

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

ФД.2 «Разработка безопасных мобильных приложений для OS Android»

направления подготовки

10.03.01 "Информационная безопасность"

Профиль "Безопасность автоматизированных систем"

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 2
часов в неделю – 2
всего часов – 72,
в том числе:
лекции – 16
коллоквиумы – 2
лабораторные занятия – 18
самостоятельная работа – 36
зачет – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: изучение вопросов обеспечения информационной безопасности, возникающих при использовании мобильных устройств, а также основ разработки защищенных мобильных приложений для OS Android.

Задачи изучения дисциплины:

- формирование у обучаемых целостного представления о комплексном подходе к обеспечению безопасности при использовании в информационной системе мобильных устройств;
- приобретение обучаемыми необходимого объема знаний и практических навыков в области разработки, распространения и эксплуатации защищенных мобильных приложений для OS Android.

2. Место дисциплины в структуре ООП ВО

Для успешного усвоения дисциплины «Разработка безопасных мобильных приложений для OS Android» 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 следующей компетенции:

- способностью использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-16).

Студент должен знать:

- процедуру формирования цифровой подписи кода приложения, необходимой для доступа и использования различных функций безопасности мобильных устройств Android;
- правила, процедуры, практические приемы для управления информационной безопасностью.

Студент должен уметь:

- разрабатывать модели угроз и нарушителей информационной безопасности в процессе разработки, распространения и эксплуатации защищенных мобильных приложений;
- рационально выбирать методы и средства для реализации процессов разработки, распространения и эксплуатации защищенных мобильных приложений;
- составлять комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

Студент должен владеть:

- навыками в области разработки, распространения и эксплуатации защищенных мобильных приложений для OS Android;
- методами организации и управления деятельностью служб защиты информации на предприятии.