Аннотация к рабочей программы дисциплины
«Б1.О.07 «Криптография и сетевая безопасность»»

Объем трудоемкости: 5 зачетных единиц

Цель дисциплины:

Цели изучения дисциплины определены государственным образовательным стандартом высшего образования и соотнесены с общими целями ООП ВО по направлению подготовки 01.04.02 Прикладная математика и информатика, в рамках которой преподается дисциплина. Преподавание дисциплины Б1.О.07 «Криптография и сетевая безопасность» строится исходя из требуемого уровня базовой подготовки студентов магистратуры, обучающихся по направлению 01.04.02 Прикладная математика и информатика.

В современном мире безопасность информационных систем является важным аспектом стабильной и успешной работы в различных сферах деятельности человека, предприятий, государств, содружеств и т. д.

Конечными целями преподавания дисциплины являются:

– основы обеспечения компьютерной и сетевой безопасности;

− основы безопасности информационных экономических систем предприятия;

− знание федеральных законов по обеспечения информационной безопасности, обработки персональных данных;

− владение основными алгоритмами математики криптографии; − знание и использование различных криптосистем шифрования.

Основа изучения дисциплины Б1.О.07 «Криптография и сетевая безопасность» – реализация требований, установленных Федеральным государственным образовательным стандартом высшего профессионального образования к подготовке студентов бакалавриата, обучающихся по направлению 01.04.02 Прикладная математика и информатика.

Задачи дисциплины:

− научить студентов использовать в своей практической деятельности различные алгоритмы шифрования;

− ознакомить с компьютерными технологиями в области персональной и сетевой безопасности;

− привить студентам умения и навыки самостоятельного изучения специальной литературы по информационной безопасности.

Место дисциплины в структуре образовательной программы

Дисциплина Б1.О.07 «Криптография и сетевая безопасность» относится к обязательной части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана.

Дисциплина изучается в 1-м семестре и использует разносторонние знания, полученные в предыдущих семестрах. Преподавание дисциплины ведется в виде лекций, лабораторных и самостоятельных занятий. Большая часть лекционного материала дается в интерактивном режиме. Основная цель лабораторных занятий – практическая реализация изученных методов.

Студенты, обучающиеся дисциплине «Криптография и сетевая безопасность» должны владеть навыками логического мышления. Обязательным для них является знание основ безопасности информационных систем. Студент должен уметь использовать навыки работы с алгоритмами защиты информации, технологиями и программами для решения изобретательских и нестандартных задач в области безопасности, в частности безопасности предприятия. Слушатель должен быть готов использовать знания, полученные в рамках дисциплины «Криптография и сетевая безопасность» в своей практической и научно-теоретической деятельности.

Требования к уровню освоения дисциплины

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

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ОПК-1 Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий	
ИОПК-1.1 Анализирует проблемы и формулирует задачи исследования. в области фундаментальной и прикладной математики	Знает: -основные теоретические основы криптографии и сетевой безопасности, связанные с математическими понятиями (теория чисел, алгебра, теория групп, теория вероятностей, комбинаторика и теория информации). -современные исследовательские направления и актуальные проблемы в области криптографических алгоритмов и протоколов. -методы анализа сложности и защищенности криптографических систем.
	Умеет -анализировать существующие математические модели и алгоритмы, используемые в криптографии и сетевой безопасности. -выявлять актуальные проблемы и недостатки в существующих методах и протоколах. -формулировать конкретные задачи исследования на основе анализа актуальных проблем и научных данных. -оценивать степень актуальности и практической значимости предстоящего исследования.
	Владеет: -навыками критического анализа проблем, связанных с безопасностью информации, и их формулировки. -способностью определять приоритетные направления исследований в области математических основ криптографии и сетевой безопасности.
ИОПК-1.2 Решает актуальные задачи фундаментальной и прикладной математики	Знает -основные математические методы и алгоритмы, применяемые для решения задач криптографии и сетевой безопасности — например, факторизация, дискретный логарифм, криптографические протоколы, теория информации и теория графов.

	-современные подходы к моделированию и анализу защищенности криптографических систем. -методы численного и теоретического анализа сложности алгоритмов и оценки их стойкости.
	Умеет -применять математические методы при решении конкретных задач, связанных с криптографией и безопасностью сетей. -разрабатывать и реализовывать алгоритмы для решения поставленных задач (например, генерация ключей, создание криптоустойчивых протоколов). -анализировать эффективность, безопасность и надежность криптографических решений. -оценивать риск уязвимостей и эффективности решений на основе математического анализа.
	Владеет -навыками практического применения математических методов для решения актуальных задач в области криптографической защиты информации и сетевой безопасности. -умением самостоятельно интерпретировать результаты математического анализа в контексте безопасности системы. -способностью искать пути улучшения и оптимизации существующих криптографических решений в соответствии с актуальными требованиями.
ОПК-3 Способен разрабатывать математические модели и проводить их анализ при решении задач в области профессиональной деятельности	
ИОПК-3.1 Анализирует проблемную область и разрабатывает математические модели для решения прикладных задач профессиональной деятельности	Знает: -основные понятия и требования к моделированию прикладных задач в области информационной безопасности, такие как моделирование угроз, анализ уязвимостей, оценка безопасности и эффективности криптографических протоколов. -стандартные математические методы и подходы для построения моделей — например, теория графов, математическая логика, теория вероятностей, теория информации, комбинаторика.

	-современные криптографические стандарты и протоколы, особенности их уязвимостей и анализа.
	Умеет -анализировать исходные данные прикладной задачи, выделять ключевые параметры и угрозы. -формулировать математическую модель, отражающую сущность и критериографии решения задач безопасности (например, моделирование атак, анализ вероятности уязвимостей). -разрабатывать алгоритмы и методы решения поставленных задач на основе выбранной модели. -оценивать эффективность и безопасность разработанных моделей и решений, интерпретировать полученные результаты.
	Владеет: -навыками профессионального анализа проблемной области и постановки конкретных прикладных задач. -умением разрабатывать адекватные математические модели, учитывающие специфику задач криптографии и сетевой безопасности. -способностью применять разработанные модели для тестирования криптографических протоколов, оценки уязвимостей и нахождения решений. -умением представлять результаты моделирования для последующей оценки и принятия решений специалистами по безопасности.
ИОПК-3.2 Исследует применимость и анализирует эффективность модели для решения прикладных задач профессиональной деятельности	Знает: Основные критерии эффективности криптографических моделей и протоколов. Методы анализа применимости и производительности решений.
	Умеет: Оценивать актуальность модели для конкретных задач в области безопасности. Анализировать эффективность и уязвимости модели на практике.
	Владеет: Навыками тестирования и оценки эффективности разработанных решений и моделей.

	Умением делать выводы о целесообразности использования модели в профессиональной деятельности.
ИОПК-3.3 Разрабатывает и реализует алгоритмы, структуры данных и программные модули для решения прикладных задач, исходя из требований проекта и особенностей задачи.	Знает: Основные алгоритмы криптографической защиты и принципы их реализации. Структуры данных и программные методы для обеспечения безопасности. Требования к пользовательским и системным криптографическим компонентам.
	Умеет: Анализировать прикладную задачу, выявлять требования безопасности. Проектировать и реализовать алгоритмы и модули, соответствующие поставленной задаче и требованиям проекта. Использовать языки программирования и средства разработки для интеграции криптографических решений.
	Владеет: Навыками написания программных модулей для криптографических приложений. Умением учитывать особенности и ограничения криптографических алгоритмов при кодировании. Способностью тестировать и оптимизировать реализованные криптоалгоритмы и модули.

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

№	Наименование тем		Количество часов			
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Введение в дисциплину	21	4		4	13
2.	Математика криптографии	22	4		4	14
3.	Алгоритмы шифрования	22	4		4	14
4.	Безопасность информационных систем предприятия	22	4		4	14
5.	Алгоритмы реализации электронно-цифровой подписи	22	4		4	14
6.	Безопасность корпоративной сети	22	4		4	14

7.	Безопасность в клиентско-серверных приложений	22	4		4	14
	Итого по разделам:	153	28		28	97
	Промежуточная аттестация (ИКР)	0,3				
	Контроль самостоятельной работы (КСР)					
	Подготовка к экзамену	26,7				
	ИТОГО по дисциплине	**180**				

Курсовые работы: курсовые работы не предусмотрены.
Форма проведения аттестации по дисциплине: экзамен

Автор Осипян В. О., проф. кафедры анализа данных и искусственного интеллекта, доктор физ.-мат. наук