

Аннотация рабочей программы дисциплины

Б1.О.28 «Криптографические протоколы»

Направление подготовки/специальность

02.03.02 Фундаментальная информатика и информационные технологии

Курс 4 Семестр 8 Количество з.е. 3

Объем трудоемкости: 3 зачетных единицы (108 часов, из них – 42 часа аудиторной нагрузки: лекционных 14 ч., лабораторных работ - 28 ч., 6 часов самостоятельной работы, 6 часов КСР, 0,3 часа ИКР, 53,7 часов подготовки к экзамену).

Цель дисциплины: изучение математических основ криптологии, основных криптоалгоритмов, стандартных криптопротоколов и аспектов их применения.

Задачи дисциплины:

В результате освоения данной компетенции студент должен:

знать основные блоки симметричных шифров, математические аспекты безопасности шифров, стандарты и ГОСТы криптопротоколов.

уметь построить программную реализацию существующих криптоалгоритмов средствами произвольного языка, построить криптопротокол обмена информацией с помощью встроенных библиотек, построить модель реализации заданной атаки на криптопротокол;

владеть навыками свободного обращения с программными реализациями криптоалгоритмов; навыками построения архитектуры защищенных программных систем с применением существующих протоколов.

.

Место дисциплины в структуре образовательной программы

Курс «Криптографические протоколы» относится к части, формируемой участниками образовательных отношений блока Б1 Дисциплины (модули) и является обязательной.

Для изучения дисциплины студент должен владеть знаниями, умениями и навыками по дисциплинам: Алгебра, Дискретная математика, Теория графов и ее приложения, Комбинаторный анализ, Информационная безопасность, Программирование в компьютерных сетях, Интерпретируемые языки программирования, Платформо-независимое программирование, с которыми дисциплина связана логически и содержательно-методически.

Дисциплина является предшествует изучению дисциплин: «Преддипломная практика», «Защита выпускной квалификационной работы»

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

Код и наименование индикатора	Результаты обучения по дисциплине (<i>знает, умеет, владеет (навыки и/или опыт деятельности)</i>)
ОПК-5	Способен устанавливать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности
Формулировки индикаторов	
ОПК-5.1. Знает методику установки и администрирования информационных систем и баз данных. Знаком с содержанием Единого реестра российских программ. ОПК-5.2. Умеет реализовывать техническое сопровождение информационных систем и баз данных. ОПК-5.3. Имеет практический опыт участия в научных студенческих конференциях, очных, виртуальных, заочных обсуждениях научных проблем в области информационных технологий.	
ПК-1	Способен понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания, современные языки программирования и программное обеспечение; операционные системы и сетевые технологии
Формулировки индикаторов	
ПК-1.1. Знает основы научно- исследовательской деятельности в области информационных технологий, имеет научные знания в теории информационных систем. ПК-1.2. Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности. ПК-1.3. Имеет практический опыт научно- исследовательской деятельности в области информационных технологий.	

Структура и содержание дисциплины

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	КСР	ЛР	СРС
1	2	3	4	5	6	7
1	Раздел 1. Математические основы криптологии.	20	4		14	2
2	Раздел 2. Криптоалгоритмы.	12	4		6	2
3	Раздел 3. Криптопротоколы	22	6	6	8	2
	Итого по разделам дисциплины	54	14	6	28	6
	ИКР	0,3				
	Подготовка к экзамену	53,7				53,7
	<i>Итого по дисциплине:</i>	108				

Курсовые проекты или работы: не предусмотрены

Вид аттестации: экзамен.

5.1 Основная литература:

1. Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г.А. Ганеш ; под ред. С. М. Молявко ; пер. с англ. В. Д. Хорева. - 4-е изд. - Москва : Лаборатория знаний, 2020. - 428 с. - URL: <https://e.lanbook.com/book/151552> (дата обращения: 13.04.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-00101-700-4. - Текст : электронный.

2. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. - 3-е изд., стер. - Санкт-Петербург : Лань, 2024. - 456 с. - URL: <https://e.lanbook.com/book/362942> (дата обращения: 19.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-48774-5. - Текст : электронный.

3. Математические методы защиты информации : учебное пособие для вузов / С. М. Рацеев. - Санкт-Петербург : Лань, 2022. - 544 с. - URL: <https://e.lanbook.com/book/193323> (дата обращения: 15.12.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-8589-5. - Текст : электронный.

4. Криптографические методы защиты информации для обучающихся компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд., испр. - Москва : Юрайт, 2022. - 473 с. - URL: <https://urait.ru/bcode/489242> (дата обращения: 26.01.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-12474-3. - Текст : электронный.

5. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Юрайт, 2022. - 349 с. - URL: <https://urait.ru/bcode/489919> (дата обращения: 30.05.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-02883-6. - Текст : электронный.

Автор Руденко О.В. – доцент кафедры вычислительных технологий