АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

ТЕОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ

(название дисциплины)

10.03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(код направления (специальности) подготовки)

5

(семестр)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- Целями освоения дисциплины «Теория защиты информации» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность», ознакомление студентов с вопросами сущности и значения информационной безопасности и защиты информации, определение теоретических, концептуальных, методологических и организационных основ обеспечения информационной безопасности в компьютерных системах. Изучение основных моделей каналов утечки в компьютерных системах и моделей управления доступом в компьютерных системах.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

- Данная дисциплина относится к базовой части Блока Б1 (Б1.Б.21). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и практических занятий.
- Дисциплина изучается на 3 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по направлению 10.03.01 «Информационная безопасность» по курсам «Информатика», «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Структуры данных», «Технологии и методы программирования». Курс тесно взаимосвязан с другими дисциплинами. Он является базовым для изучения таких дисциплин как «Защита информации в корпоративных ИС», «Программно-аппаратные средства защиты информации», «Базы данных», «Система защиты информации на предприятии», «Корпоративные информационные системы» и т.д.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины бакалавр должен обладать следующими общекультурными и профессиональными способностями:

- ОК-5 – способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;
- ОПК-7 – способностью 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.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

- Введение. Основные понятия и определения, в построении формальных моделей контроля доступа
- Понятие об угрозах конфиденциальности, целостности и доступности в терминах управления доступом. Базовая теорема безопасности
- Дискреционное, мандатное и ролевое управление доступом. Ключевые особенности, специфика реализации
- Модель Харрисона-Руззо-Ульмана. Элементарные операторы модели. Принцип построения команд в модели ХРУ.
- Модель матрицы доступов. Монотонная ТМД и ее каноническая форма. Способы формирования команд в модели ТМД.
- Классическая модель take-grant. Де-юре правила модели. Понятие о tg-связном подграфе, теорема о пролиферации права внутри tg-связного подграфа.
- Расширенная модель take-grant. Де-факто правила расширенной модели.
- Модель мандатного управления доступом Белла-ЛаПадулы. Правила NRU и NWD. Политика low-watermark в модели
- Модель мандатного управления целостностью Биба. Угрозы целостности, решетка уровней целостности. Правила NRD и NWU.
- Модель системы военных сообщений (СВС). Общие положения. Терминалы и устройства доступа в модели

СВС.

- Модели безопасности информационных потоков. Автоматная и программная модели контроля информационных потоков.
- Вероятностная модель контроля информационных потоков. Схема компьютерной системы в рамках понятийного аппарата этой модели.
- Понятие ролевого разграничения доступа. Ролевые модели доступа в СУБД.
- Основные положения модели администрирования РРД. Администрирование множеств авторизованных ролей пользователей.
- Модель мандатного РРД. Управление правами ролей в случае наличия решетки конфиденциальности. Связь между дискреционным и мандатным РРД.
- Субъектно-ориентированная модель безопасности программной среды. Изолированная программная среда.
- Проблемы применения моделей безопасности при построении информационных систем в защищенном исполнении. Проблема адекватности модели безопасности реальной компьютерной системе.
- Реализация дискреционной политики в операционных системах Windows и GNU/Linux. Реализация дискреционного управления доступом в СЗИ.

Составитель: доцент кафедры ИЗИ к.т.н. Тельный А.В.
должность, ФИО, подпись

Заведующий кафедрой ИЗИ М.Ю. Монахов
ФИО, подпись

Директор института ИТР А.А. Галкин
ФИО, подпись

Дата, Печать института (факультета)