Аннотация к рабочей программы дисциплины

Б1.В.ДВ.03.02«Математические методы защиты информации»

Объем трудоемкости: __2_ зачетных единиц
Цель дисциплины:

Курс посвящен изучению современных концепций информационной безопасности и их применения в обеспечении защиты информации и безопасного использования программных средств в вычислительных системах. Цель курса – научить студента методам информационной безопасности и их использовании в области защиты информации. Задачей курса является изложение теории информационной безопасности и практики применения алгоритмов криптозащиты.

Воспитательной целью дисциплины является формирование у студентов научного, творческого подхода к освоению технологий, методов и средств производства и защиты программного обеспечения. Дать студентам математические основы защиты информации.

Отбор материала основывается на необходимости ознакомить студентов со следующей современной научной информацией:

методы защиты информации;

области применения защиты информации;

о технологиях анализа шифров.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

Студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие программе дисциплины.

Студент в рамках курса должен знать области применения задач информационной безопасности; методы защиты информации; области применения различных методов информационной безопасности; этапы, методы и инструментальные средства информационной безопасности. принципы построения и функционирования систем информационной безопасности; классификацию шифров; основы организации идентификации и цифровой подписи; принципы построения и применения паролей; уметь проводить анализ и определять оптимальный метод защиты информации; формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; формулировать и решать задачи организации процесса цифровой подписи; формулировать и решать задачи организации процесса идентификации; реализовать на языке программирования заданный метод защиты информации; решать задачи анализа шифра.

Задачи дисциплины

Основные задачи курса на основе системного подхода:

- Описать проблемную область информационной безопасности.
- Дать описание практического применения теории конечных полей в теории защиты информации.
- Расширить понятия о генерации псевдослучайных последовательностях.
- Расширить понятия о способах защиты информации.
- Расширить понятия о методах построения современных программных систем.
- Дать навыки практической работы с методами защиты информации.
- Дать навыки практической работы по решению задач идентификации.
- Дать навыки практической работы по решению задач цифровой подписи.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

Место дисциплины в структуре образовательной программы

Дисциплина «Математические методы защиты информации» относится к «Часть, формируемая участниками образовательных отношений» Блока 1 «Дисциплины (модули)» учебного плана.

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

ПК-4 **Способен активно участвовать в разработке системного и прикладного программного обеспечения**

ИД-1.ПК-4 ***Проводит классификацию и осуществляет выбор современных инструментальных средств разработки прикладного программного обеспечения вычислительных средств и систем различного функционального назначения, с учетом тенденций развития функций и архитектур в соответствующих проблемно-ориентированных систем и комплексов***

Знать *Принципы построения архитектуры программного обеспечения и виды архитектуры программного обеспечения*

Типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения

Методы и средства проектирования программного обеспечения

Методы и средства проектирования программных интерфейсов

Архитектура, устройство и функционирование вычислительных систем

Сетевые протоколы

Возможности ИС, предметная область автоматизации

Управление рисками проекта

Возможности ИС

Уметь *Использовать существующие типовые решения и шаблоны проектирования программного обеспечения*

Применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов

Планировать работы в проектах в области ИТ

Применять методы проведения экспериментов

Владеть *Разработка, изменение и согласование архитектуры программного обеспечения с системным аналитиком и архитектором программного обеспечения*

Проектирование структур данных

Проектирование программных интерфейсов

Качественный анализ рисков в проектах в области ИТ

Внедрение результатов исследований и разработок в соответствии с установленными полномочиями

ИД-2.ПК-4 ***Реализует приемы работы с современными инструментальными средствами, поддерживающими создание программных проблемно-ориентированных продуктов***

Знать *Возможности современных и перспективных средств разработки программных продуктов, технических средств*

Современные структурные языки программирования

Принципы построения архитектуры программного обеспечения и виды архитектуры программного обеспечения

Типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения

Методы и средства проектирования программного обеспечения

Методы и средства проектирования программных интерфейсов

Уметь *Использовать существующие типовые решения и шаблоны проектирования программного обеспечения*

Применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов

Использовать существующие типовые решения и шаблоны проектирования программного обеспечения

Применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов

Владеть *Устранение обнаруженных несоответствий*

Внедрение результатов исследований и разработок в соответствии с установленными полномочиями

Проектирование структур данных

Проектирование программных интерфейсов

ПК-5 Способен применять основные алгоритмические и программные решения в области информационно-коммуникационных технологий, а также участвовать в их разработке

ИД-1.ПК-5 ***Демонстрирует способность анализа предметной области и требований к информационной системе с использованием основных концептуальных положений функционального, логического, объектно-ориентированного и визуального направлений программирования***

Знать *Типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения*

Методы и средства проектирования программного обеспечения

Методы и средства проектирования баз данных

Основы системного администрирования

Архитектура, устройство и функционирование вычислительных систем

Сетевые протоколы

Основы современных операционных систем

Основы современных систем управления базами данных

Современный отечественный и зарубежный опыт в профессиональной деятельности

Уметь *Использовать существующие типовые решения и шаблоны проектирования программного обеспечения*

Применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов

Анализировать входные данные

Владеть *Проектирование структур данных*

ИД-2.ПК-5 ***Определяет элементы проблемной области и их взаимодействие, архитектуру программной системы, ее функциональные возможности и логику работы с использованием основных концептуальных положений функционального, логического, объектно-ориентированного и визуального направлений программирования***

Знать *Типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения*

Методы и средства проектирования программного обеспечения

Методы и средства проектирования баз данных

Методы и средства проектирования программных интерфейсов

Основы системного администрирования

Основы администрирования СУБД

Архитектура, устройство и функционирование вычислительных систем

Сетевые протоколы

Основы современных операционных систем

Основы современных систем управления базами данных

Современный отечественный и зарубежный опыт в профессиональной деятельности

Уметь *Использовать существующие типовые решения и шаблоны проектирования программного обеспечения*

Применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов

Устанавливать программное обеспечение

Анализировать входные данные

Владеть *Проектирование структур данных*

Проектирование баз данных

Проектирование программных интерфейсов

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) дисциплины, изучаемые в 7 семестре

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Базовые понятия и история развития информационной безопасности.	**8**			4	4

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
2.	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	**10**			6	4
3.	Шифры замены. Шифры перестановки. Шифры гаммирования.	**8**			4	4
4.	Блочные системы шифрования.	**12**			6	6
5.	Поточные системы шифрования.	**14**			8	6
6.	Идентификация. Цифровые подписи.	**19,8**			6	13,8
ИТОГО по разделам дисциплины		**69,8**			**34**	**37,8**
Контроль самостоятельной работы (КСР)						
Промежуточная аттестация (ИКР)		0,2				
Подготовка к текущему контролю						
Общая трудоемкость по дисциплине		**72**				

Курсовые работы: *не предусмотрена*
Форма проведения аттестации по дисциплине: *зачет*

Автор В.В. Подколзин