АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Криптографические методы защиты информации»

по специальности 10.05.03 «Информационная безопасность автоматизированных систем»
специализация «Безопасность открытых информационных систем»

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

- приобретение общих представлений о криптографических методах и средствах обеспечения информационной безопасности;
- знакомство с важнейшими криптоалгоритмами, принципами их построения.

Задачи освоения дисциплины:

- освоение основных методов выбора алгоритмов для различных применений и оценки их качества;
- дать основы системного подхода к организации защиты информации; принципов синтеза и анализа шифров;
- дать основы математических методов, используемых в криптоанализе.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к базовой части цикла Б1 образовательной программы и читается в 7-м семестре студентам специальности «Информационная безопасность автоматизированных систем» очной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Математический анализ», «Алгебра и геометрия», «Дискретная математика», «Теория вероятностей и математическая статистика», «Информатика». Предполагается также знакомство с одним из языков программирования высокого уровня (например, C/C++).

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: теоретико-числовые методы в криптографии, вычислительные методы в алгебре и теории чисел.

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих специальных дисциплин: «Криптографические протоколы и стандарты», «Методы алгебраической геометрии в криптографии», а также для прохождения учебной, производственной и преддипломной практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Процесс изучения дисциплины «Криптографические методы защиты информации» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОК-6 – способностью работать в коллективе,	Владеть:

толерантно воспринимая социальные, культурные и иные различия	криптографической терминологией
ОПК-1 – способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач	Уметь: применять математические методы исследования моделей шифров
ОПК-2 – способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	Знать: основные задачи и понятия криптографии; частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки
ОПК-3 – способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	Владеть: навыками использования ЭВМ в анализе простейших шифров
ОПК-5 – способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знать: основные задачи и понятия криптографии
ПК-1 – способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	Владеть: криптографической терминологией
ПК-2 – способностью создавать и исследовать модели автоматизированных систем	Знать: модели шифров и математические методы их исследования Владеть: навыками математического моделирования в криптографии
ПК-3 – способностью проводить анализ защищенности автоматизированных систем	Знать: требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования
ПК-5 – способностью проводить анализ рисков информационной безопасности автоматизированной системы	Знать: требования к шифрам и основные характеристики шифров
ПК-6 – способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Знать: требования к шифрам и основные характеристики шифров
ПК-11 – способностью разрабатывать политику	Знать:

информационной безопасности автоматизированной системы	основные задачи и понятия криптографии
ПК-13 – способностью участвовать в проектировании средств защиты информации автоматизированной системы	Знать: требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры Уметь: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах Владеть: криптографической терминологией
ПК-14 – способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Знать: требования к шифрам и основные характеристики шифров
ПК-15 – способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	Знать: требования к шифрам и основные характеристики шифров
ПК-22 – способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Уметь: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах Владеть: криптографической терминологией
ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Знать: основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры
ПК-26 – способностью администрировать подсистему информационной безопасности автоматизированной системы	Знать: типовые шифры с открытыми ключами;
ПК-27 – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Знать: типовые шифры с открытыми ключами Владеть: навыками использования типовых криптографических алгоритмов; навыками использования ЭВМ в анализе простейших шифров

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часов)

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;
- проведение практических занятий;

- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение экзамена.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к лабораторным работам, их оформление.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: лабораторные работы, проверка решения задач.

Промежуточная аттестация проводится в форме: экзамен.