Аннотация рабочей программы дисциплины
Б1.Б.19 Информационная безопасность

Направление подготовки: 02.03.03 "Математическое обеспечение и администрирование информационных систем"
Тип образовательной программы прикладной бакалавриат
Профиль: Общий
Форма обучения: очная

1. Цели и задачи дисциплины (модуля)

Целями освоения дисциплины «Информационная безопасность» являются ознакомление студентов с теоретическими основами информационной безопасности, основами криптографии и основами обеспечения защиты информации, формирование практических умений и навыков, необходимых для приобретения квалификации бакалавра информационных технологий, формирование ключевых профильных компетенций. Задачи освоения дисциплины: дать специальные знания по дисциплине, достичь достаточного уровня знаний по криптографическим и организационным методам обеспечения информационной безопасности и сформировать у студентов практические навыки работы со средствами обеспечения информационной безопасности.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» относится к дисциплинам вариативной части по направлению подготовки 020302 «Фундаментальная информатика и информационные технологии». Знания, умения и навыки, формируемые в процессе освоения дисциплины «Информационная безопасность» используются при прохождении производственной практики и выполнении выпускной квалификационной работы. Для усвоение дисциплины «Информационная безопасность» необходимы знания и навыки, сформированные дисциплинами «Информатика и программирование», «Дискретная математика», «Теория вероятностей и математическая статистика», «Языки программирования», «Теория чисел и ее приложения».

3. Требования к результатам освоения дисциплины (модуля):

Процесс изучения дисциплины направлен на формирование следующих компетенций:
ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

В результате изучения дисциплины студент должен:
Знать: международные и национальные стандарты в области информационной безопасности; основные виды угроз информационной безопасности и способы противодействия этим угрозам; основные нормативные правовые документы в сфере информационной безопасности; основные прикладные алгоритмы криптографии; основные средства обеспечения информационной безопасности; инфраструктуру открытых ключей; формальные модели безопасности.

Уметь:
соблюдать основные требования по противодействию наиболее распространенным угрозам информационной безопасности. составлять политики безопасности уровня методов

предприятия; анализировать и выбирать средства обеспечения информационной безопасности; анализировать алгоритмы взаимодействия на наличие уязвимостей

Владеть: основными навыками защиты информации; приемами анализа и классификации угроз информационной безопасности; основными навыками использования нормативных документов при организации обеспечения информационной безопасности на предприятии; навыками реализации прикладных алгоритмов криптографии в языках программирования, работы с криптопровайдерами, использования криптографических примитивов в языках программирования.

4. Объем дисциплины (модуля) и виды учебной работы (разделяется по формам обучения)

Вид учебной работы	**Всего часов / зачетных единиц**	**Семестры**			
		5	6		
Аудиторные занятия (всего)	153	66	87		
В том числе:	-	-	-	-	-
Лекции	70	30	40		
Практические занятия (ПЗ)					
Семинары (С)					
Лабораторные работы (ЛР)	70	30	40		
Самостоятельная работа (всего)					
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы					
Вид промежуточной аттестации (*зачет, экзамен*)	72	36	36		
Контактная работа (всего)	153	66	87		
Общая трудоемкость часы	225	102	123		
зачетные единицы	8	3	5		

5. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	**Наименование раздела**	**Наименование темы**	**Виды занятий в часах**					
			Лекц.	**Практ. зан.**	**Семин**	**Лаб. зан.**	**СРС**	**Всего**

1	2	3	4	5	6	7	8	9
1	Криптографические основы информационной безопасности	Основы криптографии	2			1		3
2		Симметричные криптосистемы	2			3		5
3		Поточные шифры	2			2		4
4		Блочное шифрование	4			4	2	10
5		Особенности блочного шифрования	4			4	2	10
6	Прикладные алгоритмы	Коды аутентификации сообщений	2			4		6
7		Хеш-функции	2			2		4
8		Стандарты аутентичного шифрования	4			4		8
9		Цифровая подпись	2			4		6
10		Схемы разделения секрета	2			2		4
11		Финансовая криптография	2			0	2	4
12		Доказательство знания	2			2		4
14	Организационные основы информационной безопасности	Информационная безопасность	2			2		4
15		Законодательный уровень обеспечения информационной безопасности	2			2	2	6
16		Виды и классификация возможных нарушений информационной	4			4	4	12

		безопасности						
17		Политика безопасности	2			4	2	8
18		Компьютерные вирусы	2			4	1	7
19		Модели безопасности и их применение	2			1		3
20		Безопасность беспроводных сетей	2			1		3

6. Форма промежуточной аттестации

Экзамен в 5,6 семестре.