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

«Б.1.3.10.1 Угрозы информационной безопасности автоматизированных систем»

направления подготовки
10.03.01 «Информационная безопасность»
Профиль «Безопасность автоматизированных систем»

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 2
часов в неделю – 2
всего часов – 72,
в том числе:
лекции – 16
коллоквиум – 2
практические занятия – 18
самостоятельная работа – 36
зачет – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины «Угрозы информационной безопасности автоматизированных систем»: изучение основных понятий, типов и источников угроз информационной безопасности в автоматизированных системах.

Задачи изучения дисциплины:

- формирование у обучаемых целостного представления об источниках угроз информационной безопасности;
- дать представление о видах и возможных методах и путях реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;
- приобретение обучаемыми необходимого объема знаний и практических навыков в области построения модели угроз информационной безопасности.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Угрозы информационной безопасности автоматизированных систем» относится к числу дисциплин специализации профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Технологии и методы программирования», «Основы информационной безопасности», «Криптографические методы защиты информации», «Сети и системы передачи информации», «Безопасность операционных систем».

Дисциплина «Угрозы информационной безопасности автоматизированных систем» является предшествующей и необходимой для изучения следующих дисциплин специализации: «Создание автоматизированных систем в защищенном исполнении», «Оценка информационной безопасности автоматизированных систем в защищенном исполнении», «Управление информационной безопасностью». Знания и практические навыки, полученные по дисциплине «Угрозы безопасности информации», используются при подготовке выпускной квалификационной работы.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ОПК-5 способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ОПК-7 способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций

ПК-7 способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ

Студент должен знать:

- понятие и принципы разработки модели угроз и модели нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
- угрозы безопасности информации, потенциально и/или реально существующие в процессе создания и эксплуатации автоматизированных систем;
- методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении с учетом угроз безопасности информации;
- технологии моделирования угроз безопасности информации при проектировании автоматизированных систем в защищенном исполнении;
- нормативные правовые акты, руководящие и методические документы, регламентирующие вопросы моделирования и определения актуальности угроз безопасности информации;
- состав и содержание мер по определению угроз безопасности информации в процессе создания и эксплуатации
- автоматизированных систем в защищенном исполнении;

Студент должен уметь:

- разрабатывать модели угроз и модели нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
- выявлять, классифицировать угрозы безопасности информации, потенциально и/или реально существующие в процессе создания и эксплуатации автоматизированных систем;
- выбирать методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении с учетом угроз безопасности информации;
- применять современные технологии моделирования угроз безопасности информации при проектировании автоматизированных систем в защищенном исполнении;
- применять нормативные правовые акты, руководящие и методические документы, регламентирующие вопросы моделирования и определения актуальности угроз безопасности информации;

- проводить анализ достаточности мер по определению угроз безопасности информации в процессе создания и эксплуатации автоматизированных систем в защищенном исполнении

Студент должен владеть навыками:

- навыком разработки разрабатывать моделей угроз и моделей нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
- навыком определения угроз безопасности информации, потенциально и/или реально существующие в процессе создания и эксплуатации автоматизированных систем;
- навыком выбора методов и средств для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении с учетом угроз безопасности информации;
- навыком применения современных технологий моделирования угроз безопасности информации при проектировании автоматизированных систем в защищенном исполнении;
- навыком применения нормативных правовых актов, руководящих и методических документов, регламентирующих вопросы моделирования и определения актуальности угроз безопасности информации;
- навыком анализа достаточности мер по определению угроз безопасности информации в процессе создания и эксплуатации автоматизированных систем в защищенном исполнении.