Аннотация рабочей программы дисциплины

Б1.О.36 «Безопасность информационных систем»

Курс 4 Семестр 7 Количество з.е. 3
Объем трудоемкости: 3 зачетных единиц (108 ч., из них – 50 час. аудиторной нагрузки: лекционных 16 ч., лабораторных работ – 34 ч., 20 часов самостоятельной работы, 4 часов 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 «Безопасность информационных систем» относится к базовой части Б1.О.36.

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

1. Алгебра и геометрия
2. MLOps&DevOps
3. Параллельное и низкоуровневое программирование
4. Технологии тестирования программного обеспечения
5. Администрирование информационных сетей
6. Технологии управления данными NoSQL

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-1	***Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач***
УК-1.2	Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи Знает методы критической оценки доказательств и синтеза разнотипных источников. Умеет выстраивать систематический обзор темы, сопоставлять стандарты/исследования и обосновывать выбор. Владеет полным циклом трассируемости: от постановки задачи до решений с источниками и ограничениями.
ОПК-4	***Способен находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем***
ОПК-4.2	Тестирует и внедряет алгоритмы в реальные задачи, оценивая их точность и производительность Знает тонкости производительности/надёжности и методов их верификации в проде. Умеет проектировать эксперименты, автоматизировать тестирование и интегрировать метрики в мониторинг. Владеет практиками DevSecOps для устойчивых релизов (quality gates, «красная линия»).
ОПК-8	***Способен использовать основы правовых знаний в различных сферах жизнедеятельности***
ОПК-8.1	Соблюдает нормы авторского права и лицензирования при использовании и разработке программного обеспечения Знает юридические нюансы совместимости лицензий, перераспространения и деривативов. Умеет разрешать лицензионные коллизии и оформлять корректное уведомление/NOTICE в релизах. Владеет управлением лицензиями на уровне CI/CD (политики отклонения, отчётность SBOM).
ОПК-8.2	Понимает юридические основы кибербезопасности и ответственности за нарушения в цифровой среде Знает взаимодействие технических и правовых требований в ИБ (логирование, хранение, раскрытие инцидентов). Умеет проектировать меры соответствия, учитывающие архитектуру сервиса и риски для субъектов данных. Владеет подготовкой комплексных материалов аудита/комплаенса для учебного кейса.
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	Определяет ценностные предпосылки, когнитивные искажения, культурно-обусловленные предвзятости в данных, алгоритмах, постановке задач для ИИ. Самостоятельно анализирует обучающую выборку на предмет репрезентативности, возможных искажений, скрытых предвзятостей. Соотносит технические характеристики модели с потенциальными рисками её применения (например, низкая устойчивость к шуму — риск в медицинской диагностике).
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.
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 _7_ 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	22	5		11	6
2.	Безопасность ПО, инфраструктуры и облака	22	5		11	6
3.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	24	6		12	6
ИТОГО по разделам дисциплины		**68**	**16**		**34**	**18**
Контроль самостоятельной работы (КСР)		4				

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
Промежуточная аттестация (ИКР)		0,3				
Подготовка к текущему контролю		35,7				
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.