АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Модели безопасности компьютерных систем

по специальности 10.05.03 информационная безопасность автоматизированных систем

1. Цели и задачи освоения дисциплины

Целью **дисциплины** «Модели безопасности компьютерных систем» является обучение студентов принципам формального моделирования и анализа безопасности компьютерных систем, реализующих управление доступом и информационными потоками.

Задачи освоения дисциплины:

развитие у студентов соответствующих профессиональных компетенций;

изучение основных формальных моделей политик безопасности, моделей дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков;

приобретение практических навыков разработки математических моделей безопасности для защищаемых компьютерных систем;

формирование у будущего специалиста в области компьютерной безопасности таких качеств, как строгость в суждениях, творческое мышление, организованность и работоспособность, дисциплинированность, самостоятельность и ответственность.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП:

Дисциплина «Модели безопасности компьютерных систем» относится к числу вариативных дисциплин блока Б1 программы подготовки специалистов по специальности 10.05.03 – «Информационная безопасность автоматизированных систем».

Дисциплина читается в 8-ом семестре студентам очной формы обучения. Для ее успешного изучения необходимы знания и умения, приобретенные в следующих предшествующих учебных дисциплинах: Алгебра и геометрия, Безопасность операционных систем, Безопасность систем баз данных, Вычислительные методы в алгебре и теории чисел, Дискретная математика, Дифференциальные уравнения, Криптографические методы защиты информации, Математическая логика и теория алгоритмов, Математический анализ, Методы принятия оптимальных решений, Организационное и правовое обеспечение информационной безопасности, Основы научных исследований, Открытые информационные системы, Сети и системы передачи информации, Теория вероятностей и математическая статистика, Технологии и методы программирования.

Результаты освоения дисциплины «Модели безопасности компьютерных систем» будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: Администрирование сетей ЭВМ, Безопасность открытых информационных систем, Разработка и эксплуатация автоматизированных систем в защищённом исполнении, а также при прохождении практик и выполнении НИР.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ПК-3 - Способен разрабатывать проектные решения по защите информации в автоматизированных системах	**Знать:** Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем Принципы формирования политики информационной безопасности в автоматизированных системах **Уметь:** Применять действующую нормативную базу в области обеспечения защиты информации Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе **Владеть:** Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах
ПК-6 - Способен проводить контроль защищенности информации от НСД	**Знать:** Методы защиты информации от несанкционированного доступа и специальных программных воздействий на нее Методы и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий **Уметь:** Проводить оценку защищенности информации от несанкционированного доступа и специальных воздействий Проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации **Владеть:** Навыками проведения контроля защищенности информации от несанкционированного доступа и специальных воздействий

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часа)

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;
- проведение лабораторных занятий;
- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение зачета.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к лабораторным работам, их оформление.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля:
Подготовка ответов на вопросы по темам при выполнении лабораторных работ.
Промежуточная аттестация проводится в форме зачета.