

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Костромской государственный университет»
(КГУ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки 01.03.02 «Прикладная математика и
информатика»

Направленность подготовки «Прикладная математика и информатика»

Квалификация (степень) выпускника: бакалавр

Кострома


Рабочая программа дисциплины «Информационная безопасность» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 01.03.02 Прикладная математика и информатика (уровень подготовки бакалавриат), утвержденным приказом Министерства образования и науки РФ от 12 марта 2015 года № 228 (рег. 14 апреля 2015 г., № 36844). Год начала подготовки 2017, 2018.

Разработал:  Сухов Андрей Константинович, доцент, к.ф.-м.н., доцент
подпись

Рецензент:  Леготин Денис Леонидович, доцент, к.ф.-м.н., доцент
подпись


УТВЕРЖДЕНО:

На заседании кафедры прикладной математики и информационных технологий
Протокол заседания кафедры № 10 от 03.06.2017 г.

Заведующий кафедрой прикладной математики и информационных технологий
 Секованов Валерий Сергеевич, д.п.н, к.ф.-м.н., профессор КГУ

ПЕРЕУТВЕРЖДЕНО:

На заседании кафедры прикладной математики и информационных технологий
Протокол заседания кафедры № 9 от 22.05.2018 г.

Заведующий кафедрой прикладной математики и информационных технологий
 Секованов Валерий Сергеевич, д.п.н, к.ф.-м.н., профессор КГУ

1. Цели и задачи освоения дисциплины

Обмену разнородной информацией влечет за собой не только прогрессивные начала, но и вызывает потребность защиты данных от несанкционированного доступа с целью предотвращения их изменения и уничтожения, нарушению информационных прав граждан. Курс «Информационная безопасность» посвящен изучению современного представления о методах и средствах обеспечения защиты компьютерной информации.

Цель дисциплины: познакомить студентов с тенденциями развития, терминологией и основными понятиями теории защиты информации, а так же с методами защиты компьютерной информации.

Задачи дисциплины:

- основным понятиям и определениям информационной безопасности;
- противостоять угрозам, которым подвергается информация;
- защите от вредоносных программ и компьютерных вирусов;
- методам и средствам защиты информации в компьютерных сетях.

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

знать:

- основные понятия и определения информационной безопасности;
- методы противостояния угрозам, которым подвергается информация;
- способы защиты от вредоносных программ и компьютерных вирусов;
- методы и средства защиты информации в компьютерных сетях.

уметь:

- выявлять источники, риски и формы атак на информацию,
- работать с различными антивирусными программами,
- разрабатывать политику защиты компьютерной информации в соответствии со стандартами безопасности,
- использовать методы шифрования данных.
- выявлять источники, риски и формы атак на информацию,
- работать с различными антивирусными программами,
- разрабатывать политику защиты компьютерной информации в соответствии со стандартами безопасности,
- использовать методы шифрования данных.

владеть:

- методами обеспечения эффективной защиты информации и криптографии.

освоить компетенции:

ОПК-4 – 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-10 – способностью к реализации решений, направленных на поддержку социально-значимых проектов, на повышение информационной грамотности населения, обеспечения общедоступности информационных услуг.

3. Место дисциплины в структуре ОП ВО

Дисциплина «Численные методы» относится к вариативной части профессионального цикла. В отношении технологического содержания она дополняет дисциплины «Дискретная математика», «Языки и методы программирования», «Визуальное программирование». В отношении класса решаемых задач она находится в одном ряду с дисциплинами «Системное и прикладное программное обеспечение», «Дифференциальные уравнения», «Функциональный анализ».

Для изучения дисциплины «Численные методы» необходимы знания, умения и навыки, формируемые предшествующими дисциплинами «Компьютерные сети», «Основы информатики», «Языки программирования и методы трансляции».

4. Объем дисциплины «Информационная безопасность»

4.1. Объем дисциплины в зачётных единицах с указанием академических (астрономических) часов и виды учебной работы

| Виды учебной работы, | Очная форма |
|--|-------------------|
| Общая трудоемкость в зачетных единицах | 2 |
| Общая трудоемкость в часах | 72 |
| Аудиторные занятия в часах, в том числе: | 36 |
| Лекции | 18 |
| Практические занятия | - |
| Лабораторные занятия | 18 |
| Контроль | - |
| Самостоятельная работа в часах | 36 |
| Форма промежуточной аттестации | Зачёт – 8 семестр |

4.2. Объем контактной работы на 1 обучающегося

| Виды учебных занятий | Очная форма |
|----------------------|-------------|
| Лекции | 18 |
| Практические занятия | - |
| Лабораторные занятия | 18 |
| Консультации | 0,9 |
| Зачет/зачеты | 0,25 |
| Экзамен/экзамены | - |
| Курсовые работы | - |
| Курсовые проекты | - |
| Всего | 37,15 |

**5.Содержание дисциплины «Информационная безопасность»,
структурированное по темам (разделам), с указанием количества
часов и видов занятий**

5.1 Тематический план учебной дисциплины

| № п/п | Наименование темы | Всего з.е./час | Аудиторные занятия | | | Контроль | Самос. |
|-------|--|----------------|--------------------|--------|--------|----------|--------|
| | | | Лекции | Практ. | Лабор. | | |
| 1. | Актуальность информационной безопасности, понятия и определения. | 0,44/16 | 2 | - | 2 | - | 12 |
| 2. | Угрозы информации. | 0,44/16 | 4 | - | 4 | - | 8 |
| 3. | Методы и средства защиты компьютерной информации. | 0,44/16 | 4 | - | 4 | - | 8 |
| 4. | Криптографические методы защиты информации | 0,68/24 | 8 | | 8 | | 8 |
| | ИТОГО: | 2/0 | 0 | - | 0 | - | 0 |

5.2. Содержание:

Тема 1. Актуальность информационной безопасности, понятия и определения. Актуальность информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Классификация компьютерных преступлений. Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet. Понятия и определения в информационной безопасности.

Тема 2. Угрозы информации. Виды угроз информационной безопасности. Источники угроз информационной безопасности. Условия существования вредоносных программ. Классические компьютерные вирусы. Сетевые черви. Троянские программы. Спам. Хакерские утилиты и прочие вредоносные программы. Кто и почему создает вредоносные программы.

Тема 3. Методы и средства защиты компьютерной информации. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы. Методы обеспечения информационной безопасности. Ограничение доступа. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Выбор средств информационной защиты. Стандарты безопасности. Критерии безопасности компьютерных систем.

Тема 4. Криптографические методы защиты информации. Доступность, целостность и конфиденциальность информации. Криптоанализ и шифрование. Симметричное шифрование информации. Подстановочные и перестановочные шифры. Асимметричное шифрование информации. Открытый и закрытый ключ. Односторонние преобразования. Алгоритмы шифрования: RSA, укладка ранца, Эль-

Гамаля. Принцип работы, криптостойкость, применение. Цифровая подпись. Длинная арифметика.

6. Методические материалы для обучающихся по освоению дисциплины «Численные методы»

6.1. Самостоятельная работа обучающихся по дисциплине

| № п/п | Раздел (тема) дисциплины | Задание | Часы | Методические рекомендации по выполнению задания | Форма контроля |
|-------|--|---|------|---|---|
| 1 | Актуальность информационной безопасности, понятия и определения. | Изучение теоретического материала | 12 | Используйте литературу [1], [2], [5] | Устный опрос |
| 2 | Угрозы информации. | Изучение литературы, составление компьютерных программ | 8 | Используйте литературу [1], [2], [5] | Индивидуальное собеседование, проверка домашних заданий |
| 3 | Методы и средства защиты компьютерной информации. | Изучение литературы, составление компьютерных программ, решение задач | 8 | Используйте литературу [1], [2], [3] | Индивидуальное собеседование, проверка домашних заданий, контрольная работа |
| 4 | Криптографические методы защиты информации | Решение индивидуальных заданий | 8 | Используйте литературу [1], [3], [4] | Проверка заданий |

6.3. Тематика и задания для лабораторных занятий

Лабораторные занятия 1. Простые числа.

Проверка является ли натуральное число простым. Генерация заданных простых чисел. Целочисленное деление.

Лабораторные занятия 2. Методы симметричного шифрования.

Код Цезаря. Аффинное шифрование. Квадрат Полибия. Перестановочные шифры.

Лабораторные занятия 3. Метод асимметричного шифрования RSA.

Задание открытого и закрытого ключей. Шифрование и дешифровка отдельного символа, строки. Цифровая подпись.

Лабораторные занятия 4. Метод асимметричного шифрования укладка ранца.

Задание открытого и закрытого ключей. Шифрование и дешифровка отдельного символа, строки.

Лабораторные занятия 5. Метод асимметричного шифрования Эль-Гамала.

Задание открытого и закрытого ключей. Шифрование и дешифровка отдельного символа, строки. Цифровая подпись.

Вопросы к зачету

1. Актуальность информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Классификация компьютерных преступлений. Способы совершения компьютерных преступлений.
2. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet. Понятия и определения в информационной безопасности.
3. Виды угроз информационной безопасности. Источники угроз информационной безопасности. Условия существования вредоносных программ. Классические компьютерные вирусы.
4. Сетевые черви. Троянские программы. Спам. Хакерские утилиты и прочие вредоносные программы. Кто и почему создает вредоносные программы.
5. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы. Методы обеспечения информационной безопасности. Ограничение доступа. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ.
6. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Выбор средств информационной защиты. Стандарты безопасности. Критерии безопасности компьютерных систем.
7. Криптографические методы защиты информации. Доступность, целостность и конфиденциальность информации. Криптоанализ и шифрование.
8. Симметричное шифрование информации. Подстановочные и перестановочные шифры.
9. Асимметричное шифрование информации. Открытый и закрытый ключ. Односторонние преобразования.
10. Алгоритм шифрования RSA. Принцип работы, криптостойкость, применение. Цифровая подпись. Длинная арифметика.
11. Алгоритм шифрования укладка ранца. Принцип работы, криптостойкость, применение. Цифровая подпись. Длинная арифметика.
12. Алгоритм шифрования Эль-Гамала. Принцип работы, криптостойкость, применение. Цифровая подпись. Длинная арифметика.

Для сдачи зачета студент должен представить отчеты по всем разработанным программам текущего семестра и ответить на вопросы зачета.

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины «Численные методы»

а) основная:

1. Сычев Ю.Н. Информационная безопасность, 2011 г.
2. Мельников В.П. Информационная безопасность: 3е издание – М: Издательский центр «Академия», 2008
3. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие – СПб: Питер, 2008

б) дополнительная литература

- II. Мельников В.П. Информационная безопасность и защита информации: учебное пособие – М: Издательский центр «Академия», 2007
- III. Галатенко В.А. Основы информационной безопасности: курс лекций - М: Интернет – Университет Информационных технологий, 2006
1. Филин С.А. Информационная безопасность: учебное пособие – М: Альфа-Пресс, 2006
2. Ярочкин В.И., Бузанова Я.В. Теория безопасности – М: Академический проект, 2005
3. Прохожев А.А. Общая теория национальной безопасности: учебник – М: РАГС, 2005
4. Байбурин В.Б., Бровков М.Б., Пластун И.Л. Введение в защиту информации: учебное пособие – М: Инфра-М, 2004

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Библиотека КГУ <http://library.ksu.edu.ru/>
2. Национальный открытый университет ИНТУИТ (www.intuit.ru)

Электронные библиотечные системы:

3. ЭБС «Лань»
4. ЭБС «Университетская библиотека online»
5. ЭБС «Znanium»

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий по дисциплине необходим компьютерный класс с проектором. Необходимое программное обеспечение:

- среда программирования;
- офисный пакет.