ИБ) и практических методов защиты современных информационных систем, включая ИИ-системы, чат-боты, большие языковые модели (LLM) и Retrieval-Augmented Generation (RAG), на базе стандартов, фреймворков и лучших практик.

Задачи дисциплины:

1. Изучение основ ИБ: свойства безопасности, угрозы и уязвимости, модели нарушителя, управление рисками, политика безопасности.
2. Освоение средств защиты: криптография, контроль доступа, аутентификация/авторизация, сетевые экраны, IDS/IPS, SIEM.
3. Безопасность программного обеспечения и Secure SDLC (SAST/DAST, управление зависимостями/секретами), DevSecOps.
4. Безопасность облачных и контейнерных сред (IAM, политика сети, реестр образов, сканирование уязвимостей).
5. Специальный модуль: безопасность ИИ-систем и LLM/RAG: угрозы (prompt-injection, jailbreak, model/RAG poisoning, model-DoS, insecure output handling), защиты (guardrails, проверка источников, контент-фильтрация, аудит и трассировка, верификация цитат), соответствие OWASP LLM Top-10 и фреймворкам NIST AI RMF 1.0, ISO/IEC 23894:2023.

Место дисциплины в структуре ООП ВО:

Дисциплина «Основы информационной безопасности» относится к базовой части Б1.В.02.

Дисциплина в значительной степени **взаимодействует для формирования компетенций** с дисциплинами:

1. Мультиагентные системы
2. Операционные системы
3. Нейросетевые технологии

Требованием к «входным» знаниям является понимание основ сетей и операционных систем, навыки программирования на Python, знание базовой веб-архитектуры и облачных технологий.

Результаты обучения (знания, умения, опыт, компетенции):

Содержание и структура дисциплины:

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

УК-3	***Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде***
УК-3.1	Понимает основные аспекты межличностных и групповых коммуникаций; соблюдает нормы и установленные правила поведения в организации Знает подходы к лидерству/делегированию. Умеет управлять командой в инцидент-сценариях. Владеет публичной защитой с технико-рисковым обоснованием.
ПК-4	***Способен планировать необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции***
ПК-4.1	Использует современные инструментальные средства разработки баз данных, прикладного программного обеспечения и систем различного функционального назначения Знает основы DevSecOps-подхода при выборе инструментальных средств. Умеет интегрировать инструменты статического и динамического анализа в процесс разработки. Владеет настройкой автоматизированных пайплайнов для обеспечения безопасности и качества ПО.
ПК-4.2	Применяет современные приемы работы с инструментальными средствами, поддерживающими создание программных продуктов и программных комплексов на базе языков программирования, баз данных и пакетов прикладных программ Знает тонкости криптоконфигов TLS/SSH и supply-chain риски. Умеет писать собственные правила Semgrep/IDS. Владеет построением «красной линии» в CI с SLA на исправления.
ПК-4.3	Способен использовать методы эффективного управления командой при разработке, внедрении и сопровождении программных продуктов Знает практики policy-as-code. Умеет внедрять риск-ориентированное планирование релизов. Владеет настройкой security-gates и KPI процесса.
SS-1	***Способен осуществлять свою трудовую деятельность с учетом определения корректной роли ИИ в различных процессах, критического анализа последствий применения ИИ-технологий, этических принципов***
SS-1.1	Учитывает в разработке и эксплуатации систем ИИ философские основания концепций интеллекта, языка, знания, агентности Понимает различие между вычислением и мышлением, между данными, информацией и знанием. Учитывает это различие в работе с ИИ на разных стадиях жизненного цикла.
SS-3	***Способен осуществлять свою трудовую функцию с учетом неопределенности как сущностной черты функционирования искусственного интеллекта***
SS-3.1	Учитывает в работе когнитивные искажения человека и примеры их проявления при работе с данными и ИИ, выявляет предвзятости систем ИИ,

	аргументированно оценивает надежность данных и выдачи ИИ, применяет базовые принципы критического мышления (оценка источников, проверка аргументов, отличие факта от интерпретации). Распознаёт очевидные когнитивные искажения в работе человека (например, подтверждение своей точки зрения, слепое доверие алгоритму), обращает внимание на возможную предвзятость ИИ; воспринимает необходимость критически относиться к результатам ИИ.
LC-1 Б	***Способен проводить анализ бизнес-проблем с оценкой перспективности применения ИИ для их решения, осуществлять постановку задачи машинного обучения, формулировать требования к системе ИИ***
LC-1.3	Готовит и ведет документы для реализации проектов в области ИИ Оценивает технические требования на основе формализованной постановки
ML-5 П	***Способен разрабатывать и (или) применять методы повышения устойчивости, надежности, безопасности алгоритмов МО***
ML-5.1	Обосновывает способы и варианты применения методов повышения устойчивости, надежности, безопасности алгоритмов МО задачах ИИ, включая их преобразование и адаптацию к специфике задачи Обосновывает выбор и применение методов повышения устойчивости и надежности моделей с учётом специфики задачи, включая адаптацию моделей и использование подходов объяснимого ИИ и доверенного ИИ. Учитывает риски атак и методы их противодействия.
ML-5.2	Применяет методы повышения устойчивости, надежности, безопасности алгоритмов МО для проверки разведочных гипотез и подготовки данных к применению современных методов ИИ Использует продвинутые методы дообучения моделей при подготовке данных, применяет методы повышения устойчивости моделей к атакам и искажениям данных
ML-5.3	Оценивает результативность применения методов повышения устойчивости, надежности, безопасности алгоритмов МО в задачах ИИ на основе сопоставления с аналогами Проводит комплексный анализ результативности с учётом объяснимости моделей, устойчивости к атакам, использует методы доверенного ИИ для оценки.
AI S-1 Б	***Способен управлять рисками в разработке систем ИИ, выстраивать управление безопасностью ИИ в компании с учетом этики ИИ***
AI S-1.1	Выявляет и моделирует угрозы на всём жизненном цикле ИИ-систем, оценивает и приоритизирует риски Понимает основные категории рисков и атак на ИИ (data poisoning, model stealing, evasion). Применяет типовые методики (STRIDE, MITRE ATLAS) по готовым шаблонам. Следует в работе ГОСТ Р ISO/IEC 27005-2010; ПНСТ 836-2023 «ИИ. Функциональная безопасность»; методики ФСТЭК по оценке угроз (2024); Знает международные фреймворки и стандарты NIST AI RMF 1.0; ISO/IEC 27005 (risk); MITRE ATLAS; STRIDE/PASTA.
AI S-1.2	Обеспечивает соответствие нормативным требованиям и принципам доверенного/этичного ИИ Знаком с Кодексом этики в сфере ИИ РФ (2021) , базовых принципах Responsible AI, законом 152-ФЗ «О перс. данных» и основами GDPR. Может описать процесс Data Impact Assessment.

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в _8_ семестре *(очная форма)*

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Основы ИБ и управление рисками	15	9		4	2
2.	Безопасность ПО, инфраструктуры и облака	17	9		5	3
3.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	18	10		5	3
ИТОГО по разделам дисциплины		**50**	**28**		**14**	**8**
Контроль самостоятельной работы (КСР)		4				
Промежуточная аттестация (ИКР)		0,3				
Подготовка к текущему контролю		53,7				
Общая трудоемкость по дисциплине		**108**				

Примечание: Л – лекции, КСР – контрольные и самостоятельные работы, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

Курсовые проекты или работы.
Не предусмотрены учебным планом

Вид аттестации: ЛР, проект по кейсами индустриальных партнеров, экзамен.

Автор В.И.Шиян, ст. преп. КВТ

Автор Т.А.Приходько, доц. КВТ, к.т.н., доц.