Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Институт коммерции, маркетинга и сервиса
Кафедра электронной коммерции и управления электронными ресурсами

АННОТАЦИЯ

по дисциплине

«Информационная безопасность корпоративных информационных систем»

направление подготовки 09.03.03 Прикладная информатика
профиль «Прикладная информатика в электронной экономике»
всех форм обучения

Год начала подготовки:2016

Соответствует РПД Зав. кафедрой д.э.н., проф.

_____**УМУ СГЭУ** _____ / Погорелова Е.В

Учебно-методическое управление

Квалификация (степень) выпускника - бакалавр

Самара 2016 г.

1 Место дисциплины в структуре ООП

Цели и задачи дисциплины

Дисциплина «Информационная безопасность корпоративных информационных систем» должна обеспечить формирование профессиональных компетенций с целью реализации на практике комплекса знаний по защите информации путем выполнения сложных работ, связанных с обеспечением комплексной защиты информации на основе разработанных программ и методик, а также проведения сбора и анализа материалов учреждений, организаций и предприятий отрасли с целью выработки и принятия решений и мер по обеспечению защиты информации и эффективному использованию средств автоматического контроля, обнаружения возможных каналов сетевых атак и утечки сведений, представляющих служебную или коммерческую тайну.

Основные задачи дисциплины «Информационная безопасность корпоративных информационных систем»:

- комплексное использование методологии защиты информации;
- изучение методов и средств обнаружения атак на корпоративные автоматизированные информационные системы (КАИС);
- освоение практических навыков работы по использованию современных информационных технологий прогнозирования вероятных угроз и возможности противодействия выявленным информационным угрозам для обеспечения эффективного функционирования социально-экономических субъектов.

Дисциплина «Информационная безопасность корпоративных информационных систем» относится к блоку Б1.Дисциплины (модули) учебного плана и входит в базовую часть (Б1.Б.15). Для изучения дисциплины необходимы знания, умения и компетенции студента, которые были получены при изучении дисциплин: Операционные системы; Программная инженерия; Вычислительные системы, сети и телекоммуникации.

Знания, полученные при изучении данной дисциплины, необходимы при выполнении выпускной работы.

2. Планируемые результаты обучения

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4) (этап формирования компетенции – начальный);
- способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4) (этап формирования компетенции – промежуточный);
- способностью проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе (ПК-1) (этап формирования компетенции – промежуточный);
- способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (ПК-18) (этап формирования компетенции – начальный).

В результате изучения дисциплины в разрезе дескрипторных характеристик компетенций студенты должны владеть:

1. Способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4):

– **знать:** основы правовых знаний в различных сферах деятельности;

– **уметь:** применять основы правовых знаний в различных сферах деятельности;

– **владеть:** основными методами, способами и средствами получения правовых знаний в различных сферах деятельности с помощью компьютерных технологий.

2. Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4) и способностью проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе (ПК-1);

- **знать:** особенности процессов формализации требований заказчика, языки формального описания прикладных задач, принципы администрирования программных систем MS Office, Windows;
- **уметь:** проводить аудит локальной системы и формулировать постановку задачи на языке моделирования;
- **владеть:** навыками работы с CASE программами и навыками расчета технико-экономического обоснования проектных решений.

3. Способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (ПК-18).

- **знать:** основные модели представления и реализации информационных угроз, методы и этапы проведения анализа структуры и содержания информационных угроз, методы моделирования и развития систем обнаружения информационных атак.
- **уметь:** формулировать задачи и выбирать адекватные средства противодействия информационным угрозам; пользоваться математическим аппаратом и соответствующими информационными технологиями; проводить содержательный анализ и интерпретацию информационных угроз.
- **владеть:** методикой разработки эффективных моделей противодействия информационным угрозам; методикой администрирования подсистем информационной безопасности КАИС.

3. Объем дисциплины и виды учебной работы

Вид учебной работы	**Всего часов /зачетных единиц**	**7 семестр**
Аудиторные занятия	72/2	72/2
В том числе:		
Лекции	18/0,5	18
Практические занятия (ПЗ)		
Семинары (С)		
Лабораторные работы (ЛР)	54/1,5	54
Самостоятельная работа (всего)	62/1,72	62
В том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Реферат		
Другие виды самостоятельной работы		
Вид промежуточной аттестации (зачет)	зачет 10/0,28	зачет 10
Общая трудоемкость 144 часов 4 зачетных единиц	144/4	144