МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Костромской государственный университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

Направление подготовки 10.03.01 Информационная безопасность

Направленность «Организация и технология защиты информации»

Квалификация (степень) выпускника: Бакалавр

Кострома

Рабочая программа дисциплины «Математические основы криптологии» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность
Приказ Минобрнауки России от 1.12.2016 № 1515. Зарегистрировано в Минюсте России, регистрационный № 44821 от 20 декабря 2016 года.

Год начала подготовки 2017

Разработал: _____ Волков Антон Андреевич, доцент кафедры защиты информации, к.т.н.

Рецензент: _____ Алексеев Дмитрий Станиславович, доцент кафедры защиты информации, к.т.н.

УТВЕРЖДЕНО:

На заседании кафедры защиты информации

Протокол заседания кафедры № 13 от 6 июля 2017 г.

Заведующий кафедрой защиты информации

_____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 12 от 27 июня 2018 г.

Заведующий кафедрой защиты информации

_____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _11_ от _30.05.2019_____ г.

Заведующий кафедрой защиты информации

_____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _8_ от _6.04.2020_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _6_ от _22.01.2021_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

1. Цели и задачи освоения дисциплины

«Математические основы криптологии» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»; формирование у бакалавров знаний и навыков в предметной области. Предмет курса - криптографические методы.

Профессиональные цели курса —изучение и освоение математических методов криптологии, наиболее применяемых в области комплексной защиты объектов информатизации. Формирование практических навыков для решения задач по основам теории информации, реализовывать, применять и анализировать основные компьютерные методы криптологии.

Задачи дисциплины:

- дать основы: -системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- алгебраических и теоретико-числовых принципов синтеза и анализа шифров;
- математических методов, используемых в криптоанализе и криптографии.

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

знать

- типичные слабости реализации современных криптографических систем;
- стандарты, модели и методы шифрования;
- основные алгоритмы идентификации и аутентификации.

уметь

- реализовать криптографические алгоритмы и протоколы;

владеть

- реализации простейших криптографических алгоритмов и протоколов.

освоить компетенции:

- способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);

3. Место дисциплины в структуре ОП ВО

Дисциплина «Математические основы криптологии» относится к циклу дисциплин по выбору.

Дисциплина изучается на втором курсе, требования к входным знаниям, умениям и навыкам определяются требованиями к уровню подготовки по дисциплине «Информатика» за курс средней школы, блок математических дисциплин.

Изучение дисциплины является основой для освоения последующих дисциплин/практик: «Сети и системы передачи информации»

4. Объем дисциплины (модуля)

4.1. Объем дисциплины в зачетных 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:	50
Лекции	16
Практические занятия	34

Лабораторные занятия	-
Самостоятельная работа в часах	22
Форма промежуточной аттестации	Зачет

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	16
Практические занятия	-
Лабораторные занятий	34
Консультации	0,8
Зачет/зачеты	0,25
Экзамен/экзамены	-
Курсовые работы	–
Курсовые проекты	–
Всего	51,05

5.Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием количества часов и видов занятий

5.1 Тематический план учебной дисциплины

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	практические	
1.	Введение в теорию чисел	6	2	2	2
2.	Теория делимости	8	2	4	2
3.	Сравнения	8	2	4	2
4.	Криптопротокол ключевого обмена DH.	8	2	4	2
5.	Криптосистема RSA на основе модулярной арифметики	10	2	6	2
6.	Электронная подпись	8	2	4	2
7.	Хеш-функции	8	2		2
8.	Элементы высшей алгебры	10	2	6	2
Зачёт		6			6
Всего:		**216**	**16**	**34**	**22**

5.2. Содержание:

ТЕМА 1. Теория делимости. Основные понятия и теоремы теории делимости. Наибольший общий делитель, алгоритм поиска. Наименьшее общее кратное, алгоритм поиска. Простые числа. Разложение на простые множители и его единственность. Алгоритм Евклида и цепные дроби.

ТЕМА 2. Сравнения. Свойства сравнений. Классы вычетов. Полная и приведенная системы вычетов. Теоремы Эйлера и Ферма. Сравнения первой степени. Китайская теорема об остатках. Сравнения любой степени по-простому и составному модулю. Символ Лежандра и Якоби. Первообразные корни, индексы и характеры по модулю.

ТЕМА 3. Криптопротокол ключевого обмена DH.

Протокол Диффи — Хеллмана. Основными задачи, возникающие при анализе криптографических протоколов. Проблема распределения ключей. Понятие безопасности протокола. Схема открытого распределения ключей. Создание открытого и секретного ключей.

ТЕМА 4. Криптосистема RSA на основе модулярной арифметики. Основные термины и определения. RSA. Криптосистема с открытым ключом. Открытый ключ, Закрытый ключ. История исследования. Описание алгоритма. Шифрование и дешифрование. Методы криптоанализа RSA, генерация простых чисел, схема с общим модулем, алгоритм Шора.

ТЕМА 5. Электронная подпись. Описание алгоритма цифровой подписи. Система Рабина. Задача о рюкзаке. Признаки простоты и алгоритмы генерации простых чисел. Электронные цифровые подписи: Рабина, Диффи-Лампорта, DSS, Эль-Гамаля, Российского стандарта.

ТЕМА 6. Хеш-функции. Задача дискретного логарифмирования. Определение и принцип действия. Анализ безопасности хеш-функций. Итеративная хеш-функция. Хеш-функции на основе итеративных блочных симметричных шифров.

ТЕМА 7. Элементы высшей алгебры. Теория групп. Группы и подгруппы. Гомоморфизмы групп. Группы подстановок. Действие группы на множестве. Кольца и поля. Простые и максимальные идеалы. Поля Галуа. Евклидовы кольца. Конечные расширения полей. Неприводимые многочлены и их порядки. Линейные рекуррентные последовательности. Поточные криптосистемы.

6. Методические материалы для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы.

Обучающемуся важно помнить, что лекция эффективно помогает ему овладеть программным материалом благодаря расстановке преподавателем необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации. Кроме того, во время лекции имеет место прямой визуальный и эмоциональный контакт обучающегося с преподавателем, обеспечивающий более полную реализацию воспитательной компоненты обучения.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков применения методов формирования, организации и поддержки комплекса мер по обеспечению информационной безопасности объекта защиты;
- совершенствование навыков поиска публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации студента.

6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

№ п/п	Раздел (тема)	Задание	Методические рекомендации по выполнению задания	Форма контроля
1	2	3	4	5
1.	Тема № 1	Усвоить	1. Изучить значение и место курса в подготовке специалистов по защите информации. Литература основная[1-2], дополнительная [1-2]	Контрольный опрос
2.	Тема № 2	Усвоить	1. Выучить основные свойства сравнений. 2. Усвоить принципы решения типовых задач с применением сравнений. Литература основная[1-2], дополнительная [1-2]	Контрольный опрос
3.	Тема № 3	Приобрести навык	1. Приобрести навык математической реализации протокол Диффи — Хеллмана. 2. Изучить понятие открытого и секретного ключей. Литература основная[1-2], дополнительная [1-2]	Проверка выполнения лабораторной работы
4.	Тема № 4	Усвоить	1. Изучить принципы RSA шифрования 2. Изучить принципы криптосистем с открытым ключом. Открытый ключ.	Контрольный опрос
5.	Тема № 5	Усвоить	1. Признаки простоты и алгоритмы генерации простых чисел. 2. Изучить Описание алгоритма цифровой подписи. Литература основная[1-2], дополнительная [1-2]	Проверка выполнения практического задания
6.	Тема № 6	Усвоить	1. Изучить алгоритмы для решения задачи дискретного логарифмирования. Литература основная[1-2], дополнительная [1-2]	Контрольный опрос
7.	Тема № 7	Приобрес-ти навык	1. Изучить основные понятия поточных криптосистем. Литература основная[1-2], дополнительная [1-2]	Проверка выполнения

Формой отчетности по данной дисциплине является зачет. Необходимые условия зачета – выполнение более 10 лабораторных работ.

6.2. Тематика и задания для практических занятий (*при наличии*)

Тема 1. Нахождение НОД, НОК, коэффициентов Безу.
Тема 2. Использование м. теоремы Ферма и Эйлера.
Тема 3. Решение диофантовых уравнений, сравнений.
Тема 4. Решение систем сравнений методом прямой подстановки, с использованием китайской теоремы об остатках.
Тема 5. Нахождение квадратичных вычетов.
Тема 6. Вычисление символов Якоби, порядка первообразного корня.
Тема 7. Решение сравнений методом индексирования.
Тема 8. Разложение выражений в цепную дробь.
Тема 9. Шифр Цезаря.
Тема 10. Алгоритм Base 64.

Тема 11. Реализация алгоритма RSA.
Тема 12. Векторный шифр Аббата Тритемиуса.
Тема 13. Применение Хэш-функции в шифровании.
Тема 14. Матричный 3d криптопротокол

6.3. Тематика и задания для лабораторных занятий

Не предусмотрены

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

Основная

1. **Фомичев, В.М.** Методы дискретной математики в криптологии / В.М. Фомичев. - Москва : Диалог-МИФИ, 2010. - 436 с. : ил. - Библиогр.: с. 422-428. - ISBN 978-5-86404-234-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=447668
2. **Фомичев, В.М**. Дискретная математика и криптология : курс лекций / В.М. Фомичев ; под общ. ред. Н.Д. Подуфалова. - : Диалог-МИФИ, 2003. - 397 с. : табл., схем. - Библиогр. в кн. - ISBN 5-86404-185-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=89387

Дополнительная

1. **Гультяева, Т.А.** Основы теории информации и криптографии : конспект лекций / Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2010. - 88 с. : табл., схем. - ISBN 978-5-7782-1425-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=228963
2. **Логачев, О. А.** Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко ; Ин-т проблем информационной безопасности МГУ. - М. : МЦНМО, 2004. - 470с. - (Новые математические дисциплины) (Информационная безопасность: криптография). - Библиогр.: с. 430-461. - Предм. указ.: с. 462-469. - ISBN 5-94057-117-4 : 160.00.

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

Информационно-образовательные ресурсы:
1. www.atlas.Krasnodar.ru -КФ НТЦ «Атлас»: защита информации.

Электронные библиотечные системы:
1. Университетская библиотека онлайн http://biblioclub.ru
2. «Лань» http://e.lanbook.com/
3. ЭБС «Znanium»
4. Справочно-информационная система (СИС) «Гарант».
5. Справочно-информационная система «Консультант».
6.Электронно-библиотечная система (ЭБС) «Инфра-М».

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

Лекционная аудитория, оснащенная проектором, компьютером.
Учебный класс, меловая или маркерная доска