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.1.3.12.1 Информационная безопасность Интернет-приложений»

направления подготовки
10.03.01 "Информационная безопасность"
Профиль "Безопасность автоматизированных систем"

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 4
часов в неделю – 7
всего часов – 144,
в том числе:
лекции – 36
коллоквиумы – 8
практические занятия – 33
самостоятельная работа – 67
экзамен – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: обучение студентов основам обеспечения информационной защищённости Интернет-приложений, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных веб-сайтов, а также содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Задачи изучения дисциплины:

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

2. Место дисциплины в структуре ООП ВО

Дисциплина «Информационная безопасность Интернет-приложений» относится к числу дисциплин по выбору.

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 определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).

Студент должен знать:

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

Студент должен уметь:

- проводить анализ Интернет-приложений 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 Интернет-приложений;

- реализовывать меры противодействия выявленным угрозам безопасности Интернет-приложений с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения;
- составлять комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;
- реализовывать системы защиты Интернет-приложений в соответствии со стандартами по оценке защищенных систем.

Студент должен владеть:

- навыками работы с нормативно-правовыми актами и методическими документами;
- 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 Интернет-приложений;
- навыками комплексного анализа защищенности Интернет-приложений;
- методами организации и управления деятельностью служб защиты информации на предприятии.