

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ
УНИВЕРСИТЕТ

Институт систем управления

Кафедра прикладной информатики и информационной безопасности

АННОТАЦИЯ

по дисциплине

«Управление информационной безопасностью»

**направление подготовки 10.03.01 Информационная безопасность
профиль «Организация и технология защиты информации»
очной формы обучения**

Соответствует РПД



Зав. кафедрой

A handwritten signature in black ink is written over a horizontal line. Below the signature, the name "Абросимов А.Г." is printed in black.

Самара 2015 г.

1. Цели и задачи дисциплины

Изучение дисциплины «**Управление информационной безопасностью**» направлено на усвоение роли и места защиты информации в системе обеспечения комплексной безопасности предприятия (организации) в различных условиях ее деятельности, на четкое понимание принципов, задач, функций, методов и технологий управления системой защиты информации, а также на умение осуществлять комплекс управленческих мероприятий по информационной безопасности предприятия; осуществлять подбор, расстановку, обучение персонала предприятия приемам и способам защиты информации.

В ходе занятий по дисциплине получают первичные знания о задачах, о структуре, должностном составе и других организационно-правовых основах организации и деятельности службы безопасности на предприятиях различных форм собственности.

2. Место дисциплины в структуре ООП

Дисциплина «Управление информационной безопасностью» относится к циклу профессиональных дисциплин образовательной программы направления «Информационная безопасность» профиль «Организация и технология защиты информации» базируется на знаниях, полученных при изучении дисциплин: «Теория информационной безопасности и методология защиты информации», «Правовая защита информации», «Инженерно-техническая защита информации», «Информатика» и другие.

3. Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Общекультурные компетенции (ОК):

способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК - 6);

способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления (ОК - 8).

Профессиональные компетенции (ПК):

способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК - 3);

способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК - 4);

способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации

с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК - 5);

способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК - 6);

способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК - 8);

способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК - 9);

Студент, изучающий дисциплину должен:

Знать:

- перспективы развития и совершенствования организационно-правовых мероприятий по защите информации;
- роль и место организационной защиты информации в системе комплексной безопасности предприятия;
- особенности защиты информации на предприятиях различных форм собственности;
- порядок засекречивания и рассекречивания, сведений, документов и продукции;
- порядок организации и осуществления допуска и доступа к конфиденциальной информации и документам;
- порядок подготовки и проведения совещаний и заседаний по конфиденциальным вопросам;
- организацию охраны предприятий;
- задачи и функции службы защиты информации;
- структуру и штаты службы защиты информации.

Уметь:

- осуществлять подбор, расстановку, обучение персонала предприятия приемам и способам защиты информации;

Владеть:

- методами и технологиями управления системой защиты информации, а также правильно организовывать и осуществлять комплекс организационных и управленческих мероприятий по информационной безопасности предприятия;
- владеть методами анализа и оценки риска, методами определения размеров возможного ущерба вследствие разглашения сведений, составляющих государственную и другие виды тайн;
- владеть методами организации и управления службами защиты информации.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов/зач. единиц	Сем. 7 по УП
Аудиторные занятия	72/2,0	72/2,0
В том числе:		
Лекции	36/2,0	36/2,0
Практические занятия (ПЗ)		
Семинары (С)		
Лабораторные работы (ЛР)	36/2,0	36/2,0
Самостоятельная работа (всего)	72/2,0	72/2,0
В том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Реферат		
Другие виды самостоятельной работы		
Вид промежуточной аттестации (зачет, экзамен)	Экзамен	Экзамен
Общая трудоемкость 144 час	144/4,0	144/4,0