


|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации<br>Ульяновский государственный университет | Форма |  |
| Ф – Аннотация рабочей программы дисциплины   |       |   |

## 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 обязательной части цикла Б1 образовательной программы и читается в 7-м семестре и 8-м семестрах 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 |
|--|--|
| ОПК-3 – Способен использовать математические методы, необходимые для решения задач | Знать:<br>алгоритмы проверки чисел и многочленов на про-   |

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации<br>Ульяновский государственный университет | Форма |  |
| Ф – Аннотация рабочей программы дисциплины   |       |   |

|  |  |
|--|--|
| профессиональной деятельности  | <p>стоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах;</p> <p>Уметь:</p> <p>проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ;</p> <p>Владеть:</p> <p>навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.</p>   |
| ОПК-9 – Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации | <p>Знать:</p> <p>основные задачи, решаемые криптографическими методами;</p> <p>математические модели шифров, подходы к оценке их стойкости;</p> <p>зарубежные и российские криптографические стандарты;</p> <p>основные виды симметричных и асимметричных криптографических алгоритмов;</p> <p>Уметь:</p> <p>корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами;</p> <p>применять математические методы при исследовании криптографических алгоритмов;</p> <p>Владеть:</p> <p>криптографической терминологией;</p> <p>навыками использования типовых криптографических алгоритмов;</p> |

#### 4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 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.

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации<br>Ульяновский государственный университет | Форма |  |
| Ф – Аннотация рабочей программы дисциплины   |       |   |

## **6. Контроль успеваемости**

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

Промежуточная аттестация проводится в форме: экзамен.