



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

Н.Г. Косарев
(подпись)

Н.Г. Косарев

« 13 » июня 20 18 г.

Рабочая программа дисциплины
Информационная безопасность

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



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» по направлению 01.03.01 Математика в 5 семестре. Цель преподавания – ознакомить студентов с задачами и методами информационной безопасности, в объеме 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 входит в состав базовой части ОП.

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:

ОПК-2; способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ПК-1; способностью к определению общих форм и закономерностей отдельной предметной области

ПКВ-1 способность использовать знания математики и компьютерных наук в различных сферах профессиональной деятельности, в том числе в образовании, в областях, использующих математические методы и компьютерные технологии

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 (ОПК-2).

Уметь:

вычислять электронные подписи в простейших случаях, выполнять базовые настройки Windows для обеспечения информационной безопасности (ОПК-2, ПК-1, ПКВ-1).

Владеть:

методами вычисления электронной подписи, опытом настройки Windows для обеспечения информационной безопасности (ОПК-2, ПК-1, ПКВ-1)



Основная профессиональная образовательная программа
01.03.01 Математика
(Математика)

4. Объем и содержание дисциплины

Объем дисциплины составляет 3 зачетных единиц (108 академических часов).

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 лекцион- ного типа	Занятия семинар- ского типа	
1.	Симметричная криптография	5	2	2	Опорный конспект
2.	Электронная подпись	5	8	6	
3	Безопасность Windows	5	8	8	
3	Антивирусы	5	8	6	
4	Безопасность сетей TCP/IP	5	4	4	
5	Симметричная криптография	5	6	6	
Итого за семестр:			36	32	Зачёт
Итого по дисциплине:			36	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



Основная профессиональная образовательная программа
01.03.01 Математика
(Математика)

- Как определить наличие вируса?
- Брандмауэры
- Обнаружение вирусов
- Режим работы антивируса
- Drweb
- Безопасность TCP-IP сетей
- Технология Ethernet
- Технология TCP/IP
- Встроенные команды Windows для ip-сетей
- http-протокол
- Сниффер
- 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



Основная профессиональная образовательная программа
01.03.01 Математика
(Математика)

- Приложения
- Задачи
- Вопросы по криптографии
- Варианты контрольной работы

5. Образовательные технологии

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. 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. Кострикин А. И. Введение в алгебру. М.: Наука, 1977.- 495 с. 108 экземпляров.

2. Яцкин Н. И. Алгебра: Теоремы и алгоритмы: Учеб. пособие. Иваново: ИвГУ, 2008. – 606 с. – 98 экз.

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

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

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



Основная профессиональная образовательная программа
01.03.01 Математика
(Математика)

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ LibreOffice, интернет-браузер Yandex Browser, Code::Blocks, IDLE, Maxima, VirtualBox, Visual Studio 2013.

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: кандидат физ. – мат. наук, доцент
С.И. Хашин

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

«29» августа 20 16 г., протокол № 1

Программа обновлена

протокол заседания кафедры № 1 от «30» августа 20 17 г.

Программа обновлена

протокол заседания кафедры № 9 от «1» июня 20 18 г.

Программа обновлена

протокол заседания кафедры № 1 от «30» августа 20 19 г..

Согласовано:

Руководитель ОП Кононенко П.Г. Кононенко
(подпись)