МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Утверждено:
на заседании кафедры
протокол № 5 от 25.01. 2021 г.

Зав. кафедрой _____/*Хабибуллин Б.Н.*/

Согласовано:
Председатель УМК факультета математики и информационных технологий

_____/ Ефимов А.М.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

дисциплина Криптографические методы защиты информации

Часть, формируемая участниками образовательных отношений

программа бакалавриата

Направление подготовки (Специальность)
02.03.01 Математика и компьютерные науки
(шифр, название направления)

Направленность (профиль) подготовки
Математическое и компьютерное моделирование

Квалификация
бакалавр

Разработчики (составители)	
доцент, к.ф.-м.н., доцент	_____ Цыганов Ш.И.
ассистент	_____ Белова А.С.

Для приёма: 2021

Уфа 2021 г.

Составитель: к.ф.-м.н., доцент кафедры высшей алгебры и геометрии Ш.И. Цыганов, ассистент кафедры высшей алгебры и геометрии А.С. Белова.

Рабочая программа дисциплины актуализирована на заседании кафедры высшей алгебры и геометрии протокол от «25» января 2021 г. №_5

Дополнения и изменения, внесённые в рабочую программу дисциплины, утверждены на заседании кафедры высшей алгебры и геометрии: обновлён фонд оценочных средств. протокол № 5 от «25» января 2021 г.

Заведующий кафедрой  / Б.Н. Хабибуллин/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций
2. Цель и место дисциплины в структуре образовательной программы
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)
4. Фонд оценочных средств по дисциплине

   4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

   4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.
5. Учебно-методическое и информационное обеспечение дисциплины

   5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

   5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	ПК-1. Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	ПК-1.1 Обладает базовыми знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий.	Знать: современную научно-техническую литературу в области криптографической защиты
		ПК-1.2 Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в математике и информатике.	Уметь: Систематизировать нормативно-правовую документацию в области криптографии
		ПК-1.3 Имеет практический опыт научно-исследовательской деятельности в математике информатике.	Владеть: Навыками изучения научно-технической информации, в том числе на иностранном языке

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Криптографические методы защиты информации» относится к части, формируемой участниками образовательных отношений.

Дисциплина изучается на 3 курсе в 6 семестре.

Цель дисциплины «Криптографические методы защиты информации» - сформировать терминологический фундамент в области криптографии, методологические основы применения криптографической защиты в современных системах связи и телерадиовещания, навыки практического использования криптографических протоколов и алгоритмов.

Задачи изучения дисциплины - дать основы: 1) системного подхода к организации

защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических методов; 2) принципов синтеза и анализа криптосистем; 3) математических методов, используемых для оценки стойкости криптосистем.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения школьного курса алгебры и начала анализа, геометрии и информатики. Компетенции, сформированные при изучении дисциплины «Криптографические методы защиты информации», используются при изучении следующих дисциплин: Уравнение пьезопроводности в задачах нефтедобычи, Компьютерные методы решения задач комплексного анализа, Методы сжатия данных и помехозащитное кодирование и иное.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

Код и формулировка компетенции ПК-1. Способен консультировать и использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в профессиональной деятельности

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-1.1 Обладает базовыми знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий.	,Знать: современную научно-техническую литературу в области криптографической защиты	Отсутствие знаний современной научно-технической литературы в области криптографической защиты	Частичные знания современной научно-технической литературы в области криптографической защиты	Полные и четкие, но содержащие отдельные пробелы знания современной научно-технической литературы в области криптографической защиты	Полные и четкие знания современной научно-технической литературы в области криптографической защиты
ПК-1.2 Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в математике и информатике.	Уметь: Систематизировать нормативно-правовую документацию в области криптографии	Отсутствие умений систематизировать нормативно-правовую документацию в области криптографии	Фрагментарные умения систематизировать нормативно-правовую документацию в области криптографии	В целом успешные, но содержащие отдельные пробелы умения систематизировать нормативно-правовую документацию в области криптографии	Сформированное умение систематизировать нормативно-правовую документацию в области криптографии

ПК-1.3 Имеет практический опыт научно-исследовательской деятельности в математике информатике.	Владеть: Навыками изучения научно-технической информации, в том числе на иностранном языке	Отсутствие готовности использовать навыки изучения научно-технической информации, в том числе на иностранном языке	В целом успешная, но не систематическая готовность использовать навыки изучения научно-технической информации, в том числе на иностранном языке	В целом успешная, но содержащая отдельные пробелы готовность навыки изучения научно-технической информации, в том числе на иностранном языке	Успешная готовность использовать навыки изучения научно-технической информации, в том числе на иностранном языке

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ПК-1.1 Обладает базовыми знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий.	,Знать: современную научно-техническую литературу в области криптографической защиты	Контрольная работа, Лабораторная работа
ПК-1.2 Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в математике и информатике.	Уметь: Систематизировать нормативно-правовую документацию в области криптографии	Контрольная работа, Лабораторная работа
ПК-1.3 Имеет практический опыт научно-исследовательской деятельности в математике информатике.	Владеть: Навыками изучения научно-технической информации, в том числе на иностранном языке	Контрольная работа, Лабораторная работа

Критериями оценивания при *модульно-рейтинговой системе* являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (*для экзамена:* текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; *для зачета:* текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

(*для экзамена:*

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины

Криптографические методы защиты информации

Направление подготовки *02.03.01 Математика и компьютерные науки*

курс 3, семестр 6

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Обзор современных систем шифрования Основные операции, используемые в современных алгоритмах шифрования Современные симметричные системы шифрования (блочные и поточные)				
Текущий контроль			**0**	**10**
1. Аудиторная работа, работа на семинаре	**0,5**	**12**	**0**	**6**
2.Домашняя работа	**0,5**	**8**	**0**	**4**
Рубежный контроль			**0**	**10**
Контрольная работа, Лабораторная работа	**2,5**	**4**	**0**	**10**
Модуль 2. Режимы использования блочных шифров. Требования к поточным шифрам. Универсальные методы криптоанализа.				
Текущий контроль			**0**	**13**
1. Аудиторная работа	**0,5**	**16**	**0**	**8**
2.Домашняя работа	**0,5**	**10**	**0**	**5**
Рубежный контроль			**0**	**12**
Контрольная работа, Лабораторная работа	**2,4**	**5**	**0**	**12**
Модуль 3. Математика для систем с открытым ключом. Алгоритм шифрования RSA. Алгоритмы асимметричного шифрования, основанные на задаче дискретного логарифмирования				
Текущий контроль			**0**	**13**
1. Аудиторная работа, работа на семинаре	**0,5**	**16**	**0**	**8**
2.Домашняя работа	**0,5**	**10**	**0**	**5**
Рубежный контроль			**0**	**12**
Контрольная работа, Лабораторная работа	**3**	**4**		**12**
Поощрительные баллы				
1. Студенческая олимпиада или конкурс рефератов			**0**	**5**
2. Волонтерская работа при проведении олимпиад и конференций			**0**	**5**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			**0**	**-6**
2. Посещение практических (семинарских, лабораторных занятий)			**0**	**-10**

Итоговый контроль				
Экзамен			**0**	**30**
Итого			**45**	**100**

Экзаменационные билеты

Структура экзаменационного билета: экзаменационный билет состоит из трех теоретических вопросов.

Примерные вопросы для экзамена:

1. История развития криптографии

2. Основные понятия

3. Модели шифров и открытых текстов. Критерии распознавания открытых текстов

4. Шифры замены. Обобщенная модель. Алгоритм Якобсона.

5. Шифры перестановки и методы их вскрытия.

6. Дисковые шифры.

7. Шифры гаммирования. Возможность восстановления вероятности знаков гаммы. Восстановление текстов при неравновероятной гамме.

8. Повторное использование гаммы. Использование неисправности в реализации шифра Вернама.

9. Криптоанализ шифра Виженера. Ошибка шифровальщика (пропуск участка открытого текста).

10. Энтропия. Избыточность. Формула неопределенности шифра по ключу. Теорема о числе ложных ключей. Расстояние единственности

11. Стойкость шифров. Виды криптоатак. Совершенный шифр. Утверждение о совершенном шифре. Теорема Шеннона о совершенном шифре. Примеры совершенных шифров. Практическая стойкость.

12. Имитостойкость. Совершенная имитостойкость. Помехоустойчивость. Шифры, не распространяющие искажений, изометрии. Теорема Маркова

13. Статистика в криптографии.

14. Тесты на случайность битовой последовательности.

15. Сети Фейстеля. Схема шифрования DES. 3DES, DESX. 4 основных режима блочного шифрования.

16. Схема шифрования ГОСТ – 28147-89. Различия между DES и ГОСТ.

17. Шифр AES.

18. Понятие булевой функции. Виды представлений булевой функции (СДНФ, СКНФ, многочлен Жегалкина, многочлен с действительными коэффициентами, ряд Фурье).

19. Понятие статистического аналога и статистической структуры двоичной функции. Определение статистической структуры методом быстрого преобразования Фурье. Линейный криптоанализ.

20. Понятие вероятностной функции. k-выравнивающая и k-равновероятная двоичная функция. Понятие совершенной нелинейности.

21. Определение ЛРП. Понятие генератора и минимального многочлена ЛРП. Формула вычисления минимального многочлена через характеристический многочлен и генератор ЛРП.

22. Длина подхода и период последовательности и многочлена над полем. Критерий примитивности неприводимого многочлена. Теорема о случайности к-грамм в ЛРП максимального периода

23. Синхронные системы и системы с самосинхронизацией. Принципы построения поточных систем. Управляющий и шифрующий блоки. Линейный конгруэнтный генератор. Генераторы с неполиномиальной зависимостью. ЛРС. Требования к управляющему блоку и шифрующему блоку.

24. Схема шифрсистемы А5. Шифрсистема Гиффорда. Фильтрующие генераторы. Комбинирующие генераторы

25. Композиция ЛРС. Схемы с динамическим изменением закона рекурсии. Генераторы Макларена-Марсальи

Образец экзаменационного билета:

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ВЫСШЕЙ АЛГЕБРЫ И ГЕОМЕТРИИ

Экзаменационный билет №1
по дисциплине «Криптографические методы защиты информации »

1. Схема шифрования ГОСТ – 28147-89. Различия между DES и ГОСТ. (10 баллов)
2. Композиция ЛРС. Схемы с динамическим изменением закона рекурсии. Генераторы Макларена-Марсальи (10 баллов)
3. Определение ЛРП. Понятие генератора и минимального многочлена ЛРП (10 баллов)

Зав. кафедрой Хабибуллин Б.Н.. /_____/

Перевод оценки из 100-балльной в четырехбалльную производится следующим образом:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов);

- хорошо – от 60 до 79 баллов;

- удовлетворительно – от 45 до 59 баллов;

- неудовлетворительно – менее 45 баллов.

Критерии оценки (в баллах):

- 25-30 баллов *выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;*

- 17-24 баллов *выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки;*

- 10-16 *баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент не решил задачу или при решении допущены грубые ошибки;*

- 1-10 баллов *выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.*

В 6 семестре студенту представляется 1 лабораторная работа. Первая лабораторная работа состоит тестового задания, на каждое задание студент должен привести пример. В случае, если студент не справляется с более 50% заданий по всем лабораторным работам, он не допускается к сдаче экзамена. У каждого студента есть возможность пересдать лабораторную работу.

Лабораторная работа №1

1. Конфиденциальность защищаемой информации обеспечивается с помощью...
   - электронной подписи
   - шифрования
   - хэш-функции

2. Способность шифра противостоять попыткам противника по имитации или подмене зашифрованной информации называется
   - имитостойкостью.
   - криптостойкостью.
   - помехозащищенностью.

3. Если криптоаналитик может взломать шифр, но не обладает необходимыми вычислительными ресурсами, то считается, что
   - шифр является практически стойким.
   - шифр является теоретически стойким.
   - шифр является практически имитостойким.

4. Если для шифрования и расшифрования используется один и тот же ключ, то шифр является
   - симметричным.
   - ассиметричным.
   - блочным.

5. Шифры, в которых знание ключа шифрования не позволяет определить ключ расшифрования называются
- поточными.
- симетричными.
- ассиметричными.

6. Шифры, в которых каждый символ открытого текста зашифровывается независимо от других называются
- блочными.
- имитозащищенными.
- поточными.

7. Шифрование информации предназначено для обеспечения
- целостности защищаемой информации
- конфиденциальности защищаемой информации
- доступности защищаемой информации

8. Исходные данные с доступным семантическим содержанием, подлежащие криптографическому преобразованию, называются
- открытый текст
- шифртекст
- имитовставка

9. Параметр шифра, определяющий выбор конкретного варианта преобразования зашифрования или расшифрования из множества преобразований, составляющих шифр, называется…
- алгоритм
- шифр
- ключ

10. Процесс преобразования шифртекста в открытый текст при неизвестном ключе называется…
- дешифрование
- зашифрование
- расшифрование

11.Если за один такт шифрования преобразованию подвергается группа знаков открытого текста, то такой шифр называется
- блочным
- поточным
- ассиметричным

12. На основе сети Фейстеля построен алгоритм шифрования
- AES
- ГОСТ 28147
- RC4

13. Режим использования блочного шифра, при котором блочный шифр может использоваться как поточный называется
- режим простой замены со сцеплением.
- режим гаммирования с обратной связью
- режим простой замены.

14. Режим простой замены заключается в обработке блоков открытого текста независимо от других обработку блоков открытого текста в зависимости от результата зашифрования
- предыдущего блока
- обработку блоков открытого текста в режиме наложения гаммы

15. Шифр называется блочным, если…
- за один такт шифрования преобразованию подвергается группа знаков открытого текста
- за один такт шифрования преобразованию подвергается один знак открытого текста
- группа знаков открытого текста преобразуется за несколько тактов шифрования

16. Если управляющая гамма поточного шифра зависит только от ключа и не зависит от открытого текста и шифротекста, то такой шифр называется
- синхронным.
- самосинхронизирующимся.
- независимым.

17. Достоинством поточных шифров по сравнению с блочными является
- наличие открытого ключа
- высокая стоимость реализации
- высокая скорость работы

18 Недостатком генераторов псевдослучайных последовательностей является
- сложность реализации
- зависимость от параметров окружающей среды
- периодичность последовательности

19. Если управляющая гамма поточного шифра зависит от ключа и от открытого текста и шифротекста, то такой шифр называется
- синхронным.
- самосинхронизирующимся.
- независимым.

20. В алгоритме ГОСТ 34.12-15 размера блока составляет
- 64 бита
- 128 бит, 192 бита и 256 бит
- 64 бита и 128 бит

Критерии оценки (в баллах*)*
Лабораторная работа №1
20 баллов выставляется студенту, если верно решены все задания;
10 баллов выставляется студенту, если верно решено 1 задание;

В 6 семестре запланирована курсовая работа.

Примерные темы курсовой работы:

1. Программная реализация шифров замены.
2. Программная реализация шифров перестановки.
3. Программная реализация шифра Плейфера.
4. Программная реализация шифра Хилла.
5. Разработка шифра, основанного на композиции шифра замены и перестановки, с оценкой его криптостойкости.
6. Анализ криптостойкости блочных криптосистем (ГОСТ 28147-89, DES, IDEA, AES).
7. Алгоритм электронной цифровой подписи на основе решения системы сравнений.
8. Анализ методов сокращения длины электронной цифровой подписи.
9. Алгоритмы коллективной электронной цифровой подписи.

10. Алгоритмы композиционной электронной цифровой подписи.

11. Сравнительный анализ современных программных, программно-аппаратных и аппаратных средств криптографической защиты информации.

12. Разработка схемы криптографического генератора, основанного на комбинировании LFSR-генераторов, с оценкой его качества.

13. Разработка схемы криптографического генератора, основанного на комбинировании конгруэнтных генераторов, с оценкой его качества.

14. Оценка качества криптографических генераторов, основанных на алгоритмах Фибоначчи.

Критерии оценки:

Оценка «отлично» выставляется, если

- Курсовая работа выполнена,
- Тема полностью раскрыта,
- Охвачен весь круг вопросов по теме курсовой,
- Приведено достаточное количество примеров.

Оценка «хорошо» выставляется, если

- Курсовая работа выполнена,
- Тема полностью раскрыта,
- Охвачен весь круг вопросов по теме курсовой,
- Приведено недостаточное количество примеров.

Оценка «удовлетворительно» выставляется, если

- Курсовая работа выполнена,
- Тема не полностью раскрыта,
- Охвачен не весь круг вопросов по теме курсовой,
- Приведено недостаточное количество примеров

Оценка «неудовлетворительно» выставляется, если курсовая работа не выполнена.

1. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Орлов, В.А. Теория чисел в криптографии [Электронный ресурс]: учебное пособие / В.А. Орлов, Н.В. Медведев, Н.А. Шимко, А.Б. Домрачева. — Электрон. дан. — Москва: МГТУ им. Н.Э. Баумана, 2011. — 223 с. — Режим доступа: https://e.lanbook.com/book/106532.

2. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс]: монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва: Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: https://e.lanbook.com/book/5192.

3. Панкратова, И.А. Булевы функции в криптографии [Электронный ресурс]: учебное пособие / И.А. Панкратова. — Электрон. дан. — Томск: ТГУ, 2014. — 88 с. — Режим доступа: https://e.lanbook.com/book/76702.

4. Серёдкин, А.Н. Основы защиты информации и информационные технологии. В 3 частях. Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ

[Электронный ресурс]: учебное пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза: ПензГТУ, 2013. — 180 с. — Режим доступа: https://e.lanbook.com/book/62755

Дополнительная литература

1. Серёдкин, А.Н. Основы защиты информации и информационные технологии. В 3 частях. Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ [Электронный ресурс]: учебное пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза: 9 ПензГТУ, 2013. — 180 с. — Режим доступа: https://e.lanbook.com/book/62755. 2. Боровков А.А. Математическая статистика. М.: «Наука», 1984.
2. Кукина, Е.Г. Введение в криптографию: сборник задач и упражнений [Электронный ресурс] / Е.Г. Кукина, В.А. Романьков. — Электрон. дан. — Омск: ОмГУ, 2013. — 91 с. — Режим доступа: https://e.lanbook.com/book/75394

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1	Электронно-библиотечная система «ЭБ БашГУ»	Собственная электронная библиотека учебных и научных электронных изданий, которая включает издания преподавателей БашГУ	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация в Библиотеке БашГУ, дальнейший доступ из любой точки сети Интернет	https://elib.bashedu.ru/
2	Электронно-библиотечная система «Университетская библиотека online»	Полнотекстовая БД учебных и научных электронных изданий	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация из сети БашГУ, дальнейший доступ из любой точки сети Интернет	http://www.biblioclub.ru/
3	Электронно-библиотечная система издательства «Лань»	Полнотекстовая БД учебных и научных электронных изданий	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация из сети БашГУ, дальнейший доступ из любой точки сети Интернет	http://e.lanbook.com/

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1. ***учебная аудитория для проведения занятий лекционного типа:*** аудитории № 530, 528 (физмат корпус - учебное). **2.** ***учебная аудитория для проведения занятий семинарского типа:*** аудитории № 511, 531 (физмат корпус - учебное). **3.** ***учебная аудитория для курсового проектирования (выполнения курсовых работ):*** аудитории № 511, 517, 531 (физмат корпус - учебное). **4.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитории № 530, 511, 517 (физмат корпус - учебное). ***5. учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитории № 530, 511, 517 (физмат корпус - учебное). **6.** ***помещения для самостоятельной работы:*** читальный зал № 1 (главный корпус).	**Аудитория № 511:** Учебная мебель, доска настенная меловая, мультимедиа проектор Mitsubishi EX 320U 3D 2.4кг., экран на штативе DraperDiplomat (1:1) 84/84* 213*213 MW , компьютер в составе: системный блок DEPO 460MD/3-540/T500G/DVD-RW, монитор 20. **Аудитория № 517:** Учебная мебель, доска настенная меловая, мультимедиа-проектор Sony VPL-EX120, XGA, 2600 ANSI, 3,2 кг, экран настенный Projecta SlimScreen 200*200 cm Matte White, потолочное крепление для проектора, доска аудитор.ДА32. **Аудитория № 528:** Учебная мебель, доска настенная меловая. **Аудитория № 530:** Учебная мебель, доска настенная меловая. **Аудитория № 531:** Учебная мебель, доска настенная меловая, мультимедиа-проектор Sony VPL-EX120, XGA, 2600 ANSI, 3,2 кг, потолочное крепление для проектора (2101068302), доска аудитор.ДА32. **Читальный зал №2:** Учебная мебель, учебно-наглядные пособия, стенд по пожарной безопасности, моноблоки стационарные – 8 шт, принтер – 1 шт., сканер – 1 шт.	1. Windows 8 Russian. Windows Professional 8 Russian Upgrade. Договор № 104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian. Договор № 114 от 12.11.2014 г. Лицензии бессрочные.

Приложение № 1

МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Криптографические методы защиты информации на 6 семестр
(наименование дисциплины)

очная
форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (з.е. / часов)	3 / 108
Учебных часов на контактную работу с преподавателем:	
лекций	16
практических/ семинарских	
лабораторных	16
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	3.2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	2,2
Учебных часов на самостоятельную работу обучающихся (СР)	38
из них, предусмотренные на выполнение курсовой работы / курсового проекта	20
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	34,8

Форма(ы) контроля:
Экзамен 6 семестр
Курсовая работа 6 семестр

№ п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР/СЕМ	ЛР	СР		
1	2	3	4	5	6	8	9
1.	Модуль 1. Обзор современных систем шифрования Основные операции, используемые в современных алгоритмах шифрования Современные симметричные системы шифрования (блочные и поточные)	8		4	16	[3]: Гл.5, §20-22	Контрольная работа, Лабораторная работа, экзамен
2.	Модуль 2. Режимы использования блочных шифров. Требования к поточным шифрам. Универсальные методы криптоанализа.	4		4	11	[3]: Гл.2, §8, Гл.3, §9-15	Контрольная работа, Лабораторная работа, экзамен
3.	Модуль 3. Математика для систем с открытым ключом. Алгоритм шифрования RSA. Алгоритмы асимметричного шифрования, основанные на задаче дискретного логарифмирования.	4		8	11	[3]: Гл.4, §17-19	Контрольная работа, Лабораторная работа, экзамен
	Всего часов:	16		16	38		