ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
10.05.03 – Информационная безопасность автоматизированных систем

Аннотация рабочей программы дисциплины «Моделирование угроз информационной безопасности»

Общая трудоемкость дисциплины составляет 6 зач. единиц, 216 часов, форма промежуточной аттестации – экзамен.

Программой дисциплины предусмотрены следующие виды занятий: лекционные – 54 часа, практические – 18 часов, лабораторные – 36 часов, самостоятельная работа обучающегося составляет 108 часов.

Дисциплина подразумевает изучение следующих основных разделов:

Понятие угрозы информационной безопасности. Содержание модели угроз безопасности информации и модели нарушителя. Способы и подходы в моделировании угроз информационной безопасности.

Методики построения защищенных программных продуктов в различных системах программирования с использованием различных технологий, языков и средств создания программ.

Понятие скрипт-вирусов. Деструктивные воздействия в распределённых вычислительных системах (РВС). Классификация. Моделирование поведения. Угрозы атак на UNIX-системы.

Типовые угрозы безопасности РВС. Модели механизмов реализации типовых угроз безопасности РВС.

Моделирование атак на беспроводные сети. Угрозы в wi-fi сетях. Угрозы, направленные на взлом криптографических протоколов. Моделирование атак на криптографические протоколы. Атаки на протокол WEP.

Выявление уязвимостей в корпоративных информационных системах: искусство фаззинга.