Аннотация
рабочей программы дисциплины
«Информационная безопасность и защита информации»

подготовки бакалавра по направлению 38.03.05 «Бизнес информатика»
профиль «ИТ менеджмент в бизнесе»

1.Цели и задачи дисциплины.

Цель дисциплины - формирование у студентов навыков, связанных с обеспечением защиты информации; творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности объектов информатизации; создание представления об основах информационной безопасности, принципах и методах противодействия несанкционированному информационному воздействию; развитие способностей к логическому и алгоритмическому мышлению.

Задачи дисциплины:

- изучить место и роль информационной безопасности в системе национальной безопасности Российской Федерации; основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; 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 методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- сформировать умения и навыки проведения анализа и оценки угроз информационной безопасности объекта;
- обучить работе с современными технологиями обеспечения информационной безопасности.

2.Место дисциплины в структуре ОП:

Дисциплина «Информационная безопасность и защита информации» является дисциплиной блока дисциплин по выбору, углубляющих знания, полученные по обязательным дисциплинам образовательной программы направления 38.03.05 Бизнес-информатика.

Дисциплины, предшествующие изучению дисциплины «Информационная безопасность и защита информации»:

- Управление информационно-технологическими проектами;
- Информационные системы управления организацией;
- Информационные технологии в профессиональной деятельности;
- Информационно-технологическая инфраструктура организации;
- Корпоративные системы электронного документооборота.

Изучается в 6 семестре.

3.Требования к результатам освоения дисциплины:

Процесс изучения дисциплины «Информационная безопасность и защита информации» направлен на формирование следующих компетенций: ПК-11, ПК-21, ПКП-1.

В результате изучения дисциплины студенты должны:

знать:

- стандарты, законы по вопросу информационного права и информационной безопасности;
- виды интеллектуальных прав;
- виды рисков информационной уязвимости в компьютерных системах;

- стандарты, методы и модели информационной безопасности ИТ-инфраструктуры предприятия;
- принципы и методы противодействия несанкционированному информационному воздействию;
- методологии построения и управления ИТ- инфраструктурой организации;
- рекомендации международных стандартов по управлению ИТ-услугами;
- методы и системы управления ИТ-инфраструктурой предприятия;

уметь

- оперировать понятиями и категориями права на результаты интеллектуальной деятельности и средства индивидуализации;
- проводить анализ рисков информационной безопасности автоматизированной системы;
- проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня безопасности применения автоматизированных систем;
- определять ресурсы, необходимые для обеспечения надежности функционирования информационных систем;
- оптимизировать ИТ-процессы;

владеть:

- навыками анализа нормативных правовых актов для определения субъектов права на защиту;
- методикой консультирования заказчиков по вопросам информационной безопасности;
- навыками выбора ресурсов ИТ в условиях меняющихся бизнес-потребностей.

Формы контроля.

Текущий контроль:

- контрольная работа.

Промежуточный контроль:

- зачет.

4.Обьём дисциплины и виды учебной работы

Планируемая трудоёмкость дисциплины составляет 144 часа.