АННОТАЦИЯ рабочей программы дисциплины
Б1.О.36 «Безопасность информационных систем»

Объем трудоемкости: 3 зач.ед. (108 часов)

Цели дисциплины:

Формирование у студентов навыков разработки требований к безопасности информационных систем с использованием основных алгоритмов криптографии и различных криптосистем шифрования.

Задачи дисциплины:

- Изучить использование в своей практической деятельности различные алгоритмы шифрования;
- Освоение возможностей компьютерными технологиями в области персональной и сетевой безопасности;
- Приобретение навыков самостоятельного изучения специальной литературы по информационной безопасности;

Место дисциплины в структуре ООП ВО

Дисциплина «Безопасность информационных систем» относится к обязательной части учебного плана.

Данная дисциплина тесно связана с дисциплинами: «Алгебра и геометрия», «Основы программирования», «Параллельное и низкоуровневое программирование».

Материал курса является связкой между математикой, программированием и прикладными задачами, связанными с безопасностью информационных систем на предприятии. Знания, полученные в данной дисциплине, используются в ходе изучения курсов «Правовые основы оценки проектных решений», «Математические модели защиты информации» и др.

Требования к уровню освоения дисциплины

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

Код и наименование индикатора*	Результаты обучения по дисциплине
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 и стратегии эффективного поиска информации. Умеет формулировать цели поиска и подбирать оптимальные источники информации. Анализировать и критически оценивать найденные данные. Владеет навыками использования цифровых ресурсов и специализированного программного обеспечения для поиска и обработки информации.
ОПК 4 Способен участвовать в разработке технической документации программных продуктов и программных комплексов	
ОПК 4.1 Обладает знаниями об основных стандартах, нормах и правил разработки технической документации программных продуктов и программных комплексов	Знает основные элементы технической документации (описания архитектуры, руководства пользователей, спецификации интерфейсов, инструкции по установке и развертыванию). Умеет создавать техническую документацию, соответствующую стандартам и требованиям заказчика. Владеет программами и сервисами для подготовки качественной технической документации (Word, LaTeX, Dia, PlantUML).
ОПК 4.2 Способен применять стандарты, нормы и правила при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла программных продуктов и программных комплексов	Знать международные и российские стандарты оформления технической документации (ISO, ГОСТ Р, отраслевые регламенты). Уметь применять стандарты и регламенты для эффективного сопровождения всех стадий разработки программных продуктов. Владеть практическим опытом работы с системами управления версиями и хранения документации (GitHub, Confluence, Jira Docs).
ОПК 6 Способен использовать в педагогической деятельности научные основы знаний в сфере информационно-коммуникационных технологий	
ОПК 6.2 Обосновывает выбор конкретной ИКТ-технологии для решения педагогической задачи	Знает особенности и возможности различных информационно-коммуникационных технологий (ИКТ), используемых в образовательном процессе. Умеет аргументированно обосновывать выбор технологии исходя из поставленных учебных целей и потребностей учащихся. Владеет техническими умениями работы с современными технологиями обучения (интерактивные доски, онлайн-платформы, виртуальная реальность и др.).
ML-5 Способен разрабатывать и (или) применять методы повышения устойчивости надежности безопасности алгоритмов машинного обучения	
ML-5.1 Обосновывает способы и варианты применения методов повышения устойчивости, надежности, безопасности алгоритмов машинного обучения задачах искусственного интеллекта, 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-1.1 Выявляет и моделирует угрозы на всём жизненном цикле ИИ-систем, оценивает и приоритизирует риски	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.
AI S-1.2 Обеспечивает соответствие нормативным требованиям и принципам доверенного/этичного ИИ.	Выполняет базовые тесты устойчивости (noise, simple adversarial examples) в песочнице. Участвует в подготовке сценариев red-team-тестов по готовым шаблонам. Знает международные стандарты и фреймворки MITRE ATLAS; OWASP ML Sec Top 10; гайд «AI Red Teaming Regulations»
SS-1.1 Определяет ценностные предпосылки, когнитивные искажения, культурно-обусловленные предвзятости в данных, алгоритмах, постановке задач для ИИ	Понимает, что качество обучающей выборки существенно определяет этико-социальные аспекты функционирования ИИ.

Распределение трудоёмкости дисциплины по видам работ

Вид учебной работы		Всего часов	Семестры (часы)
			7
Контактная работа, в том числе:		**54,3**	**54,3**
Аудиторные занятия (всего):		**50**	**50**
Занятия лекционного типа		**16**	16
Лабораторные занятия		**34**	34
Занятия семинарского типа (семинары, практические занятия)			
Иная контактная работа:		**4,3**	**4,3**
Контроль самостоятельной работы (КСР)		**4**	4
Промежуточная аттестация (ИКР)		**0,3**	0,3
Самостоятельная работа, в том числе:		**18**	**18**
Проработка учебного (теоретического) материала		**12**	12
Выполнение индивидуальных заданий (типовой расчет)		**6**	6
Подготовка к текущему контролю			
Контроль:		**35,7**	**35,7**
Подготовка к экзамену		**35,7**	35,7
Общая трудоемкость	**час.**	**108**	**108**
	в том числе контактная работа	**54,3**	**54,3**
	зач. ед	**3**	**3**

Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Основы информационной безопасности	8	2		4	2
2.	Методы криптографической защиты данных	10	2		6	2
3.	Средства защиты персональных данных и конфиденциальной информации	8	2		4	2
4.	Обеспечение безопасности приложений и веб-сервисов	8	2		4	2
5.	Мониторинг и аудит безопасности информационных систем	14	4		6	4
6.	Организационные меры и регламенты обеспечения безопасности	8	2		4	4
7.	Практикум по защите ИИ-моделей и аналитических платформ	10	2		6	2
ИТОГО по разделам дисциплины		**68**	**16**		**34**	**18**
Контроль самостоятельной работы (КСР)		4				
Промежуточная аттестация (ИКР)		0,3				
Подготовка к текущему контролю		35,7				
Общая трудоемкость по дисциплине		**108**				

Курсовые работы: не предусмотрены

Форма проведения аттестации по дисциплине: экзамен.

Автор: Грищенко В.И. – ст. преподаватель кафедры анализа данных и искусственного интеллекта КубГУ