Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет
имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ

по дисциплине

С.3.2.2 «Комплексное обеспечение информационной безопасности автоматизированных систем»

специальности подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
Специализация «Создание автоматизированных систем в защищенном исполнении»

форма обучения – очная
курс – 5
семестр – 9
зачетных единиц – 6
часов в неделю – 5
всего часов – 216,
в том числе:
лекции – 36
лабораторные занятия – 54
самостоятельная работа – 126
курсовой проект – 9 семестр
экзамен – 9 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем»: подготовка студентов к деятельности по созданию систем информационной безопасности автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите, на базе комплексного подхода применения правил, процедур, практических приемов, руководящих принципов, методов, средств обеспечения информационной безопасности.

Задачи изучения дисциплины:

сформировать способность к комплексному применению мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированной системы.

2. Место дисциплины в структуре ООП ВПО

Дисциплина «Комплексное обеспечение информационной безопасности автоматизированных систем» относится к числу дисциплин вариативной части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин «Техническая защита информации», «Криптографические методы защиты информации», «Организационное и правовое обеспечение информационной безопасности», «Программно-аппаратные средства защиты информации», «Разработка и эксплуатация защищенных автоматизированных систем».

Знания, умения и навыки, сформированные при изучении дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем» необходимы при выполнении научно-исследовательской и выпускной квалификационной работ.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ПК-6 способность использовать нормативные правовые акты в своей профессиональной деятельности;

ПК-21 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;

ПК-22 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы;
ПК-33 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;
ПК-34 способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы;
ПК-35 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;
ПК-36 способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы;
ПК-37 способность администрировать подсистему информационной безопасности автоматизированной системы;
ПК-38 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы;
ПК-39 способность управлять информационной безопасностью автоматизированной системы;

Студент должен знать:

- требования нормативных правовых документов при построении комплексных систем защиты информации;
- принципы и методы проектирования системы управления информационной безопасностью автоматизированной системы;
- средства защиты информации и средства контроля защищенности автоматизированной системы;
- понятие, состав и содержание политики информационной безопасности организации, методы контроля эффективность ее реализации;
- содержание принципа комплексности при применении основных мер по защите информации в автоматизированных системах;
- информационно-технологические ресурсы автоматизированной системы и требования информационной безопасности при их применении;
- средства защиты информационно-технологических ресурсов автоматизированной системы;
- процедуру администрирования подсистему информационной безопасности автоматизированной системы;
- Принципы разработки частных политик информационной безопасности автоматизированной системы;
- методы управления информационной безопасностью автоматизированной системы

Студент должен уметь:

- применять нормативные правовые документы при построении комплексных систем защиты информации;
- выполнять задачи по проектированию системы управления информационной безопасностью автоматизированной системы;
- осуществлять выбор средств защиты информации и средств контроля защищенности автоматизированной системы при проектировании комплексных систем защиты информации;
- формировать политику информационной безопасности организации и контролировать эффективность ее реализации;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
- обеспечивать эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;
- эффективно применять средств защиты информационно-технологических ресурсов автоматизированной системы;
- администрировать подсистему информационной безопасности автоматизированной системы;
- выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы;
- управлять информационной безопасностью автоматизированной системы.

Студент должен владеть:

- навыками работы с нормативными правовыми актами при построении комплексных систем защиты информации;
- навыком участия в проектировании системы управления информационной безопасностью автоматизированной системы;
- навыком участия в выборе средств защиты информации и средств контроля защищенности автоматизированной системы при проектировании комплексных систем защиты информации;
- навыком формирования политики информационной безопасности организации и контроля эффективность ее реализации;
- навыками формирования комплекса мер для обеспечения информационной безопасности автоматизированных систем;
- навыком обеспечения эффективного применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;

- навыком эффективного применения средств защиты информационно-технологических ресурсов автоматизированной системы;
- навыком администрирования подсистемы информационной безопасности автоматизированной системы;
- навыком выполнения частных политик информационной безопасности автоматизированной системы и осуществления мониторинга безопасности автоматизированной системы;
- навыком управления информационной безопасностью автоматизированной системы.