АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

09.03.01 Информатика и вычислительная техника

Профиль: *Вычислительные машины, комплексы, системы и сети*

Б1.В.11 «Защита информации»

№ п.п.	Индекс	Наименование дисциплины	Курс	Курс	Контроль	Академических часов								з.е.	Компетенции	Группа
						Контакт	Контакт	Лек	Лаб	Пр	КРП	СР	Контроль			
11	Б1.В.11	Защита информации	4	7	Экз	**144**	54	28	26			54	36	4	ПК-7	ВМ-18

Формируемые компетенции: ПК-7

Содержание дисциплины

Лекции 14 шт. по 2 часа:

1.1. 1.1. Правовая основа информационной безопасности информационных систем.
1.2. Правовая защита информации персонального характера, персональные данные.
1.3. Законодательство РФ в области информационной безопасности.
1.4. Требования законодательства РФ по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей и меры по их обеспечению.
1.5. Основные положения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» с изменениями и дополнениями.
1.6. Виды, источники и классификация угроз информационной безопасности.
1.7. Угрозы безопасности персональных данных, уязвимости информационных систем ПД.
1.8. Базовая модель угроз безопасности персональных данных.
1.9. Основы аудита информационной безопасности. Политика и концепция информационной безопасности организации.
1.10. Основные методы и средства организации защиты информации.
1.11. Информационные системы персональных данных.

1.12. Организация и ведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах ПД.
1.13. Основные принципы защищенного электронного документооборота.
1.14. Электронная цифровая подпись. Система криптографической защиты Крипто-Про.
Лабораторные работы 6 шт. по 2 часа:
2.1. Законодательство РФ в области информационной безопасности. Правовая охрана компьютерных программ и баз данных.
2.2. Правовая защита персональных данных. Требования законодательства РФ по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей и меры по их обеспечению.
2.3. Анализ актуальных угроз информационной безопасности (согласно опубликованным сведениям ФСТЭК). Использование приложения Cisco Packet Tracer для моделирования элементов информационной безопасности (организация защиты на сетевом уровне) в вычислительных сетях.
2.4. Анализ уязвимостей информационных систем персональных данных. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Использование приложения Cisco Packet Tracer для моделирования элементов информационной безопасности (организация защиты на прикладном уровне, списки управления доступом с целью разграничения доступа к ресурсам ПК) в вычислительных сетях.
2.5. Общая система оценки уязвимостей (Common Vulnerability Scoring System – CVSS). Изучение возможностей CVSS –калькулятора. Разработка политики безопасности организации.
2.6. Изучение основных элементов программных средств, обеспечивающих защиту от вредоносных программ на примере антивируса Касперского. Разработка политики безопасности организации. Изучение основных элементов государственных информационных систем персональных данных. Организация и ведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Заполнение уведомления об обработке (о намерении осуществлять обработку) персональных данных.
Лабораторные работы 1 шт. 2 часа:
2.7. Основные принципы применения электронной цифровой подписи. Система криптографической защиты КриптоПро.

Год начала подготовки (по учебному плану) __2018___
Образовательный стандарт (ФГОС) __№ 929 от 19.09.2017___