Аннотация по дисциплине

Б1.В.ДВ.03.02 МАТЕМАТИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки/специальность *01.03.02 Прикладная математика и информатика*

Направленность (профиль) / специализация *Программирование и информационные технологии*

Курс 4 Семестр 7 Количество з.е. 3

Цель изучения дисциплины

Курс посвящен изучению современных концепций информационнойбезопасности и их применения в обеспечении защиты информации и безопасного использования программных средств в вычислительных системах. Цель курса – научить студента методам информационной безопасности и их использовании в области защиты информации.

Студент после освоения курса приобретает теоретические знания и практические навыки в области применения задач информационной безопасности; методов защиты информации; области применения различных методов информационной безопасности; этапы, методы и инструментальные средства информационной безопасности; принципах построения и функционирования систем информационной безопасности; классификации шифров; основах организации идентификации и цифровой подписи; принципах построения и применения паролей; умеет проводить анализ и определять оптимальный метод защиты информации; формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; формулировать и решать задачи организации процесса цифровой подписи; формулировать и решать задачи организации процесса идентификации; реализовать на языке программирования заданный метод защиты информации; решать задачи анализа шифра.

Задачи курса

Основные задачи курса на основе системного подхода:

- Описать проблемную область информационной безопасности.
- Дать описание практического применения теории конечных полей в теории защиты информации.
- Расширить понятия о генерации псевдослучайных последовательностях.
- Расширить понятия о способах защиты информации.
- Расширить понятия о методах построения современных программных систем.
- Дать навыки практической работы с методами защиты информации.
- Дать навыки практической работы по решению задач идентификации.
- Дать навыки практической работы по решению задач цифровой подписи.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке бакалавра.

Место дисциплины в структуре ООП ВО.

Курс «Математические методы защиты информации» входит в вариативную часть Блока 1 «Дисциплины (модули)» дисциплин, формирующих знания и навыки в области

разработки современного программного обеспечения. Курс опирается на знания курсов «Математическая логика и дискретная математика», «Языки программирования и методы трансляции», «Основы сетевых технологий». Курс расширяет знания студентов в области создания программных систем, защиты данных и знаний.

Коды формируемых компетенций и требования к результатам освоения содержания дисциплины

Студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие программе дисциплины.

В результате освоения дисциплины студент должен:

Знать:

1. Математические основы теории передачи и защиты информации
2. Проблемы передачи, обнаружения и исправления внутриканальных ошибок;
3. Способы кодирования информации;
4. Знать источники угроз безопасности информации и методы оценки уязвимости;
5. Методы создания, организации и обеспечения функционирования систем;
6. Основные границы относительно мощности кодов.

Уметь:

7. Анализировать политику безопасности;
8. Профессионально грамотно сформулировать конфиденциальную задачу;
9. На практике осуществлять концепцию обеспечения информационной безопасности.

Владеть:

10. Владение основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления информацией;
11. Основными методами и средствами безопасной защиты информации;
12. Современными технологиями защиты информации в целом.

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-1	способностью собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям	4, 5, 6	7	11, 12
2.	ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	1, 2, 3	8, 9	10

Основные разделы программы

Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы дисциплины, изучаемые в 6 семестре (очная форма).

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	Основы теории защиты информации	14			8	6
2	Линейное и нелинейное кодирование. Корректирующие свойства кодов	22			12	10
3	Конечные поля	30			16	14
4	Обнаружение и исправление ошибок	25			16	9
5	Обзор изученного материала и прием зачета	11			2	8,7
	Контроль самостоятельной работы (КСР)	6				
	Промежуточная аттестация (ИКР)	0,2				
	Итого по дисциплине:	108			54	47,8

Формы текущего контроля и промежуточной аттестации

Для текущего контроля используются собеседование, выполнение индивидуальной задачи.

Вид промежуточной аттестации: зачет.

Основная литература.

1. Баранова, Е.К. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Е. К. Баранова, А. В. Бабаш . - 3-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2017. - 322 с. - http://znanium.com/catalog.php?bookinfo=763644
2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. - http://biblioclub.ru/index.php?page=book&id=438331.
3. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия [Текст] : учебное пособие для студентов вузов / О. Р. Лапонина ; [под ред. В. А. Сухомлина]. - 2-е изд., испр. - М. : Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний , 2007. - 531 с

Составитель:

д.ф.-м.н., профессор КИТ Осипян В.О.