Аннотация к рабочей программе дисциплины
«Программно-аппаратные средства защиты информации»

Рабочая программа по курсу «Программно-аппаратные средства защиты информации» разработана для студентов по направлению 10.03.01 «Информационная безопасность».

Учебным планом предусмотрены лекционные занятия (36 часов), практические занятия (18 часов), лабораторные работы (18 часов) самостоятельная работа студентов (36 часов). Дисциплина «Дискретная математика» реализуется на 3 курсе в 6 семестре.

Цель: формирование основополагающих знаний по программному и аппаратному обеспечению информационной безопасности в области системного анализа и принятия решений.

Задачи:

- угроз информационной безопасности в автоматизированных системах обработки данных;
- принципов разделения доступа и защиты программ и данных от НСД;
- использования программно-аппаратных средств защиты информации;
- проектирования систем защиты информации в АСОД.
- изучение основных угроз безопасности информации в автоматизированных системах и освоение методов защиты от данных угроз;
- изучение методов, алгоритмов, программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
- изучение основных мер по защите информации и программных продуктов от несанкционированного доступа, модификации и изучения в автоматизированных системах;
- изучение современных технологий защищенных сетей передачи данных в автоматизированных системах.

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции.

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-1) способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает	архитектуру и базовые принципы функционирования вычислительных систем, сетей и современных многозадачных многопользовательских операционных систем
	Умеет	развертывать и настраивать программные и аппаратные средства для защиты локальных и распределенных вычислительных систем
	Владеет	программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах
(ПК-12) способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знает	методы и программно-аппаратные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации
	Умеет	настраивать каналы безопасного обмена информацией в локальных и распределенных автоматизированных системах
	Владеет	программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах
(ПК-15) способностью разрабатывать планы и программы проведения научных исследований и технических разработок	Знает	модульную структуру подсистемы безопасное™ современных операционных систем и способы интеграции средств защиты
	Умеет	настраивать системы обнаружения вторжений и антивирусные системы
	Владеет	программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах
(ОПК-7) способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей	Знает	методы и алгоритмы управления и генерации ключей и их аппаратно-программная реализация и применение в автоматизированных системах
	Умеет	настраивать системы предотвращения вторжений
	Владеет	инструментарием, обеспечивающим программно-аппаратную защиту информационных ресурсов от изучения, модификации и копирований

функционирования объекта защиты		
(ПСК-3.2) способностью формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта и его информационных составляющих, с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объектов и локализации защищаемых элементов	Знает	организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации
	Умеет	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
	Владеет	методами формирования требований по защите информации
(ПСК-3.3) способностью разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, проводить выбор необходимых технологий и технических средств, организовать внедрение и последующее сопровождение	Знает	комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации
	Умеет	проводить выбор необходимых технологий и технических средств, организовать их внедрение
	Владеет	методами формирования требований по защите информации