Аннотация к рабочей программе дисциплины

Автор: Урбан В.А, доцент, канд.техн.наук

Наименование дисциплины: Б1.О.10 Методы и средства криптографической защитыинформации

Цель освоения дисциплины: заключается в формировании у студентов знаний теории и методов защиты информации путем криптографической защиты сообщений, осуществления секретной связи на основе симметричных и асимметричных криптосистем, а также методов реализации электронной (цифровой) подписи; раскрытие возможностей и особенностей криптографии и криптоанализа применительно к задачам проектирования защищенных систем и сетей связи и передачи данных

1. Требования к результатам освоения дисциплины:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине (модулю)**
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1 Применяет математические модели и решать задачи криптографического преобразования при решении задач защиты информации	*Знать:* Основные принципы построения криптоалгоритмов *Уметь:* Строить современные шифрсистемы *Владеть:* Криптографической терминологией
	ОПК-9.2 Определяет и анализирует технические каналы утечки информации	*Знать:* Каналы утечки информации и методы их оценки *Уметь:* Изучать и анализировать характеристики и особенности применения основных приборов и оборудования, используемых для выявления каналов утечки информации *Владеть:* Расчета контролируемой зоны, в пределах которой могут происходить утечки информации
	ОПК-9.3 Проводит работы по установке и настройке средств технической защиты информации	*Знать:* Понятие составляющие и проблемы информационной безопасности *Уметь:* Обосновать и сформулировать решения по применению технологических и нормативно-правовых средств и методов Обеспечения информационной безопасности *Владеть:* Методом дискретного

		логарифмирования в конечных циклических группах
ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;	ОПК-4.3.1 Способен применять основные угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии и типы атак	*Знать:* Объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные и аппаратные средства *Уметь:* Применять криптографические и информационно-аналитические системы, информационные ресурсы и информационные технологии *Владеть:* Методом применения основных криптосистем и систем стенографирования
	ОПК-4.3.2 Выявляет принципы построения подсистем защиты компьютерной информации в операционных системах и в пользовательских программных приложениях	*Знать:* Основные принципы построения подсистем защиты компьютерной информации и в операционных системах и в пользовательских программных приложениях *Уметь:* Планировать программно-аппаратную подсистему политики безопасности организации *Владеть:* Методами защиты информации в операционных системах и в пользовательских приложениях
	ОПК-4.3.3 Способен использовать сертифицированные и перспективные программно-аппаратные средства и методы защиты компьютерной информации (в том числе криптографических)	*Знать:* Виды информации, подлежащей шифрованию *Уметь:* Применять частотные характеристики языков и их использование в криптоанализе *Владеть:* Методами криптоанализа простейших шифров
	ОПК-4.3.4 Выявляет средства и методы защиты от НСД хранимой информации с использованием возможностей	*Знать:* Средства и методы защиты от НСД хранимой информации с использованием возможностей устройств записи и чтения *Уметь:*

	устройств	Использовать криптографические методы при организации работ по защите информации *Владеть:* Навыками использования инструментов криптографической защиты информации

2. Содержание дисциплины:

Тема 1. Классификация криптографических систем
Тема 2. Простыешифры и их свойства
Тема 3. Симметричные системы шифрования(системы шифрования ссекретным ключом)
Тема 4. Системышифрования соткрытым ключом
Тема 5. Поточныесистемы шифрования
Тема 6.Электронно-цифровая подпись
Тема 7. Протоколыидентификации
Тема 8. Протоколыуправления ключами
Тема 9. Современныедостижения науки и техники в областисовременной криптографии

3. Общая трудоемкость дисциплины: 5 ЗЕ