АННОТАЦИЯ рабочей программы дисциплины
Б1.О.33«Защита информации»

Направление подготовки/специальность 02.03.03 Математическое обеспечение и администрирование информационных систем

Объем трудоемкости: 4 зач.ед.

Цель дисциплины:

Основной целью дисциплины является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств и коммуникаций.

При освоении дисциплины предусмотрены лекции и самостоятельная работа.

На лекциях рассматриваются методологические основы информационной безопасности, типовые угрозы и уязвимости, правовое регулирование и организационное обеспечение защиты информации, формирование требований для проектирования систем защиты информации, акцентируется внимание на безопасности в информационных системах персональных данных, государственных информационных системах и на объектах критической информационной инфраструктуры. Изучаются базовые криптографические методы, принципы и свойства дискреционных, мандатных и ролевых систем управления доступом в компьютерных системах. Даётся обзор стандартов информационной безопасности, классов защищённости, профилей защиты и оценочных уровней доверия. Обсуждаются угрозы информационной безопасности при разработке программного обеспечения, понятие не декларированных возможностей, принципы безопасного программирования, процесс создания защищённых информационных систем.

Самостоятельная работа включает: изучение учебного и информационного материала по тематике дисциплины, подготовку докладов, презентаций и отчётных работ по результатам самостоятельной домашней работы, подготовку к текущей и промежуточной аттестации.

Воспитательной целью дисциплины является формирование у студентов научного, творческого подхода к освоению информационных технологий.

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

о технологии разработки программного обеспечения для мобильных устройств;

о парадигмах визуального программирования (императивной, функциональной, логической, объектно-ориентированной);

о технологиях программирования (структурной, модульной, объектно-ориентированной, объектно-ориентированной).

Содержательное наполнение дисциплины обусловлено общими задачами подготовки бакалавра.

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

Задачи дисциплины:

Основными задачами изучения дисциплины являются:

– систематизация, формализация и расширение знаний по основным положениям защиты информации, криптографии и информационной безопасности;

– обучение студентов приемам работы с современным программным обеспечением для практического освоения принципов и методов обеспечения информационной безопасности;

– формирование комплексных знаний об основных тенденциях развития технологий, связанных с обеспечением информационной безопасности;

– формирование практических навыков применения средств защиты информации при решении профессиональных задач.

Место дисциплины в структуре ООП ВО

Дисциплина «Защита информации» относится к «Обязательная часть» Блока 1 «Дисциплины (модули)» учебного плана.

Дисциплина «Защита информации» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: Информатика, Программирование, Дискретная математика, Математическая логика и теория алгоритмов, Основы теории кодирования. Дисциплина «Защита информации» является базовой для прохождения производственной практики и написания выпускной квалификационной работы. Дисциплина «Защита информации» реализуется в 8 семестре в рамках базовой части дисциплин (модулей) Блока 1 и является обязательной дисциплиной.

Требования к уровню освоения дисциплины

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

Дисциплина «Защита информации» направлена на формирование компетенций:

ОК-4 - способность использовать основы правовых знаний в различных сферах деятельности, в части следующих результатов обучения;

ОК-4.2 уметь использовать нормативно-правовые знания в различных сферах практической деятельности;

ОПК-2 - способность осваивать методики использования программных средств для решения практических задач, в части следующих результатов обучения;

ОПК-2.1 способен на основе знания основных функций и возможностей программного обеспечения проектировать и разрабатывать программные средства для решения практических задач в соответствии с техническим заданием;

ОПК-2.2 уметь обосновывать выбор программного обеспечения и разрабатывать концептуальную и логическую модель данных;

ОПК-5 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности, в части следующих результатов обучения;

ОПК-5.3 знать основные требования информационной безопасности при решении стандартных задач профессиональной деятельности;

ПК-3 - способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности, в части следующих результатов обучения;

ПК-3.1 проводить эксперименты по заданной методике и анализировать результаты.

Основные разделы дисциплины:

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Информация и неопределённость. Численная мера неопределённости	2	2			
2.	Алгебраическая система **<A, F, R>** с заданными отношениями	3	3			
3.	Общая схема передачи, хранения и защиты информации. Кодирование информации.	2	2			

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
4.	Линейное кодирование. Свойства и способы задания линейных кодов	3	3			
5.	Основные решаемые проблемы криптографией и криптологией. Криптостойкость шифра. Принцип Керкхоффса	3	3			
6.	Математическое моделирование систем защиты информации (ВОО_СЗИ)	2	2			
7.	Методы моноалфавитных (многоалфавитных) подстановок и перестановок Применение логических функций в криптографии. Хеш-функции	3	2			
8.	Современные методы решения проблемы передачи ключей. Алгоритм генерации ключа для цифровой подписи	3	3			
9.	Аддитивная группа точек эллиптической кривой	4	2			
10.	Рюкзачная криптосистема на основе кода Варшамова	3	3			
11.	Системы ЭЦП. Установление подлинности и целостности данных	3	3			
12.	Диофантовы уравнения. Десятая проблема Гильберта. ДБК	4	3			

Курсовые работы: не предусмотрена

Форма проведения аттестации по дисциплине: зачёт

Автор Осипян В. О. проф., д. физ.-мат. наук, доцент