Аннотация к рабочей программе дисциплины
«Основы управления информационной безопасностью»

Курс учебной дисциплины «Основы управления информационной безопасностью» предназначен для обучения студентов направления 10.03.01 «Информационная безопасность», профиль «Комплексная защита объектов информатизации» и входит в состав базовых дисциплин учебного плана Б1.Б.12.06.

Общая трудоемкость освоения дисциплины составляет 108 часов (3 з.е.). Учебным планом предусмотрены лекционные занятия (18 час.), практические занятия (36 час.), самостоятельная работа (54 час.). Дисциплина реализуется на 3 курсе в 6 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Основы управления информационной безопасностью» логически и содержательно связана с такими курсами, как «Основы информационной безопасности», «Основы проектной деятельности».

Содержание дисциплины охватывает следующий круг вопросов: понятие ИБ, основные составляющие, важные проблемы, законодательный уровень ИБ, риски в области ИБ, управление рисками, организация комплексной системы защиты информации.

Цель:

- привитие стремления к поиску оптимальных, простых и надежных решений;

- изучение основ информационной безопасности, формирование у

студентов информационного мировоззрения на основе знания принципов защиты информации; воспитание информационной культуры для эффективного применения полученных знаний в профессиональной деятельности;

- развитие творческих подходов при решении сложных научно-

технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры;

- развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления;
- привитие стремления к поиску оптимальных, простых и надежных решений.

Задачи:

- изучение структур и тенденций развития концептуальных, методологических и организационных основ и современных принципов защиты информации для обеспечения информационной безопасности государства;
- формирование основных теоретических и практических знаний, раскрывающих сущность и значение национальной безопасности и защиты информации в условиях локальных и глобальных вычислительных сетей, автоматизированных информационных систем и систем телекоммуникаций;
- изучить основные положения Доктрины информационной безопасности РФ;
- изучить основы комплексной системы защиты информации;
- изучить основы организационно-правового обеспечения защиты информации;
- изучить методы и средства ведения информационных войн;
- изучить методологии создания систем защиты информации.

Для успешного изучения дисциплины «Основы управления информационной безопасностью» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и

защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-12);

- способность оценивать уязвимости информационных систем, разрабатывать требования и критерии оценки информационной безопасности, согласованных со стратегией развития информационных систем (ПК-10);

- способность разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, проводить выбор необходимых технологий и технических средств, организовать внедрение и последующее сопровождение (ПСК-3.3).

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОК-3) способностью проявлять инициативу и принимать ответственные решения, осознавая ответственность за результаты своей профессиональной деятельности	Знает	особенности организации профессиональной работы структур, учреждений, функционирующих в сфере международных связей
	Умеет	применять знания о деятельности организаций, занимающихся вопросами международных отношений при решении профессиональных задач
	Владеет	навыками аналитического оценивания изучаемых проблем, навыками решения проблем, применяя профессиональные навыки и умения
(ПК-16) способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Знает	Правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны
	Умеет	Анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	Методами формирования требований по защите информации
(ПК-17) способностью	Знает	Методы и принципы организационной

организовывать работу малого коллектива исполнителей в профессиональной деятельности		защиты информации на предприятии
	Умеет	Формулировать и настраивать политику безопасности распространенных систем, а также локальных вычислительных сетей, построенных на их основе
	Владеет	Методами формирования требований по защите информации на предприятии
(ПК-18) способностью организовывать и выполнять работы по созданию, монтажу, наладке, испытанию и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности	Знает	основные факты о системах с открытым ключом
	Умеет	строить и изучать математические модели криптоалгоритмов
	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем
(ПК-19) способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Знает	первоочередные мероприятия по обеспечению безопасности информации АС организации
	Умеет	Пользоваться нормативными документами по защите информации
	Владеет	Методиками проверки защищенности объектов информации на соответствие требований нормативных документов

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы управления информационной безопасностью» применяются следующие методы активного/интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).