

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ «Защита информации»

по основной профессиональной образовательной программе по направлению подготовки
09.03.01 «Информатика и вычислительная техника» (уровень бакалавриата)

Направленность (профиль): Программно-техническое обеспечение автоматизированных систем
Общий объем дисциплины – 3 з.е. (108 часов)

Форма промежуточной аттестации – Зачет.

В результате освоения дисциплины у обучающихся должны быть сформированы компетенции с соответствующими индикаторами их достижения:

- ОПК-2.1: Выбирает информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности;
- ОПК-2.2: Использует современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности;
- ОПК-3.1: Использует основы информационной и библиографической культуры при работе с профессиональной информацией;
- ОПК-3.2: Применяет информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности;
- ОПК-3.3: Учитывает основные требования информационной безопасности при решении стандартных задач профессиональной деятельности;

Содержание дисциплины:

Дисциплина «Защита информации» включает в себя следующие разделы:

Форма обучения очная. Семестр 8.

1. Понятие, сущность, цели и концептуальные основы защиты информации. Общий контекст защиты информации. Понятие «защита информации». Сущность и содержание защиты информации. Цели и задачи защиты информации. Концептуальная модель защиты информации. Основные свойства информации с точки зрения её безопасности. Понятие и состав защищаемой информации. Принципы отнесения информации к защищаемой. Правовое обеспечение защиты информации. Использование основ информационной и библиографической культуры, современных информационных и информационно-коммуникационных технологий и программных средств, в том числе отечественного производства при решении задачи защиты информации..

2. Объекты защиты информации. Понятие объекта защиты информации. Носители защищаемой информации как конечные объекты защиты. Средства и системы обработки информации как объекты защиты. Средства обеспечения объекта информатизации. Помещения объектов информатизации как объекты защиты. Защищаемые информационные процессы. Носители защищаемой информации..

3. Угрозы защищаемой информации. Виды, методы и средства защиты информации. {лекция с разбором конкретных ситуаций. Понятие угрозы и её взаимосвязь с уязвимостью и рисками. Общая классификация угроз безопасности информации. Технические каналы утечки информации. Цели и задачи оценки угроз защищаемой информации. Виды защиты информации и сферы их действия. Общие способы защиты информации. Общая классификация средств защиты информации. Характеристика способов и средств по видам защиты информации..

4. Технологии безопасности компьютерных систем. Угрозы безопасности информации в компьютерных системах. Защита информации от случайных угроз. Защита информации от несанкционированного доступа. Модели управления доступом к объектам компьютерных систем. Классификация компьютерных вирусов, механизмы защиты от них. Защита информации от перехвата по техническим каналам утечки информации. Защита от несанкционированного доступа и копирования информации. Состав программного и аппаратного обеспечения, предназначенного для защиты информации. Особенности инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем, предназначенного для защиты информации. Выбор и использование информационных технологий и программных средств, в том числе отечественного производства, при решении задач защиты информации. Применение информационно-коммуникационных технологий для решения задач защиты информации..

5. Криптографические методы защиты информации. Классификация методов криптографического преобразования информации. Цели криптографии. Основные понятия. Алгоритмы шифрования с симметричным ключом. Алгоритмы шифрования с открытым ключом. Электронная подпись. Функции хеширования. Протоколы аутентификации.

6. Стандарты и нормативные акты в области информационной безопасности. Состав стандартов и нормативных документов по информационной безопасности в компьютерных системах и автоматизированных системах. Документы в области защиты от вредоносного кода. Руководящие документы в области защиты автоматизированных систем. Специальные требования и рекомендации по технической защите конфиденциальной информации. Документы ФСТЭК России и ФСБ России. Состав нормативных актов по видам защищаемой информации. Решение стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

7. Комплексная система защиты информации на предприятии. Понятие и общая структура системы защиты информации. Общеметодологические требования и принципы построения систем защиты. Понятие и общая структура комплексной системы защиты информации на предприятии. Компоненты комплексной системы защиты информации на предприятии их назначение и состав. Нормативно-методические документы и стандарты для реализации различных компонентов. Определение требований информационной безопасности при разработке моделей компонентов информационных систем, включая модели баз данных и модели интерфейсов "человек - электронно-вычислительная машина".

Разработал:
старший преподаватель
кафедры ИВТиИБ

А.В. Циклаков

Проверил:
Декан ФИТ

А.С. Авдеев