

Аннотация дисциплины

Б1.В.ДВ.10.01 «Криптографические протоколы»

Объем трудоемкости: 4 зачетных единиц (144 часов, из них – 48 часов аудиторной нагрузки: лекционных 16 ч., лабораторных работ - 32 ч., 45 часов самостоятельной работы, 44,7 часов на подготовку к экзамену, 6 часов КСР, 0,3 часа ИКР).

Цель дисциплины: формирование у студентов знаний и навыков по использованию методов согласованного решения задач информационного обмена с использованием криптографии.

Задачи дисциплины: освоить основные понятия, положения и методы, используемые в криптографических протоколах; знать основные виды криптографических протоколов и уметь использовать их для безопасного информационного взаимодействия.

Место дисциплины в структуре ООП ВО:

Дисциплина «Криптографические протоколы» относится к блоку дисциплин по выбору вариативной части базового цикла Б1.В.ДВ профессиональных дисциплин основной образовательной программы.

Для изучения дисциплины студент должен владеть знаниями, умениями и навыками по информационной безопасности, криптографии и распределенным задачам и алгоритмам.

Знания, получаемые при изучении дисциплины «Криптографические протоколы», могут использоваться при работе над выпускной работой, а также при изучении дисциплин магистерского цикла.

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих **профессиональных компетенций**:

№ п.п.	Индекс компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ПК-4	способностью решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива	способы решать задачи профессиональной деятельности	решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива	способностью решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива
2.	ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом	информационно-коммуникационные технологии и основные требования информационной безопасности	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры	способами использования криптографических протоколов в области информационных технологий, а также знаниями, которые находятся на передовом рубеже криптографической науки,

		основных требований информационной безопасности			инструментами поддерживающими информационную безопасность информационных систем
--	--	---	--	--	---

Основные разделы дисциплины

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
1	2	3	4	5	6	7
1	Криптографические протоколы и основные требования	14	2		4	8
2	Протоколы рукопожатия	14	2		4	8
3	Протоколы генерации ключей	20	4		8	8
4	Протоколы идентификации и аутентификации	18	4		8	6
5	Протоколы распределения ключей	13	2		4	7
6	Доказательства с нулевым разглашением секрета	14	2		4	8
7	Подготовка к экзамену	44,7				
8	КСР	6				
9	ИКР	0,3				
	Итого по дисциплине:	144	16	–	32	45

Изучение дисциплины заканчивается аттестацией в форме экзамена.

Основная литература

1. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 5-е изд., стер. - М. : Академия, 2011. - 331 с. : ил. - (Высшее профессиональное образование . Информатика и вычислительная техника) (Учебное пособие). - Библиогр.: с. 327-328. . (36 экз. в библиотеке КубГУ).
2. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации [Текст] : учебное пособие для студентов вузов /. - М. : Горячая линия-Телеком , 2005. - 229 с. . (10 экз. в библиотеке КубГУ).

Автор канд. физ.- мат. наук, доцент Жуков Сергей Александрович