Аннотация по дисциплине

Б1.О.01 КРИПТОГРАФИЯ И СЕТЕВАЯ БЕЗОПАСНОСТЬ

Направление подготовки/специальность *02.04.02 Фундаментальная информатика и информационные технологии*

Направленность (профиль) / специализация *Интеллектуальные системы и технологии*

Курс 1 Семестр 1 Количество з.е. 5

Цель изучения дисциплины

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

Студент после освоения дисциплины 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 дисциплины

Основные задачи дисциплины 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.

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

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

Дисциплина тесно связана с дисциплинами «Математическое моделирование информационных систем и процессов», «Высокопроизводительные технологии программирования».

Коды формируемых компетенций и требования к результатам освоения содержания дисциплины

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

Знать	1) области применения задач информационной безопасности; 2) стандарты шифрования; 3) методы защиты информации; 4) области применения различных методов информационной безопасности; 5) этапы, методы и инструментальные средства информационной безопасности. 6) принципы построения и функционирования систем информационной безопасности; 7) способностью разрабатывать и анализировать концептуальные и теоретические модели 8) классификацию шифров; 9) основы организации идентификации и цифровой подписи; 10) принципы построения и применения паролей; 11) правовые и этические последствия при получении доступа к информации не санкционированным лица
Уметь	12) проводить анализ и определять оптимальный метод защиты информации; 13) формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; 14) анализировать модели шифрования при организации защиты данных 15) формулировать и решать задачи организации процесса цифровой подписи; 16) формулировать и решать задачи организации процесса идентификации; 17) реализовать на языке программирования заданный метод защиты информации; 18) использовать математический аппарат определяющий шифр; 19) решать задачи анализа шифра; 20) оценить последствия при компрометации ключа или шифра
Владеть	21) методологиями и парадигмами построение систем информационной безопасности; 22) методами проектирования систем защиты информации; 23) методами построения алгоритмов анализа; 24) методами построения систем идентификации; 25) методами определения требований и состава средств, мероприятий по системе информационной безопасности систем; 26) навыками оценки правовых и этических компрометации данных 27) методами определения и создания шифра

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны

			знать	уметь	владеть
1.	ОПК-5	способностью использовать углубленные знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов	1, 2, 3, 5, 6, 9, 10	12, 13, 19, 20	25, 26
2.	ОК-2	готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения	2, 4, 5, 6, 10	12, 13, 20	22, 25,26
3.	ПК-2	способностью использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математики, фундаментальных концепций и системных методологий, международных и профессиональных стандартов в области информационных технологий	2, 3, 5, 7, 9	14, 15, 16	21, 22, 23, 24
4.	ПК-5	способностью управлять проектами, планировать научно-исследовательскую деятельность, анализировать риски, управлять командой проекта	1, 2, 5, 7, 8, 10	12, 17, 18, 19, 20	23, 24, 25, 27

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	СР	контроль
1.	Базовые понятия и история развития информационной безопасности.	22	4	4	10	4
2.	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	33,7	6	6	15	6,7
3.	Шифры замены. Шифры перестановки. Шифры гаммирования.	31	6	6	15	4
4.	Блочные системы шифрования.	35	6	6	19	4
5.	Поточные системы шифрования.	31	6	6	15	4
6.	Идентификация. Цифровые подписи.	27	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, СР – 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