Аннотация дисциплины
«Методы и средства защиты информации»

Дисциплина «Методы и средства защиты информации» предназначена для изучения в рамках направления подготовки 11.03.02 Инфокоммуникационные технологии и системы связи, профиль «Системы радиосвязи и радиодоступа».

Дисциплина входит в вариативную часть блока 1 Дисциплины (модули) учебного плана, является дисциплиной по выбору. Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 часов. Учебным планом предусмотрены лекционные занятия (18 часов), практические занятия (36 часов). На самостоятельную работу отведено 126 часов. Дисциплина реализуется на 3-м курсе в 5-м семестре.

Для изучения дисциплины требуется знание основ построения телекоммуникационных систем и общей теории связи, изучаемых в дисциплинах «Электроника» и «Теоретические основы связи».

Целью дисциплины является ознакомление студентов с основными методами и средствами защиты компьютерной информации.

Задачи дисциплины:

- получение теоретических знаний и практических навыков при решении типовых задач по обеспечению информационной безопасности;
- изучение проблем защиты информации, стоящих перед современной вычислительной техникой;
- умение использовать полученные знания для правильного выбора решений при разработке.

Для успешного изучения дисциплины «Методы и средства защиты информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

- ОПК-3 - способность владеть основными методами, способами и средствами получения, хранения, переработки информации;
- ОПК-4 - способность иметь навыки самостоятельной работы на компьютере и в компьютерных сетях, осуществлять компьютерное моделирование устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ;

- ОПК-5 - способность использовать нормативную и правовую документацию, характерную для области инфокоммуникационных технологий и систем связи (нормативные правовые акты Российской Федерации, технические регламенты, международные и национальные стандарты, рекомендации Международного союза электросвязи);
- ПК-16 - готовностью изучать научно-техническую информацию, отечественный и зарубежный опыт по тематике исследования.

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОПК-1 - способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Знает	базовые способы оценки и повышения защищенности информационных ресурсов в корпоративных информационных системах, способы инвентаризации программных сервисов и информационных ресурсов, ключевые точки приложения информационных атак в типовой структуре корпоративных ИС, методы и алгоритмы реструктуризации и реинжиниринга информационных процессов в рамках корпоративной информационной инфраструктуры
	Умеет	ставить и решать типовые задачи в области оценки и повышения защищенности корпоративных ИС, подбирать и использовать адекватные методы и средства защиты информации, оценивать эффективность методов защиты информационных процессов
	Владеет	навыками аудита информационной безопасности с использованием современных программно-технических средств, приемами тестирования уязвимостей корпоративных программно-технических сервисов, типовыми атаками на ИС предприятий, современным аппаратом для количественной и качественной оценки результатов аудита, комплексами средств защиты информации.
ОПК-2 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с	Знает	принципы и методы организационной защиты информации, создания систем охранно- тревожной сигнализации, систем контроля и управления доступом, охранного телевидения; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и

применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности		методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; современные компьютерные технологии и программное обеспечение для решения задач, связанных с процедурами обработки аналитической информации и поиском информации.
	Умеет	квалифицированно применять полученные знания; анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; формировать комплекс мер по информационной безопасности с учетом его технической обоснованности и реализуемости; осуществлять изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.
	Владеет	методами и средствами выявления угроз безопасности автоматизированным системам; навыками организации и обеспечения режима секретности; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации; профессиональной терминологией; навыками безопасного использования технических средств в профессиональной деятельности; навыками поиска технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов в профессиональной деятельности.