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.1.1.29 «Разработка и эксплуатация защищенных 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 – 4
часов в неделю – 2
всего часов – 144,
в том числе:
лекции – 18
лабораторные занятия – 36
самостоятельная работа – 90
экзамен – 7 семестр
зачет – 7 семестр

1. Цели и задачи дисциплины

Целью изучения дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» является: приобрести теоретические знания и навыки работы, необходимые для разработки и эксплуатации автоматизированных систем, информационные ресурсы которых содержат конфиденциальную информация.

Задачами курса является изучение:

- основных информационных технологий, используемых в автоматизированных системах;
- основных средств и способов обеспечения информационной безопасности, принципы построения систем защиты информации;
- автоматизированной системы как объекта информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
- методов, способов, средств, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
- содержание и порядок деятельности персонала по эксплуатации защищенныхавтоматизированных систем и подсистем безопасности автоматизированных систем;
- методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;
- основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);
- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;
- основные методы управления информационной безопасностью;
- методы аттестации уровня защищенности автоматизированных систем.
- методами формирования требований по защите информации; приобретение навыков работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; выявление угроз информационной безопасности автоматизированных систем.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» относится к вариативной части цикла профессиональных дисциплин по направлению (10.05.03) 090303.65 "Информационная безопасность автоматизированных систем".

В результате изучения дисциплины 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;

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;

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.

Дисциплина изучается в 7 семестре. Знания, умения и навыки, полученные в результате данной дисциплины, используются для выполнения выпускных квалификационных работ.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

- способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3);
- способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4);
- способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-5);
- способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6);
- способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий(ПК-7);
- способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9);
- способностью участвовать в разработке подсистемы управления информационной безопасностью (ПК-12);
- способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности (ПК-13);
- способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности (ПК-14);
- способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-18);
- способностью применять методы анализа изучаемых явлений, процессов и проектных решений (ПК-20);
- способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-21);
- способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-24);
- способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПК-25);
- способностью обеспечить восстановление работоспособности систем защитыинформации при возникновении нештатных ситуаций (ПК-40).