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

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине

«С.3.1.18.1 Угрозы информационной безопасности автоматизированных систем»

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

форма обучения – очная
курс – 4
семестр – 7
зачетных единиц – 3
часов в неделю – 3
всего часов – 108,
в том числе:
лекции – 18
лабораторные занятия – 36
самостоятельная работа – 54
зачет – 7 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 ВПО

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:

ПСК-9.1 способностью разрабатывать модели угроз и модели нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;

ПСК-9.2 способностью принимать участие в разработке, реализации и управлении процессами создания и эксплуатации автоматизированных систем в защищенном исполнении на всех стадиях и этапах их жизненного цикла;
ПСК-9.3 способностью рационально выбирать методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
ПСК-9.4 способностью применять современные технологии проектирования автоматизированных систем в защищенном исполнении;
ПСК-9.5 способностью применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла;
ПСК-9.6 способностью проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении.

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.