АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Модели безопасности компьютерных систем

по специальности 10.05.01 компьютерная безопасность

1. Цели и задачи освоения дисциплины

Цель освоения дисциплины: обучение студентов принципам формального моделирования и анализа безопасности компьютерных систем, реализующих управление доступом и информационными потоками.

Задачи освоения дисциплины:

- развитие у студентов соответствующих общекультурных, профессиональных и профессионально-специализированных 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 ВО

Дисциплина «Модели безопасности компьютерных систем» относится к числу дисциплин блока Б1.Б программы подготовки специалистов по направлению 10.05.01 – «Компьютерная безопасность». Дисциплина читается в 8 и 9-ом семестре студентам очной формы обучения.

3. Требования к результатам освоения дисциплины

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
ОПК-9 способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными	**Знать:** формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации **Уметь:** разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации

потоками в компьютерных системах с учетом угроз безопасности информации	**Владеть:** навыками разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации
ПК-1 способностью осуществлять подбор, изучение и обобщение научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности	**Знать:** правовой и методический материал отечественного и зарубежного опыта по проблемам компьютерной безопасности **Уметь:** осуществлять подбор, обобщение научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности **Владеть:** навыками осуществлять подбор, изучение и обобщение научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности
ПК-2 способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	**Уметь:** составлять научные отчеты, обзоры по результатам выполнения исследований **Владеть:** навыками участия в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований
ПК-4 способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	**Знать:** Математические модели безопасности компьютерных систем **Уметь:** проводить анализ математических моделей безопасности компьютерных систем **Владеть:** навыками разработки математических моделей безопасности компьютерных систем
ПК-8 способностью участвовать в разработке подсистемы информационной безопасности	**Знать:** требования к разработке подсистемы информационной безопасности компьютерной системы **Уметь:** разрабатывать подсистемы информационной безопасности компьютерной системы **Владеть:**

компьютерной системы	навыками разработки подсистемы информационной безопасности компьютерной системы

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов)

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;
- проведение экзамена.

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 и экзамена.