

Аннотация к рабочей программе дисциплины «Модели безопасности компьютерных систем»

Рабочая программа учебной дисциплины «Модели безопасности компьютерных систем» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.12.04.

Общая трудоемкость освоения дисциплины составляет 144 часов (4 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (18 часов), практические занятия (18 часов), самостоятельная работа студента (72 час.). Дисциплина реализуется на 2 курсе в 4 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина логически и содержательно связана с такими курсами, как «Информатика», «Математическая логика и теория алгоритмов», «Дискретная математика», «Основы информационной безопасности»

Дисциплина имеет теоретическую направленность, при этом большое значение для освоения дисциплины имеют, как лекционные, так и практические занятия. В ходе реализации дисциплины в рамках лекционных и практических занятий применяются методы активного/ интерактивного обучения, реализующие наглядное представление результатов анализа моделей. Данная дисциплина затрагивает такие вопросы, как классификация современных компьютерных систем, основные понятия математической логики и теории алгоритмов, источники и классификация угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, защитные механизмы и средства обеспечения безопасности операционных систем.

Цель курса – обучение специалистов принципам построения формальных моделей политик безопасности, политик управления доступом и

информационными потоками, методам анализа математических моделей защищаемых систем и систем обеспечения информационной безопасности КС.

Задачи:

- изучение основных угроз безопасности информации и модели нарушителя в КС.
- изучить основные виды политик управления доступом и информационными потоками в КС.
- изучить основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.
- научить разрабатывать модели угроз и модели нарушителя безопасности КС.
- научить разрабатывать частные политики безопасности КС, в том числе политики управления доступом и информационными потоками.

Для успешного изучения дисциплины «Модели безопасности компьютерных систем» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);
- способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);
- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над

междисциплинарными и инновационными проектами (ОПК-4);

- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);

- способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8).

В результате изучения дисциплины у обучающихся формируются следующие профессиональные и профессионально-специализированные компетенции.

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-7) способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах. основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
	Умеет	осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем
	Владеет	навыком формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем
(ОПК-9) способность разрабатывать формальные модели политик безопасности,	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах;

политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации		основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
	Умеет	использовать основные виды политик управления доступом и информационными потоками в компьютерных системах; использовать основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
	Владеет	методами разработки частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
(ПК-4) способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знает	математические основы моделей безопасности. основы постановки научной задачи, определения гипотезы и методов исследования безопасности компьютерных систем
	Умеет	построить формальную модель системы, соответствующую заданной политике безопасности. научно и теоретически обосновано излагать результаты исследований безопасности компьютерных систем
	Владеет	методами анализа безопасности компьютерных систем с использованием формальных моделей безопасности. методиками исследований в области безопасности компьютерных систем

Для формирования вышеуказанных компетенций в рамках дисциплины «Модели безопасности компьютерных систем» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: конспект (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6).