МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ
Институт систем управления
Кафедра прикладной информатики и информационной безопасности

АННОТАЦИЯ

по дисциплине **«Теория информационной безопасности и методология защиты информации»**

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

Соответствует РПД

УМУ СГЭУ **Зав. кафедрой**

/Абросимов А.Г./

Самара 2015 г.

1. Цели и задачи дисциплины.

Цели: раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов.

Основные ***задачи*** дисциплины «Теория информационной безопасности и методология защиты информации»:

- ознакомить студентов с понятийным аппаратом в области информационной безопасности и защиты информации;
- рассмотреть базовые содержательные положения в области информационной безопасности и защиты информации;
- изучить современную доктрину информационной безопасности;
- определить цели и принципы защиты информации;
- ознакомить студентов с составом защищаемой информации, ее классификацией по видам тайны, материальным носителям, собственникам и владельцам;
- создать теоретическую базу для последующих дисциплин, связанных с разработкой различных способов защиты информации.

2. Место дисциплины в структуре ООП:

Дисциплина «Теория информационной безопасности и методология защиты информации» относится к относится к разделу Б3.В.ОД.11 учебного плана бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность» к группе обязательных дисциплин вариативной части. Читается студентам в четвертом семестре.

Для освоения курса студентам необходимо предварительно овладеть знаниями и умениями по дисциплинам:

- Основы информационной безопасности;
- Математика.

Знания, полученные при изучении данной дисциплины, необходимы при изучении дисциплин:

- Программно-аппаратные средства защиты информации;
- Особенности обработки секретной документации.

3. Требования к результатам освоения дисциплины:

Процесс изучения дисциплины «Теория информационной безопасности и методология защиты информации» направлен на формирование следующих компетенций:

Общекультурные компетенции:

ОК-7	способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства

Общепрофессиональные компетенции:

ПК-2	способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах
ПК-3	способностью использовать нормативные правовые документы в своей профессиональной деятельности

ПК-16	способностью использовать инструментальные средства и системы программирования для решения профессиональных задач
ПК-19	экспериментально-исследовательская деятельность: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности
ПК-30	способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности

В результате изучения дисциплины студенты должны:

знать:

- базовый понятийный аппарат в области информационной безопасности (ИБ) и защиты информации;
- виды и состав угроз информационной безопасности;
- принципы и общие методы обеспечения ИБ;
- основные положения государственной политики обеспечения ИБ;
- критерии, условия и принципы отнесения информации к защищаемой;
- виды носителей защищаемой информации;
- виды и подвиды тайн конфиденциальной информации;
- виды уязвимости защищаемой информации и формы ее проявления;
- источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;
- каналы и методы несанкционированного доступа к конфиденциальной информации;
- состав объектов защиты информации;
- классификацию видов, методов и средств защиты информации;
- состав кадрового, ресурсного и технологического обеспечения защиты информации.

уметь:

- выявлять угрозы ИБ применительно к объектам защиты;
- определять состав конфиденциальной информации применительно к видам тайны;
- выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия;
- выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации;
- определять направления и виды защиты информации с учетом характера информации и задач по ее защите;
- организовывать системное обеспечение защиты информации.

владеть:

- правовой терминологией в области защиты информации;
- научно-технической литературой и СМИ в области защиты информации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов дневной формы обучения составляет 4 зачетных единиц.

Вид учебной работы	**Всего часов/зачетных единиц**	**Семестр 4**
Аудиторные занятия	72/2	72/2
В том числе:		
Лекции	36/1	36/1
Практические занятия (ПЗ)		
Семинары (С)		
Лабораторные работы (ЛР)	36/1	36/1
Самостоятельная работа (всего)	45/1,25	45/1,25

В том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Реферат		
Другие виды самостоятельной работы	27/0,75	27/0,75
Вид промежуточной аттестации (зачет, экзамен)	экзамен	экзамен
Общая трудоемкость	144 час. 4 зач. единиц	144 час. 4 зач. единиц