



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика, алгоритмы и анализ данных)


Министерство науки и высшего образования Российской Федерации

**ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

Кафедра прикладной математики и компьютерных наук

ОДОБРЕНО:

Руководитель ОП

 Ю.А. Хашина

(подпись)

«\_1\_» сентября\_2023 г.

**Рабочая программа дисциплины**  
**Основы информационной безопасности**

|  |                                       |
|--|---------------------------------------|
| Уровень высшего образования:                           | бакалавриат                           |
| Квалификация выпускника:                               | бакалавр                              |
| Направление подготовки:                                | 01.03.01 Математика                   |
| Направленность (профиль)<br>образовательной программы: | Математика, алгоритмы и анализ данных |

Иваново



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика, алгоритмы и анализ данных)

---

### **1. Цели освоения дисциплины**

ОП имеет своей целью подготовку бакалавров для научной работы в области информационных технологий путем развития у студентов личностных качеств и формирования общекультурных и профессиональных компетенций в соответствии с ФГОС ВО.

Дисциплина читается студентам обучающимся по образовательной программе «Математика» в 3 семестре. Цель преподавания – ознакомить студентов с задачами и методами информационной безопасности, в объёме достаточном для успешного практического использования полученных знаний в дальнейшей работе по специальности, а также для самостоятельного изучения соответствующей научной литературы.

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

Дисциплина является факультативной.

Для освоения данной дисциплины обучающийся должен:

Знать: основные понятия, факты математического анализа и линейной алгебры.

Уметь: применять для решения различных задач основные понятия, факты, законы, концепции и методы естественных наук, математики, фундаментальной информатики и информационных технологий.

Владеть следующими дисциплинами:

Алгебра

Дискретная математика

Теория чисел

### **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:

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни

#### **3.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с формируемыми компетенциями**

В результате освоения дисциплины обучающийся должен:

Знать:

Основные понятия информационной безопасности: симметричную и ассиметричную электронную подпись, хэш-функции, настройки Windows (УК-2, УК-6).

Уметь:

вычислять электронные подписи в простейших случаях, выполнять базовые настройки Windows для обеспечения информационной безопасности (УК-2, УК-6).

Владеть:

методами вычисления электронной подписи, опытом настройки Windows для обеспечения информационной безопасности (УК-2, УК-6)

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

Объем дисциплины составляет 2 зачетных единиц (72 академических часов).



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика, алгоритмы и анализ данных)

**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)<br><br>Формы промежуточной аттестации |
|----------------------|---------------------------|---------|---|---------------------------|--|
|                      |                           |         | Занятия лекционного типа                                      | Занятия семинарского типа |  |
| 1.                   | Симметричная криптография | 3       | 2   | 2                         | Опорный конспект   |
| 2.                   | Электронная подпись       | 3       | 2   | 6                         | Опорный конспект   |
| 3                    | Безопасность Windows      | 3       | 2   | 8                         | Опорный конспект   |
| 4                    | Антивирусы                | 3       | 4   | 6                         | Опорный конспект   |
| 5                    | Безопасность сетей TCP/IP | 3       | 4   | 4                         | Опорный конспект   |
| 6                    | Симметричная криптография | 3       | 4   | 6                         | Опорный конспект   |
| Итого за семестр:    |                           |         | 18  | 32                        | Зачёт  |
| Итого по дисциплине: |                           |         | 18  | 32                        |  |

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

- Общие правила безопасности
- Настройки Windows
- Разметка дисков
- Виртуальные машины
- Настройки BIOS
- msconfig
- Работа с реестром
- Групповая политика
- Службы
- Автозагрузка
- Отключение автозапуска
- Журнал событий
- Настройки Internet Explorer
- Учетные записей пользователей
- Администратор и его пароль
- Скрытые сетевые ресурсы
- Антивирусы
- Последствия заражений компьютерными вирусами
- Как определить наличие вируса?
- Брандмауэры
- Обнаружение вирусов
- Режим работы антивируса
- Drweb
- Безопасность TCP-IP сетей



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика, алгоритмы и анализ данных)

---

- Технология Ethernet
- Технология TCP/IP
- Встроенные команды Windows для ip-сетей
- http-протокол
- Снiffer
- Обнаружение атак
  
- Симметричная криптография
  - История
  - Шифры-подстановки и перестановки
  - Энигма
  - Преобразование Фейстеля
  - Стандарт DES
  - ГОСТ 28147-89
  - Базовый шаг криптопреобразования
  - Режимы работы
  - Режим простой замены
  - Криптографический датчик случайных чисел
  - Гаммирование
  - Гаммирование с обратной связью
  - Другие алгоритмы шифрования
- Хеш-функции
  - MD5
  - ГОСТ Р 34.11-94
  - ГОСТ Р 34.11-2012
- Задачи
- Ассиметричная криптография
  - Длинные числа. Алгоритмы и скорость работы
  - Простые числа. Теорема Ферма. Числа Кармайкла
  - Функция Эйлера
  - Распределение простых чисел
  - Общее понятие электронной подписи.
  - Алгоритм RSA
  - El-Gamal. ГОСТ Р 34.10-94
  - Общее описание алгоритма
  - ГОСТ Р 34.10-94
  - Поля Галуа характеристики  $2^m$
  - Эллиптические кривые. Структура группы
  - ГОСТ Р 34.10-2001
- Теория чисел на Maple
- Реализация. Java
- Приложения
- Задачи
- Вопросы по криптографии
- Варианты контрольной работы

## 5. Образовательные технологии



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика, алгоритмы и анализ данных)

технологии смешанного обучения.

**6. Учебно-методическое обеспечение самостоятельной работы обучающихся**

ЭИОС «Мой университет» <https://uni.ivanovo.ac.ru>

Тесты на сайте кафедры <http://math.ivanovo.ac.ru/dalgebra/Khashin/tests/index.html>

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

Задачи для домашних работ, комплект задач обработки данных, вопросы и задачи зачёта. Форма проведения: зачёт.

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

Основная литература:

1. Анализ состояния защиты данных в информационных системах / сост. В.В. Денисов. – Новосибирск : НГТУ, 2012. – 52 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=228844> (дата обращения: 30.06.2019). – ISBN 978-5-7782-1969-4. – Текст : электронный.

2. Креопалов, В.В. Технические средства и методы защиты информации / В.В. Креопалов. – Москва : Евразийский открытый институт, 2011. – 278 с. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=90753> (дата обращения: 30.06.2019). – ISBN 978-5-374-00507-3. – Текст : электронный.

Дополнительная литература:

1. Сергеева, Ю.С. Защита информации: Конспект лекций / Ю.С. Сергеева. – Москва : А-Приор, 2011. – 128 с. – (Конспект лекций). – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=72670> (дата обращения: 30.06.2019). – ISBN 978-5-384-00397-7. – Текст : электронный.

2. Титов, А.А. Технические средства защиты информации / А.А. Титов. – Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. – 194 с. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=208661> (дата обращения: 30.06.2019). – Текст : электронный.

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);

<http://lib.ivanovo.ac.ru/index.php/polnotekstovye-resursy/ebs-universitetskaya-biblioteka>

Электронная библиотека ИвГУ <http://lib.ivanovo.ac.ru/index.php/polnotekstovye-resursy/elibnew>

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

Программное обеспечение: операционная система Windows, офисный пакет Microsoft Office и(или) LibreOffice, Интернет-браузер Internet Explorer и(или) Microsoft Edge и(или) Yandex Browser, антивирусное программное обеспечение Kaspersky Endpoint Security.

**9. Материально-техническое обеспечение дисциплины**



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика, алгоритмы и анализ данных)

---

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;
- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации, выполнения курсовых работ (проектов) с 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.



Основная профессиональная образовательная программа  
01.03.01 Математика  
(Математика, алгоритмы и анализ данных)

---

**Автор(ы) рабочей программы дисциплины:** к.ф.-м.н. доцент С.И.Хашин

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

«\_\_\_» \_\_\_\_\_ 20 \_\_\_ г., протокол № \_\_\_\_\_

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

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

Согласовано:

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