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.1.3.8.1 Обеспечение информационной безопасности организаций банковской системы»

специальности подготовки
10.05.03 "Информационная безопасность автоматизированных систем"
Специализация №9 "Создание автоматизированных систем в защищенном исполнении"

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 2
часов в неделю – 2
всего часов – 72,
в том числе:
лекции – 16
практические занятия – 16
самостоятельная работа – 40
зачет – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: обучение студентов основам проектирования, построения и анализа защищенных банковских систем, принципам и методам защиты информации в банковских сетях, а также содействие фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Задачи изучения дисциплины:

- изучение архитектуры защищенных банковских систем;
- изучение программно-аппаратных и технических средств создания защищенных банковских систем;
- изучение основных методов и программных инструментов, используемых для обеспечения информационной защищённости банковских систем;
- изучение правил организационной, технической и правовой защиты банковских систем;
- знакомство с методологией обследования и анализа защищенности банковских систем;
- получение базовых знаний и практических навыков по поиску и анализу уязвимостей банковских систем.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Обеспечение информационной безопасности организаций банковской системы» относится к числу дисциплин по выбору блока С.1.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – знать формы и способы представления данных в персональном компьютере, типовые структуры и принципы организации компьютерных сетей;

«Языки программирования» – знать язык программирования высокого уровня (объектно-ориентированное программирование), уметь работать с интегрированной средой разработки программного обеспечения, владеть навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;

«Основы информационной безопасности» – знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих, источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, владеть профессиональной терминологией в области информационной безопасности;

«Сети и системы передачи информации» – знать основные характеристики сигналов электросвязи, спектры и виды модуляции, принципы построения и функционирования систем и сетей передачи информации, способы кодирования информации, основные телекоммуникационные протоколы.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

- способность применять нормативные правовые акты в профессиональной деятельности (ОПК-6);
- способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);
- способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27).

Студент должен знать:

- методологические и технологические основы обеспечения информационной безопасности банковских систем;
- угрозы и методы нарушения информационной безопасности банковских систем;
- типовые модели атак, направленных на преодоление защиты банковских систем, условия их осуществимости, возможные последствия, способы предотвращения;
- роль человеческого фактора в обеспечении безопасности банковских систем;
- возможности, способы и правила применения основных программных и аппаратных средств защиты банковских систем;
- принципы функционирования основных сетевых протоколов (HTTP, SSL, TLS);
- основы применения межсетевых экранов для защиты банковских систем;
- методы создания защищённых банковских систем.

Студент должен уметь:

- проводить анализ банковских систем с точки зрения обеспечения информационной безопасности;
- разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы;
- применять защищенные протоколы и межсетевые экраны, необходимые для реализации систем защиты банковских систем;

- реализовывать меры противодействия выявленным угрозам безопасности банковских систем с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения;
- реализовывать системы защиты банковских систем в соответствии со стандартами Банка России.

Студент должен владеть:

- навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, веб-серверов с учетом требований по обеспечению информационной безопасности;
- навыками проектирования защищенных банковских систем;
- навыками комплексного анализа защищенности банковских систем.