Аннотация по дисциплине

Б1.О.09 КРИПТОГРАФИЯ И СЕТЕВАЯ БЕЗОПАСНОСТЬ

Направление подготовки/специальность *01.04.02 Прикладная математика и информатика*

Направленность (профиль) / специализация *Технологии программирования и разработки информационно-коммуникационных систем*

Курс 1 Семестр 1 Количество з.е. 5

Цель изучения дисциплины

Курс посвящен изучению современных концепций информационной безопасности 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 магистра.

Место дисциплины в структуре ООП ВО.

Курс «Криптография и сетевая безопасность» входит в вариативную часть Блока 1 «Дисциплины (модули)» дисциплин, формирующих знания и навыки в области разработки современного программного обеспечения. Курс опирается на знания в области дискретной математики, математической логики, программирования, базы данных. Курс

расширяет знания студентов в области создания программных систем, защиты данных и знаний.

Дисциплина тесно связана с дисциплинами «История и методология прикладной математики и информатики», «Дискретные и вероятностные математические модели», «Технологии проектирования и сопровождения программных систем», «Распределенные системы обработки информации и управления данными».

Коды формируемых компетенций и требования к результатам освоения содержания дисциплины

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

Компетенция	Компонентный состав компетенций		
	Знать	*Уметь*	*Владеть*
ОПК-5 Способностью использовать углубленные знания правовых и этических норм при оценке последствий своей профессиональной деятельности	области применения задач информационной безопасности; принципы построения и функционирования систем информационной безопасности; правовые и этические последствия при получении доступа к информации не санкционированными лицами	формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; оценить последствия при компрометации ключа или шифра	методами определения требований и состава средств, мероприятий по системе информационной безопасности систем; навыками оценки правовых и этических компрометации данных
ПК-2 Способностью разрабатывать и анализировать концептуальные и теоретические модели решаемых задач решаемых научных проблем и задач	области применения задач информационной безопасности; методы защиты информации; области применения различных методов информационной безопасности; этапы, методы и инструментальные средства информационной безопасности; методы разработки и анализа концептуальных и теоретических моделей; классификацию шифров; основы организации идентификации и цифровой подписи; принципы построения и применения паролей;	проводить анализ и определять оптимальный метод защиты информации; анализировать модели шифрования при организации защиты данных 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;	методологиями и парадигмами построение систем информационной безопасности; методами проектирования систем защиты информации; методами построения алгоритмов анализа; методами построения систем идентификации; методами определения требований и состава средств, мероприятий по системе информационной безопасности систем;

Основные разделы программы Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 1 семестре (очная форма).

Вид промежуточной аттестации: экзамен.

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа		Внеаудиторная работа	
			Л	ЛР	СРС	контроль
1	2	3	4	5	6	7

1.	Базовые понятия и история развития информационной безопасности.	18	4	4	10	4
2.	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	27	6	6	15	6,7
3.	Шифры замены. Шифры перестановки. Шифры гаммирования.	27	6	6	15	4
4.	Блочные системы шифрования.	31	6	6	19	4
5.	Поточные системы шифрования.	27	6	6	15	4
6.	Идентификация. Цифровые подписи.	23	4	4	15	4
7.	Промежуточная аттестация (ИКР)	0,3				
	Итого по дисциплине:	180	32	32	89	26,7

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

Формы текущего контроля и промежуточной аттестации

Для текущего контроля используются собеседование, выполнение индивидуальной задачи.

Вид промежуточной аттестации: экзамен.

Основная литература.

1. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - http://biblioclub.ru/index.php?page=book&id=438331.
2. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016.
3. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. – https://biblioclub.ru/index.php?page=book_red&id=458204&sr=1
4. Фороузан, Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - https://biblioclub.ru/index.php?page=book_red&id=428998&sr=1

Составитель:

к.ф.-м.н., доцент КИТ Подколзин Вадим Владиславович