



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика)

Министерство науки и высшего образования Российской Федерации

**ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

Кафедра прикладной математики и компьютерных наук

ОДОБРЕНО:

Руководитель ОП

 П. Г. Кононенко  
(подпись)

« 19 » июня 20 19 г.

**Рабочая программа дисциплины**

Криптографические методы защиты информации

Уровень высшего образования:	бакалавриат
Квалификация выпускника:	бакалавр
Направление подготовки:	01.03.01 Математика
Направленность (профиль) образовательной программы:	Математика

Иваново



## **1. Цели освоения дисциплины**

Цель курса состоит в знакомстве студентов с основными принципами построения блочных и поточных шифров, основами криптоанализа.

## **2. Место дисциплины в структуре ОП**

Дисциплина входит в часть ОП, формируемую участниками образовательных отношений. Для ее успешного изучения необходимы знания и умения, приобретенные в результате изучения следующих дисциплин: алгебра и геометрия; математический анализ; архитектура ЭВМ; языки программирования. Данная дисциплина должна подготовить студентов к освоению следующих дисциплин и практик: учебная практика, научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); производственная практика, научно-исследовательская работа; производственная практика, преддипломная.

Для освоения данной дисциплины обучающийся должен:

Знать: основные понятия алгебры и математического анализа, принципы функционирования ЭВМ

Уметь: производить вычисления в кольцах вычетов и многочленов

Иметь навыки: алгоритмизации и программирования

## **3. Планируемые результаты обучения по дисциплине**

### **3.1. Компетенции, формированию которых способствует дисциплина**

При освоении дисциплины формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

ПК-1. Способен применять в научно-исследовательской деятельности знания в области фундаментальной, прикладной математики и (или) основ информационных технологий.

### **3.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения формируемых компетенций**

В результате освоения дисциплины обучающийся должен:

Знать:

– основные понятия, факты, законы, концепции и методы криптографии и криптоанализа (ПК-1.1);

– международные и профессиональные стандарты в области информационных технологий (ПК-1.1).

Уметь:

– применять компьютеры и телекоммуникации, специальное оборудование, программные и аппаратные средства, системы обработки информации при поиске информации в области криптографии и криптоанализа (ПК-1.2);

– применять современный математический аппарат при решении задач в области криптографии и криптоанализа (ПК-1.2).

Иметь навыки:

– математического и алгоритмического моделирования при анализе задач в областях криптографии и криптоанализа (ПК-1.2);

– выявления связи задач криптографии и криптоанализа с математическими дисциплинами (ПК-1.2).

## **4. Объем и содержание дисциплины**

Объем дисциплины составляет 8 зачетных единиц (288 академических часов).



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика)

**4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и трудоемкостью занятий лекционно-семинарского типа**

Объем иной контактной работы и самостоятельной работы обучающегося по дисциплине указан в учебном плане образовательной программы.

№ п/п	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в ак. часах, по очной форме обучения)		Формы текущего контроля успеваемости (по очной форме обучения)  Формы промежуточной аттестации
			Занятия лекционно-го типа	Занятия семинарского типа	
1.	Основы криптографии	5	14	12	
2.	Основы криптоанализа	5	14	12	
3.	Блочные шифры	5	8	8	
Итого за семестр:			36	32	Зачет с оценкой
4.	Блочные шифры (продолжение)	6	14	12	
4.	Поточные шифры	6	20	18	
Итого за семестр:			34	30	Экзамен
Итого по дисциплине:			70	62	

**4.2. Развернутое описание содержания дисциплины по разделам (темам)**

1. Основы криптографии
  - 1.1. Формальное определение шифра
  - 1.2. Шифры перестановки
  - 1.3. Поточные шифры простой замены
  - 1.4. Блочные шифры простой замены
  - 1.5. Многоалфавитные шифры замены
  - 1.6. Дисковые многоалфавитные шифры замены
  - 1.7. Шифры гаммирования
2. Основы криптоанализа
  - 2.1. Характеристики текстовых сообщений
  - 2.2. Криптоанализ шифров перестановки
  - 2.3. Криптоанализ шифров простой замены
  - 2.4. Криптоанализ шифра гаммирования с периодической гаммой
  - 2.5. Криптоанализ шифра гаммирования с непериодической гаммой
3. Блочные шифры
  - 3.1. Принципы построения блочных шифров
  - 3.2. Алгоритм DES
  - 3.3. Алгоритм «Магма» (ГОСТ 28147-89)
  - 3.4. Алгоритм AES
  - 3.5. Алгоритм «Кузнечик» (ГОСТ Р 34.12-2015)
  - 3.6. Режимы использования блочных шифров
  - 3.7. Элементы криптоанализа блочных шифров
4. Поточные шифры
  - 4.1. Свойства и принципы построения поточных шифров
  - 4.2. Линейные регистры сдвига
  - 4.3. Усложнение генераторов ЛРП
  - 4.4. Примеры поточных шифров



## 5. Образовательные технологии

Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине: технология проблемного обучения

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: технологии смешанного обучения, интерактивные информационные технологии

## 6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Студенты выполняют самостоятельный поиск дополнительной информации по темам, перечисленным в п. 4.1, используя литературу, электронные ресурсы и базы данных, перечисленные в п. 8.

## 7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Промежуточная аттестация по дисциплине проводится в форме собеседования (по итогам первого семестра изучения дисциплины) и устного экзамена (по итогам года). Перечень вопросов к собеседованию и экзамену содержится в приложении 1, комплект билетов — в приложении 2.

На собеседовании оценка «удовлетворительно» выставляется студенту, если он

- **формулирует** основные понятия, факты, законы, концепции и методы криптографии и криптоанализа;

- **знает основные положения** международных и профессиональных стандартов в области криптографии и криптоанализа.

Оценка «хорошо» выставляется студенту, если в дополнение к указанному выше он

- эффективно **использует** программные и аппаратные средства, системы обработки информации при самостоятельном поиске информации в области криптографии и криптоанализа;

- пользуясь современным математическим аппаратом, фундаментальными концепциями и системными методологиями, **формулирует и обосновывает** допустимые методы решения задач в области криптографии и криптоанализа.

Оценка «отлично» выставляется студенту, если в дополнение к указанному выше он

- **использует** методы математического и алгоритмического моделирования при анализе задач в области криптографии и криптоанализа;

- **способен объяснить** взаимосвязь классических задач математики с задачами в области криптографии и криптоанализа и методами их решения.

На экзамене оценка «удовлетворительно» выставляется студенту, если он

- **формулирует** основные понятия, факты, законы, концепции и методы криптографии и криптоанализа;

- **знает основные положения** международных и профессиональных стандартов в области криптографии и криптоанализа.

Оценка «хорошо» выставляется студенту, если в дополнение к указанному выше он

- эффективно **использует** программные и аппаратные средства, системы обработки информации при самостоятельном поиске информации в области криптографии и криптоанализа;

- пользуясь современным математическим аппаратом, фундаментальными концепциями и системными методологиями, **формулирует и обосновывает** допустимые методы решения задач в области криптографии и криптоанализа.

Оценка «отлично» выставляется студенту, если в дополнение к указанному выше он

- **использует** методы математического и алгоритмического моделирования при анализе задач в области криптографии и криптоанализа;



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика)

– **способен объяснить** взаимосвязь классических задач математики с задачами в области криптографии и криптоанализа и методами их решения.

Итоговая оценка по дисциплине совпадает с оценкой, полученной на экзамене.

### **8. Учебно-методическое и информационное обеспечение дисциплины**

Основная литература:

1. Фефилов, А.Д. Методы и средства защиты информации в сетях [Электронный ресурс] / А.Д. Фефилов. - М. : Лаборатория книги, 2011. - 105 с. - URL: <http://biblioclub.ru/index.php?page=book&id=140796>

2. Методы и средства инженерно-технической защиты информации : учебное пособие [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. - М. : Флинта, 2011. - 187 с. - URL: <http://biblioclub.ru/index.php?page=book&id=93275>

3. Креопалов, В.В. Технические средства и методы защиты информации. Учебн : практическое пособие [Электронный ресурс] / В.В. Креопалов. - М. : Евразийский открытый институт, 2011. - 278 с. - URL: <http://biblioclub.ru/index.php?page=book&id=90753>

4. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В.Ф. Шаньгин. - М. : ДМК Пресс, 2010. - 544 с. - URL: <http://biblioclub.ru/index.php?page=book&id=86475>

5. Анализ состояния защиты данных в информационных системах. Учебно-методическое пособие [Электронный ресурс] / Новосибирск : НГТУ, 2012. - 52 с. - URL: <http://biblioclub.ru/index.php?page=book&id=228844>

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с. - (Организация и технология защиты информации). - ISBN 978-5-9765-1272-6 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93343>

2. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие / М.А. Иванов, И.В. Чугунков ; под ред. М.А. Иванова ; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ». - М. : МИФИ, 2012. - 400 с. : табл., схем. - ISBN 978-5-7262-1676-8 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=231673>

3. Титов, А.А. Технические средства защиты информации : учебное пособие / А.А. Титов. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 194 с. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=208661>

4. Сергеева, Ю.С. Защита информации: Конспект лекций : учебное пособие / Ю.С. Сергеева. - М. : А-Приор, 2011. - 128 с. - (Конспект лекций). - ISBN 978-5-384-00397-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=72670>

5. Ярочкин, В.И. Информационная безопасность. Учебник для вузов [Электронный ресурс] / В.И. Ярочкин. - М. : Академический проект, 2008. - 544 с. - URL: <http://biblioclub.ru/index.php?page=book&id=211164>

Ресурсы информационно-телекоммуникационной сети «Интернет»:

Система электронной поддержки образовательного процесса «Мой университет» <https://uni.ivanovo.ac.ru>

Профессиональные базы данных и информационно-справочные системы:

ЭБС «Университетская библиотека онлайн» [www.biblioclub.ru](http://www.biblioclub.ru)



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика)

---

Электронная библиотека ИвГУ <http://lib.ivanovo.ac.ru>

Электронный каталог НБ ИвГУ <http://lib.ivanovo.ac.ru/index.php/ek>

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ Microsoft Office и (или) LibreOffice, интернет-браузер Microsoft Edge и (или) Yandex Browser, кроссплатформенная среда разработки Code::Blocks.

## **9. Материально-техническое обеспечение дисциплины**

Учебные аудитории:

- для проведения занятий лекционного типа с комплектом специализированной учебной мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;

- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими средствами обучения.

Лаборатория, оснащенная лабораторным оборудованием, комплектом специализированной учебной мебели и техническими средствами обучения.

Помещение для самостоятельной работы, оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС.

Демонстрационное оборудование и учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации: демонстрационные устройства; электронные презентации.



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика)

Автор(ы) рабочей программы дисциплины: зав. кафедрой ПМиКН, к.ф.-м.н., доцент  
Соколов Е. В.

Программа рассмотрена и утверждена на заседании кафедры прикладной математики и  
компьютерных наук

« 13 » июня 2019 г., протокол № 11

Программа обновлена  
протокол заседания кафедры № \_\_\_\_\_ от « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

Согласовано:

Руководитель ОП \_\_\_\_\_ П.Г. Кононенко  
(подпись)

Программа обновлена  
протокол заседания кафедры № \_\_\_\_\_ от « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

Согласовано:

Руководитель ОП \_\_\_\_\_  
(подпись)

Программа обновлена  
протокол заседания кафедры № \_\_\_\_\_ от « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

Согласовано:

Руководитель ОП \_\_\_\_\_  
(подпись)