МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Костромской государственный университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки 10.03.01 Информационная безопасность

Направленность «Организация и технология защиты информации»

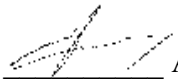
Квалификация (степень) выпускника: Бакалавр

Кострома

Рабочая программа дисциплины «Криптографические методы защиты информации» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность, утвержден 01.12.2016 г.

Год начала подготовки 2017

Разработал:  Щекочихин Олег Владимирович, к.т.н., доцент, заведующий кафедры защиты информации

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

Целями дисциплины «Криптографические методы защиты информации» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»; изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Дисциплина «Криптографические методы защиты информации» рассматривается как теоретическая и прикладная дисциплина, дающая представление об основных математических и алгоритмических подходах применяемых в шифровании информации.

Дисциплина посвящена изучению основ криптографии и криптографического анализа, применяемых при защите информации в информационных системах. Обучаемые знакомятся с понятием шифров симметричной и ассиметричной криптографии, электронной подписью, хеширование и другими математическими объектами криптографии. Изучаются соответствующие криптографические стандарты, применяемые сегодня в защите информации в России и за рубежом.

Задачи дисциплины:

- дать основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов синтеза и анализа шифров; математических методов, используемых в криптоанализе;
- ознакомление с основами математической теории криптологии;
- приобретение навыков в практическом использовании, постановке и решении задач шифрования информации
- понимание сути информационных процессов в криптографических системах
- применение компьютеров для решения задач шифрования и дешифрования;
- разработка и использование математических и вычислительных моделей процессов шифрования информации, их оптимизация и выработка направлений совершенствования.

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

знать

− принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

− принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;

уметь

− устанавливать, настраивать и обслуживать программно-аппаратные средства защиты информации;

− применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования разработки и оценки защищенности компьютерных систем;

- применять современные технологии криптографии в задачах обработки информации

владеть

- научно-технической терминологией;

− методами и средствами выявления угроз безопасности автоматизированным системам;

− организации проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.

освоить компетенции:
способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)
способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

3. Место дисциплины в структуре ОП ВО

Данная дисциплина относится к базовой части Блока Б1. В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ. Дисциплина изучается на третьем курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Основы информационной безопасности», «Техническая защита информации» по направлению подготовки 10.03.01 «Информационная безопасность», квалификации - бакалавр. Кроме того, для грамотного использования полученных знаний в профессиональной деятельности, требуется изучение курсов «Математика»; «Информатика». «Основы информационной безопасности».

Курс тесно взаимосвязан с другими дисциплинами. Он является полезным для изучения таких дисциплин как «Комплексные система зашиты информации на предприятии», «Защита информации в корпоративных ИС», «Организация и управление службой защиты информации на предприятии».

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	5
Общая трудоемкость в часах	180
Аудиторные занятия в часах, в том числе:	68
Лекции	34
Практические занятия	-
Лабораторные занятия	34
Самостоятельная работа в часах	76
Форма промежуточной аттестации	экзамен

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	34
Практические занятия	-
Лабораторные занятий	34
Консультации	3,7
Зачет/зачеты	-
Экзамен/экзамены	0,35
Курсовые работы	3
Курсовые проекты	–
Всего	75,05

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	Лабораторные	
1.	Введение. Основные задачи криптологии. Криптография и криптографический анализ.	12	2	2	4
2.	Открытый и закрытый тексты, ключ основные свойства функции шифрования и дешифрования. Примеры шифров. Шифр Цезаря, Полибия	12	2	2	4
3.	Симметричные шифры. Группа подстановок и перестановок.	12	2	2	4
4.	Чистые шифры. Шифр Вижинера и Вернама. Методы криптоанализа.	12	2	2	4
5.	Одноразовый блокнот. Теорема об абсолютно стойком шифре.	12	2	2	4
6.	Принцип Керкхоффса. Проблемы симметричной криптографии.	12	2	2	4
7.	Хеш-функции и их свойства.	12	2	2	4
8.	Хеш-функции устойчивые в слабом и сильном смысле по отношению к поиску коллизий. Парадокс о днях рождениях	12	2	2	4
9.	Блочные шифры. Стандарт DES	10	2	2	4
10.	Поточные шифры. Стандарт GOST1989/ Стандарт A5	10	2	2	4
11.	Ассиметричная криптография. Классы алгоритмический сложности	10	2	2	4
12.	Сложность математических задач. Односторонние функции.	10	2	2	4
13.	Задачи факторизации и дискретного логарифмирования.	10	2	2	4
14.	Функция Эйлера. Алгоритм RSA	10	2	2	4
15.	Электронная подпись.	10	2	2	4
16.	Криптографические протоколы	10	2	2	4
17.	Протокол анонимных вычислений. Схемы разделения секрета.		2	2	4
Экзамен		36			8
Всего:		**180**	**34**	**34**	**76**

5.2. Содержание:

1. Введение. Симметричная криптография.

Основные задачи теории криптологии. Криптография и криптографический анализ. Краткая справка по истории возникновения и развития, и современному состоянию криптографии. Основные понятия криптологии. Открытый и закрытый тексты. Шифры и ключи. Канал секретной связи. Возможности противника в канале связи. Определение криптографической системы по Шеннону. Подстановки и перестановки. Примеры шифров.

Шифры Цезаря и Полибия. Двойственность подстановки и перестановки. Теорема о сохранении энтропии открытого текста. При применении подстановки и перестановки. Взлом подстановок и перестановок методами частотного анализа закрытого текста. Шифр Вижинера. Гаммирование. Шифр Вернама и одноразовый блокнот. Теорема Шеннона об абсолютно стойком шифре. Практическая стойкость шифра. Принцип Керкхоффса. Хеш-функции и их свойства. Области применения хеш-функций в криптографии. Необходимые свойства хеш-функций для использования в электронной подписи.

2. Ассиметричная криптография. Алгоритмическая сложность.

Классы алгоритмической сложности. Сложность математических задач. Односторонние функции. Задачи факторизации и дискретного логарифмирования. Функции Эйлера. Криптографическая система RSA. Электронные деньги.

3. Криптографические протоколы. Электронная подпись. Протокол Диффи-Хелмана создания симметричного ключа. МИТМ-атака на протокол. Криптографические протоколы. Протокол анонимных вычислений. Схемы разделения секрета. СРС Ади Шамира. Пороговые схемы разделения. Криптография на эллиптических кривых.

4. Криптографический анализ. Пассивный криптографический анализ. Частотный анализ. Дифференциальный и линейный криптографический анализ. Активный криптоанализ.

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) дисциплин	Задание	Методические рекомендации по выполнению задания	Форма контроля

	ы			
1	**2**	**3**	**4**	**5**
1.	Тема № 1	Усвоить	1. Изучить задачи криптографии. Литература основная[1,2]	Контрольный опрос
2.	Тема № 2	Усвоить,	1. Изучить основные понятия криптографии. Освоить применение древних шифров Цезаря Полибия. Литература основная[1,2]	Контрольный опрос
3.	Тема № 3	Приобрес-ти навык	1. Изучить свойства симметричных шифров 2. Реализовать несколько классических алгоритмов шифрования в виде программы. Литература основная[1,2], дополнительная [4]	Проверка выполнения лабораторной работы
4.	Тема № 4	Усвоить	1. Изучить понятие чистого шифра Литература основная[1,2], дополнительная [1-8]	Контрольный опрос
5.	Тема № 5	Усвоить	1. Изучить теорему об абсолютно стойком шифре Литература основная[1-6], дополнительная [1-9]	Контрольный опрос
6.	Тема № 6	Усвоить	1. Изучить принципы Керкхоффса. Оценить их актуальность на сегодняшний момент. Выделить главный из них. Литература основная[1-4], дополнительная [1-8]	Контрольный опрос
7.	Тема № 7	Приобрес-ти навык	1. Изучить понятие хеш-функций и их свойства. 2. Реализовать вычисление хеш-функции в виде программы на любом языке программирования. Литература основная[1-4], дополнительная [1-8]	Проверка выполнения лабораторной работы
8.	Тема № 8	Усвоить	1. Изучить понятие коллизии хеш-функций. Литература основная[1-4], дополнительная [1-8]	Контрольный опрос
9.	Тема № 9	Усвоить, Приобрес-ти навык	1. Изучить алгоритм шифрования DES. 2. Изучить возможности его применения. 3. Реализовать алгоритм шифрования DES самостоятельно, сравнить результаты работы алгоритма с известными решениями. Литература основная[1-4], дополнительная [1-8]	Проверка выполнения лабораторной работы
10.	Тема № 10	Усвоить	1. Изучить понятие поточных шифров Литература основная[1-4], дополнительная [1-9]	Контрольный опрос
11.	Тема № 11	Приобрес-ти навык	1. Изучить понятие ассиметричной криптографии. 2. Усвоить отличия симметричной и ассиметричной криптографии, сферы возможного применения. Литература основная[1-4], дополнительная	Контрольный опрос

			[1-8]	
12.	Тема № 12	Усвоить	1.Изучить понятие односторонней функции и односторонней функции секретом Литература основная[1-4], дополнительная [1-8]	Контрольный опрос
13.	Тема № 13	Усвоить	Познакомиться с задачами факторизации и проблемами дискретного логарифмирования больших чисел. Литература основная[1-4], дополнительная [1-8]	Контрольный опрос
14.	Тема № 14	Приобрес-ти навык	Изучить работу алгоритма RSA. Реализовать алгоритм шифрованияRSA самостоятельно. Литература основная[1-6], дополнительная [1-8]	Проверка выполнения лабораторной работы
15.	Тема № 15	Приобрес-ти навык	Изучить алгоритм вычисления электронной подписи. Изучить инфраструктуру для применения электронной подписи. Реализовать собственный алгоритм электронной подписи (подписание и проверка) Литература основная[1-4], дополнительная [1-8]	Проверка выполнения лабораторной работы
16.	Тема № 16	Приобрес-ти навык	Изучить понятие криптографического протокола. Реализовать самостоятельно протокол обмена ключами на выбор (например, CHAP) Литература основная[1-4], дополнительная [1-9]	Проверка выполнения лабораторной работы
17.	Тема № 17	Приобрес-ти навык	Изучить алгоритмы разделения секрета Литература основная[1-4], дополнительная [1-9]	Контрольный опрос

Формой отчетности по данной дисциплине является экзамен. Необходимые условия допуска к экзамену:

- Наличие полного конспекта лекций
- Сдача всех контрольных работ (3 шт) с положительным результатом

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

Не предусмотрены

6.3. Тематика и задания для лабораторных занятий

1. Классические симметричные алгоритмы шифрования. Три криптопримитива.
2. Криптоанализ классических алгоритмов. Реализовать криптоанализ по методу индекс совпадений. Реализовать криптоанализ шифра Вижинера или Гронсфельда по методу Касиськи
3. Современные симметричные алгоритмы шифрования. Реализовать 2 современный алгоритм на выбор.
4. Хеширование. Реализовать хеш функцию не криптографическую
5. Арифметика с длинными числами.
6. Ассиметричные алгоритмы шифрования. Реализовать алгоритм RSA

7. Генераторы ключей. Реализовать генератор псевдослучайной последовательности либо генератор случайной последовательности на основе считывания случайных движений пользователя.
8. Реализовать 2 метода обмена ключами.

6.4. Тематика курсовых работ

1. Исследование алгоритмов цифровой подписи
2. Реализация современных симметричных алгоритмов шифрования для применения в локальных ИС
3. Исследование потоковых алгоритмов шифрования
4. Криптоанализ современных алгоритмов шифрования с использованием распределенных систем
5. Криптоанализ современных систем шифрования локальных ИС (архивов, текстовых файлов и т.д.)
6. Оценка безопасности подсистемы защиты операционных систем
7. Криптографические генераторы случайных и псевдослучайных последовательностей чисел
8. Применение криптографических хеш-функций.
9. Исследование криптографических протоколов используемых в интернет
10. Организация обмена ключами без третьей стороны
11. Доменная авторизация Windows в стороннем приложении

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

а) основная

1. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429092
2. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.: 60х88 1/8. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-369-01304-5, 200 экз. http://znanium.com/catalog.php?bookinfo=432654
3. Кнауб, Л.В. Теоретико-численные методы в криптографии : учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=229582
4. Баричев, С. Г.
   Основы современной криптографии : Учеб. курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - 2-е изд., перераб. и доп. - М. : Горячая линия-Телеком, 2002. - 175 с. - Библиогр.: с. 160. - ISBN 5-93517-075-2 : 41.40.

б) дополнительная

1. Моделирование системы защиты информации. Практикум : учеб. пособие / Е.К. Баранова, А.В. Бабаш. — 2-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2018. — 224 с. + Доп. материалы [Электронный ресурс; Режим доступа http: //www.znanium.com]. — (Высшее образование: Бакалавриат). — DOI: https://doi.org/10.12737/18877 http://znanium.com/catalog.php?bookinfo=916068
2. Поддержка принятия решений при проектировании систем защиты информации : монография / В.В. Бухтояров, М.Н. Жукова, В.В. Золотарев [и др.]. — М. : ИНФРА-М, 2018. – 311 с. –(Научная мысль) http://znanium.com/catalog.php?bookinfo=947806

3. Актуальные вопросы защиты информации : монография / А.В. Бабаш, Е.К. Баранова. — М. : РИОР : ИНФРА-М, 2017. — 111 с. — (Научная мысль). — http://znanium.com/catalog.php?bookinfo=854634
4. Криптографические методы защиты информации : лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет» ; авт.-сост. И.А. Калмыков, Д.О. Науменко и др. - Ставрополь : СКФУ, 2015. - 109 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458059
5. Разработка моделей криптографической защиты информации : монография / В.Г. Шубович, В.В. Капитанчук, Н.С. Знаенко, Ю.И. Титаренко ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Ульяновский государственный педагогический университет имени И.Н. Ульянова». - Ульяновск : УлГПУ, 2013. - 128 с. : схем. - Библиогр.: с. 108-112. - ISBN 978-5-86045-640-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=278070
6. Применение искусственных нейронных сетей и системы остаточных классов в криптографии : [монография] / Н. И. Червяков [и др.]. - М. : ФИЗМАТЛИТ, 2012. - 279, [1] с. - Библиогр. в конце глав. - ISBN 978-5-9221-1386-1 : 250.00.
7. Бабенко, Людмила Климентьевна Параллельные алгоритмы для решения задач защиты информации / Л. К. Бабенко, Е. А. Ищукова, И. Д. Сидоров. - М. : Горячая линия-Телеком, 2014. - 304 с. : ил. - Библиогр.: с. 222-224. - ISBN 978-5-9912-0426-2 : 340.00.
8. Малюк, А. А. Введение в защиту информации в автоматизированных системах : Учеб. пособие для студ. / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - 2-е изд. - М. : Горячая линия-Телеком, 2004. - 147 с. : ил. - (Учебное пособие для высших учебных заведений). - Библиогр.: с. 143-145. - ISBN 5-93517-062-0 : 45.75. Допущено УМО

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.
Компьютерный класс 9 персональных компьютеров