Приложение 1
к рабочей программе дисциплины
«Методы и средства защиты информации»

Аннотация рабочей программы

Дисциплина «Методы и средства защиты информации» является частью вариативного блока дисциплин учебного плана подготовки бакалавров по направлению подготовки 220400.62 «Управление в технических системах». Дисциплина реализуется на факультете автоматики и информационных технологий ФГБОУ ВПО «Самарский государственный технический университет» кафедрой «Автоматики и управления в технических системах».

Цели и задачи дисциплины: Целью освоения дисциплины «Методы и средства защиты информации» является формирование общекультурных и профессиональных компетенций, необходимых для реализации проектно-конструкторской и научно-исследовательской деятельности:

способность находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-4);

способность использовать нормативные правовые документы в своей деятельности (ОК-5);

способность разрабатывать информационное обеспечение систем с использованием стандартных СУБД (ПК-11);

готовность производить инсталляцию и настройку системного, прикладного и инструментального программного обеспечения систем автоматизации и управления (ПК-31).

Задачами изучения дисциплины являются приобретение знаний и умений и формирование навыков, способствующих формированию целевых компетенций.

Требования к уровню освоения содержания дисциплины:

В результате изучения дисциплины студент должен приобрести:

- **знания** о базовых понятиях в области информационной безопасности; современной ситуации в области информационной безопасности; основных законах в сфере информационной безопасности; об алгоритмах шифрования и дешифрования; криптосистемах, криптологических стандартах и протоколах; основах аутентификации и безопасности в компьютерных сетях;
- **умения** формулировать базовые понятия в области информационной безопасности и криптологии; классифицировать алгоритмы шифрования; выполнять шифрование и дешифрование данных; выбирать тот или иной алгоритм шифрования в зависимости от предъявляемых требований к шифрованию; генерировать устойчивые к взлому пароли;
- **навыки** криптоанализа классических шифров; использования программного обеспечения для шифрования и дешифрования; сокрытия передаваемой информации в графических файлах.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельную работу студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме проверки отчетов по лабораторным работам; рубежный контроль в форме тестирования; промежуточный контроль в форме устного экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Программой дисциплины предусмотрены лекционные (17 часов), лабораторные (51 час) занятия и 40 часов самостоятельной работы студента.