

Аннотация рабочей программы дисциплины

«Информационная безопасность»

Направление подготовки

02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль) образовательной программы

Сетевые технологии

1. Цели и задачи освоения дисциплины

Основная цель дисциплины – овладеть методами и технологиями защиты информации на автоматизированных рабочих местах и в локальных вычислительных сетях на основе:

- требований существующих нормативно-правовых актов и стандартов к организации защиты информации;
- анализа возможных угроз информационным активам и оценкой уязвимостей информационных систем;
- применения инженерно-технических, программно-аппаратных и организационных механизмов защиты информации.

Основные задачи изучения дисциплины:

- Ознакомить студентов с терминологией в сфере информационной безопасности и основными положениями существующих концепций и нормативно-правовых актов по организации защиты информации.
- Овладеть методологией анализа возможных угроз информационным активам, оценкой уязвимостей информационных систем, оценкой ценности информационных активов организации.
- Ознакомиться с механизмами эффективной защиты информационных активов организации.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность» относится к обязательным дисциплинам базовой части учебного плана. Изучается в 6 семестре (3 курс), форма промежуточной аттестации – зачет с оценкой.

Перечень дисциплин с указанием разделов (тем), усвоение которых студентами необходимо для изучения дисциплины:

- Программирование на языке высокого уровня.
- Компьютерные сети.
- Операционные системы.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

После изучения данной дисциплины студенты приобретают знания, умения и владения (навыки), соответствующие результатам основной профессиональной образовательной программы.

Формируемые компетенции <i>(код компетенции, уровень (этап) освоения)</i>	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций
ОПК-4. Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<p>31(ОПК-4). Знать основы информационной безопасности личности и общества *)</p> <p>34 (ОПК-4) Знать терминологию в сфере информационной безопасности и современные проблемы защиты информации</p> <p>35 (ОПК-4) Знать основы методологии защиты информации в информационных системах</p> <p>36 (ОПК-4) Знать содержание основных понятий по правовому обеспечению информационной безопасности</p> <p>У5 (ОПК-4) Уметь проводить анализ угроз информационной безопасности ИС</p> <p>У6 (ОПК-4) Уметь проводить анализ состояния защищенности ИС</p>
ПК-4. Способность решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива	<p>У2 (ПК-4) Уметь использовать специализированное программное обеспечение для антивирусной профилактики, а также производить поиск вредоносных программ штатными утилитами операционных систем</p> <p>В4 (ПК-4) Владеть технологиями защиты информации на рабочих станциях от возможных угроз и кибератак и навыками безопасной работы в сети Интернет</p>

* результат обучения сформулирован на основании требований профессионального стандарта 06.015 СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННЫМ СИСТЕМАМ, утв. Приказом Минтруда России от 18.11.2014, № 896н (ред. от 12.12.2016, № 727н), регистрационный номер - 153.

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Объем дисциплины (модуля) составляет 3 зачетные единицы, всего 108 часов, из которых:

- **50 час составляет контактная работа обучающегося с преподавателем¹:**
 - 34 часа – лекционные занятия,
 - 16 часов – практические занятия,
- **мероприятия промежуточной аттестации (зачет с оценкой в 6 семестре);**
- **58 часов составляет самостоятельная работа обучающегося.**

¹ Перечень видов учебных занятий уточняется в соответствии с учебным планом.

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и виды учебных занятий

Наименование и краткое содержание разделов и тем дисциплины (модуля) Форма промежуточной аттестации по дисциплине (модулю)	Всего (часы)	Контактная работа (работа во взаимодействии с преподавателем), часы из НИХ ²						Самостоятельная работа обучающегося, часы, из них		
		Лекционные	Семинарские	Практические	Лабораторные	Учебные занятия, направленные на проведение текущего контроля	Всего	Выполнение	Подготовка	Всего
6 семестр										
Тема 1.Введение в предмет. Система защиты информации хозяйствующего субъекта	8	4					4	4		4
Тема 2. Нормативно-правовое обеспечение информационной безопасности	16	6				ПЗ 3.1	6	10		10
Тема 3.Организационные меры защиты информации	18	6		2		ПЗ 3.2, ПЗ 3.3	8	10		10
Тема 4. Криптографические методы защиты информации	20	6		4		ПЗ 4.1, ПЗ 4.2, ПЗ 4,3, ПЗ 4.4	10	10		10
Тема 5. Программно-аппаратные средства защиты информации	28	8		6		ПЗ 5.1, ПЗ 5,2	14	14		14
Тема 6.Инженерно-технические средства защиты информации	18	4		4		ПЗ 6.1	8	10		10
зачет с оценкой										
Итого	108	34		16			50	58		58

² Перечень видов учебных занятий уточняется в соответствии с учебным планом.

*Опрос (ПР-1), Практические работы (ПР-2), Реферат (ПР-3), *Экзамен (УО-4). Текущий контроль проводится за счет времени, отведенного на аудиторные занятия