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., 10 часов самостоятельной работы, 2 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»

Изучение данной учебной дисциплины направлено на формирование у обучающихся универсальных/ общепрофессиональных/ профессиональных компетенций (УК/ОПК/ПК):

Код и наименование индикатора	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
ОПК-5 Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	
ОПК-5.1. Знает методику установки и администрирования информационных систем и базданных. Знаком с содержанием Единого реестра российских программ.	современные подходы к организации сложных криптосистем; основные международные стандарты, регламентирующие применение криптографических методов защиты информации
ОПК-5.2. Умеет реализовывать техническое сопровождение информационных систем и баз данных.	анализировать текущее состояние ИБ на предприятии с целью разработки требований к средствам криптографической защиты информации (СКЗИ)
ОПК-5.3. Имеет практический опыт участия в научных студенческих конференциях, очных,виртуальных, заочных обсуждениях научных проблем в области информационных технологий.	навыками решения задач количественной оценки стойкости и производительности криптографических протоколов
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	
ПК-1.1. Знает основы научно-исследовательской деятельности в области информационных технологий, имеет научные знания в теории информационных систем.	основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры
ПК-1.2. Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности.	применять математические методы исследования моделей шифров
ПК-1.3. Имеет практический опыт научно- исследовательской деятельности в области информационных технологий.	навыками использования типовых криптографических алгоритмов; навыками использования ЭВМ в анализе простейших шифров

Структура и содержание дисциплины

Вид учебной работы		Всего часов	Форма обучения
			очная
			Семестры (часы)
			8
Контактная работа, в том числе:			
Аудиторные занятия (всего):		**42**	**42**
Занятия лекционного типа		14	14
Лабораторные занятия		28	28
Занятия семинарского типа (семинары, практические занятия)		–	–
		–	–
Иная контактная работа:			
Контроль самостоятельной работы (КСР)		2	2
Промежуточная аттестация (ИКР)		0,3	0,3
Самостоятельная работа, в том числе:		**10**	**10**
Курсовая работа		–	–
Проработка учебного (теоретического) материала		2	2
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		5	5
Реферат		–	–
Подготовка к текущему контролю		3	3
Контроль:		**экзамен**	**экзамен**
Подготовка к экзамену		53,7	53,7
Общая трудоёмкость	**час.**	**108**	**108**
	в том числе контактная работа	**44,3**	**44,3**
	зач. ед.	**3**	**3**

Автор Руденко О.В. – доцент кафедры вычислительных технологий