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

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА
по дисциплине

Б.1.1.34 «Создание автоматизированных систем в защищенном исполнении»

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

форма обучения – очная
курс – 4
семестр – 7
зачетных единиц – 3
часов в неделю – 3
академических часов – 108
в том числе:
лекции – 16
практические занятия – 32
самостоятельная работа – 60
зачет – 7 семестр
курсовой проект – 7 семестр

1. Цели и задачи дисциплины

Дисциплина «Создание автоматизированных систем в защищенном исполнении» имеет **целью** изучение основных понятий, методологии и практических приемов проектирования, разработки и внедрения автоматизированных систем на предприятиях различных отраслей промышленности с учетом требований по обеспечению информационной безопасности.

Задачами дисциплины являются:

- формирование у обучаемых целостного представления о содержании и организации процессов проектирования, разработки, внедрения и эксплуатации автоматизированных систем (АС) в защищенном исполнении.
- приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации методов, процессов, инструментов и средств защиты автоматизированных систем;

2. Место дисциплины в структуре ООП ВО

Курс «Создание автоматизированных систем в защищенном исполнении»относится к дисциплинам вариативной части профессионального цикла учебного плана и читается студентам в первом семестре последнего (четвертого) года обучения. Данная дисциплина опирается на знания, полученные студентами ранеепри изучении курсовпрофессионального цикла, таких как «Безопасность операционных систем», «Безопасность систем баз данных», «Основы информационной безопасности», «Техническая защита информации», «Организация ЭВМ и вычислительных систем», «Криптографические методы защиты информации», «Сети и системы передачи информации», «Организационное и правовое обеспечение информационной безопасности»

3. Требования к результатам освоения дисциплины

В результате изучения дисциплины студент должен обладать следующими компетенциями:

- **ПК-5** - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;
- **ПК-7** - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;
- **ПК-8** - способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

- **ПСК-4.1** - способность применять нормативные правовые акты и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении.

Студент должен знать:
- основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении;
- общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем;
- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;

Студент должен уметь:
- разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;
- формировать требования к подсистемам информационной безопасности автоматизированных систем различных типов;
- осуществлять подбор и комплексирование средств защиты для автоматизированных систем в защищенном исполнении;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;
- контролировать эффективность проектирования, разработки и внедрения автоматизированных систем;

Студент должен владеть:
- навыками разработки моделей угроз и моделей нарушителей;
- методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;
- навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
- навыками участия в экспертизе состояния защищенности информации на объекте защиты.