

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

09.03.04 Программная инженерия

Аннотация рабочей программы

дисциплины «Основы информационной безопасности»

Общая трудоемкость дисциплины составляет 2 зач. единицы, 72 часа, форма промежуточной аттестации – *зачет*.

Программой дисциплины предусмотрены лекционные (17 часов), лабораторные занятия (17 часов), самостоятельная работа обучающегося составляет 28 часов.

Учебным планом предусмотрено 1 ИДЗ.

Дисциплина предусматривает изучение следующих основных разделов:

Понятие национальной безопасности, виды безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации.

Терминологические основы информационной безопасности. Основные понятия и определения. Конфиденциальность, целостность, доступность.

Общеметодологические принципы теории информационной безопасности. Комплексность. Этапы развития информационной безопасности: Системы безопасности ресурса; Этап развитой защиты; Этап комплексной защиты. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Комплексность: целевая, инструментальная, структурная, функциональная, временная.

Угрозы. Классификация и анализ угроз информационной безопасности. подверженность физическому искажению или уничтожению; возможность несанкционированной (случайной или злоумышленной) модификации; опасность несанкционированного получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные.

Методы и средства обеспечения информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации. Причины нарушения целостности информации: субъективные преднамеренные,

субъективные непреднамеренные, объективные непреднамеренные. Потенциально возможные злоумышленные действий в автоматизированных системах обработки данных.

Функции и задачи защиты информации. Методы формирования функций защиты. Скрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Легендирование. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека. Применение криптографии.