

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Луковникова Елена Ивановна
Должность: Проректор по учебной работе
Дата подписания: 16.11.2021 10:50:13
Уникальный программный ключ:
890f5aae3463de1924cbcf76ac5d7ab89e9fc7d3

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"



УТВЕРЖДАЮ

Проректор по учебной работе

E.I. Lukovnikova
19 мая

Е.И.Луковникова

20 21 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.09.01 Криптографические методы защиты информации

Закреплена за кафедрой **Информатики, математики и физики**

Учебный план b010302_21_ИПО.plx

Направление: 01.03.02 Прикладная математика и информатика

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **7 ЗЕТ**

Виды контроля в семестрах:

Экзамен 5,6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	5 (3.1)		6 (3.2)		Итого	
	уп	рп	уп	рп		
Неделя	17		16			
Вид занятий	уп	рп	уп	рп	уп	рп
Лекции	17	17	32	32	49	49
Лабораторные			32	32	32	32
Практические	34	34			34	34
В том числе инт.	16	16	12	12	28	28
Итого ауд.	51	51	64	64	115	115
Контактная работа	51	51	64	64	115	115
Сам. работа	3	3	44	44	47	47
Часы на контроль	54	54	36	36	90	90
Итого	108	108	144	144	252	252

Программу составил(и):

к.т.н., доц., Сташок Ольга Владимировна

Сташок

Рабочая программа дисциплины

Криптографические методы защиты информации

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 9)

составлена на основании учебного плана:

Направление: 01.03.02 Прикладная математика и информатика

утвержденного приказом ректора от 01.03.2021 протокол № 80.

Рабочая программа одобрена на заседании кафедры

Информатики, математики и физики

Протокол от 16 апреля 2021 г. № 9

Срок действия программы: 2021-2025 уч.г.

Зав. кафедрой Горохов Денис Борисович

ДБ

Председатель МКФ

старший преподаватель Латушкина С.В.

18 апреля 2021 г. Л

Ответственный за реализацию ОПОП

ДБ
(подпись)

Горохов Д.Б.
(ФИО)

Директор библиотеки

Солнц
(подпись)

Солнц Е.В.
(ФИО)

№ регистрации

36
(методический отдел)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	ознакомление студентов с основополагающими принципами криптографических методов и алгоритмов защиты информации; с особенностями применения соответствующих криптосистем; изучение принципов защиты информации с помощью криптографических методов и способов; приобретение практических способов применения знаний на практике в области информационной безопасности.
-----	---

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:		Б1.В.09.01
2.1	Требования к предварительной подготовке обучающегося:	
2.1.1	Математическое моделирование	
2.1.2	Теория вероятностей и математическая статистика	
2.1.3	Языки и методы программирования	
2.1.4	Средства СУБД	
2.1.5	Операционные системы	
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
2.2.1	Выполнение и защита выпускной квалификационной работы	
2.2.2	Производственная (преддипломная) практика	
2.2.3	Технические и программные средства защиты информации	
2.2.4	Основы проектирования программных комплексов	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Индикатор 1	УК-2.1 Формулирует в рамках поставленной цели проекта совокупность задач, обеспечивающих ее достижение
Индикатор 2	УК-2.2 Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения

ПК-1 : Способен разрабатывать процедуры документирования, интеграции, преобразования программных модулей, миграции и конвертации данных согласно срокам выполнения поставленных задач

Индикатор 1	ПК-1.1 Использует выбранную среду программирования для разработки процедур интеграции программных модулей согласно срокам выполнения поставленных задач
Индикатор 2	ПК-1.2 Применяет методы и средства разработки процедур для развертывания программного обеспечения, миграции и преобразования данных

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	способы достижения результатов в рамках поставленной цели; действующие правовые нормы, ресурсы, ограничения при решении задач в предметной области; проводить анализ поставленной цели и формулировать задачи, необходимые для ее достижения; анализировать альтернативные варианты; языки, утилиты и среды программирования, средства пакетного выполнения процедур; методы и средства разработки программного обеспечения, миграции и преобразования данных.
3.2	Уметь:
3.2.1	проводить анализ поставленной цели и формулировать задачи, необходимые для ее достижения; выбирать оптимальные способы решения задач предметной области в профессиональной деятельности с учетом действующих правовых норм, ресурсов и ограничений; анализировать альтернативные варианты; внедрять и адаптировать программные модули согласно срокам выполнения поставленных задач; использовать процедуры для развертывания программного обеспечения, миграции и преобразования данных.
3.3	Владеть:
3.3.1	методиками разработки цели и задач проекта; приемами планирования решения задач предметной области; навыками проектирования решения конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений; навыками программирования в современных средах; современными языками программирования; современными технологиями разработки, внедрения, адаптации и настройки программного обеспечения и информационных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
-------------	-------------	-----------------------------	----------------	-------	-------------	------------	------------	------------

	Раздел	Раздел 1. Введение в криптографию. Математические операции в криптографии.						
1.1	Лек	Основные понятия, обозначения и задачи криптографии. Виды информации, подлежащей шифрованию. Исторические примеры криптосистем.	5	1	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.2	Пр	Основные принципы криптографической защиты информации. Функции шифрования. Односторонние функции.	5	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.3	Ср	Простейшие шифры и их классификация	5	1	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.4	Лек	Совершенные шифры.	5	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	4	Лекция - беседа УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.5	Пр	Симметричные криптосистемы. Метод простой подстановки (замены). Метод перестановки. Метод блочных шифров. Метод гаммирования. Метод шифрования на основе теоремы Эйлера-Ферма. Композиция шифров. Стандарт криптосистемы США DES.	5	10	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	4	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.6	Ср	Стандарт крипто-системы России – ГОСТ 28147-89.	5	1	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.7	Экзамен	Симметричные криптосистемы.	5	14	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.8	Лек	Основные требования к шифрам, к криптографическим системам. Криптостойкость шифров.	5	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	4	Лекция - беседа УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.9	Пр	Системы защиты с открытым ключом. Криптосистема RSA.	5	6	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.10	Ср	Теоретико-числовые алгоритмы и их сложность.	5	1	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
1.11	Экзамен	Системы защиты с открытым ключом.	5	16	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
	Раздел	Раздел 2. Системы шифрования						
2.1	Лек	Системы симметричного шифрования	5	6	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2

2.2	Пр	Системы симметричного шифрования	5	6	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	4	Работа в малых группах УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
2.3	Экзамен	Системы симметричного шифрования	5	18	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
2.4	Лек	Системы асимметричного шифрования	5	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
2.5	Пр	Системы асимметричного шифрования	5	8	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
2.6	Экзамен	Системы асимметричного шифрования	5	6	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
	Раздел	Раздел 3. Симметричные криптосистемы						
3.1	Лек	Основные принципы современных симметричных алгоритмов. Поточные шифры.	6	8	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
3.2	Лаб	Блочные шифры. Причины ненадежности криптосистем. Принцип Керкхоффа для криптосистемы.	6	8	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
3.3	Экзамен	Поточные шифры. Блочные шифры.	6	24	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
3.4	Лек	Генераторы псевдослучайных чисел. Важность подбора параметров.	6	8	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
3.5	Лаб	Статичный ключ. Эфемерный ключ. Компрометация ключа. Реализация процедуры распределения ключей.	6	8	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	4	Работа в малых группах УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
3.6	Ср	Протоколы распределения секретных ключей.	6	24	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
3.7	Экзамен	Реализация процедуры распределения ключей.	6	12	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
	Раздел	Раздел 4. Криптографические системы с открытым ключом						
4.1	Лек	Формула Эйлера. Основные алгоритмы вычисления НОД.	6	5	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
4.2	Лаб	Китайская теорема об остатках. Односторонние функции.	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
4.3	Ср	Односторонние функции.	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2
4.4	Лек	Шифр RSA.	6	3	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК-2.2 ПК-1.1 ПК-1.2

4.5	Лаб	Цифровая подпись. Система электронного голосования.	6	2	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК- 2.2 ПК-1.1 ПК-1.2
	Раздел	Раздел 5. Криптографические системы, основанные на физических механизмах защиты информации.						
5.1	Лек	Криптографические системы, основанные на физических механизмах защиты информации.	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	4	Лекция - беседа УК- 2.1 УК-2.2 ПК-1.1 ПК- 1.2
5.2	Лаб	Типы, приемы и методы кодирования информации.	6	8	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	4	Работа в малых группах УК- 2.1 УК-2.2 ПК-1.1 ПК- 1.2
5.3	Ср	Криптографические системы, основанные на физических механизмах защиты информации.	6	8	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК- 2.2 ПК-1.1 ПК-1.2
5.4	Лек	Введение в криптографию и криптографические протоколы.	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК- 2.2 ПК-1.1 ПК-1.2
5.5	Лаб	Теория криптографических протоколов. Практические криптопротоколы.	6	4	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК- 2.2 ПК-1.1 ПК-1.2
5.6	Ср	Практические криптопротоколы.	6	8	УК-2 ПК-1	Л1.1 Л1.2 Л1.3Л2.1Л3. 1	0	УК-2.1 УК- 2.2 ПК-1.1 ПК-1.2

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии с использованием активных методов обучения (лекция – беседа, лекция – дискуссия, проблемная лекция, лекция-визуализация, лекция с заранее запланированными ошибками, лекция – пресс-конференция, лекция с разбором конкретных ситуаций, лекция-консультация, занятия с применением затрудняющих условий, методы группового решения творческих задач, метод развивающейся кооперации)

Технология коллективного взаимодействия (работа в малых группах) (самостоятельное изучение обучающимися нового материала посредством сотрудничества в малых группах, дает возможность всем участникам участвовать в работе, практиковать навыки сотрудничества, межличностного общения)

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

Тестовое задание для проведения текущего контроля знаний.

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.
 - симметричными.
 - 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
6.2. Темы письменных работ	
не предусмотрено	
6.3. Фонд оценочных средств	
<p>Экзаменационные вопросы как средство контроля усвоения материала в виде комплекта вопросов по всем темам. Экзаменационные вопросы - 5 семестр</p> <p>Раздел 1. Введение в криптографию. Математические операции в криптографии. 1. Определение и основные понятия криптографии. Алгоритм шифрования. 2. Периоды развития шифровального дела. Древние шифры (не меньше 5). 3. Криптография в России. Основные требования к шифрам. 4. Надежность шифра. Имитостойкость и помехоустойчивость шифров. 5. Алгоритмы. Свойства алгоритмов. Требования к алгоритмам. 6. Симметричные криптосистемы (определение, схема, достоинства и недостатки).</p> <p>Раздел 2. Системы шифрования. 7. Простая перестановка. Одиночная перестановка по ключу. Магический квадрат. 8. Блочные шифры. Поточные шифры. Атаки на шифры (3 вида) 9. Режимы работы блочного шифра: ECB и CBC (описание, формула и чертеж). 10. Режимы работы блочного шифра: CFB и OFB (описание, формула и чертеж). 11. Шифр Виженера. Шифр Вернама. Шифр DES. 12. ГОСТ 28147-89 (4 режима, схемы, достоинства и недостатки).</p> <p>Экзаменационные вопросы - 6 семестр</p> <p>Раздел 3. Симметричные криптосистемы 1. Шифр AES. Протоколы: Широкооротой лягушки, Отвэй-Риса и Цербер. 2. Асимметричные криптосистемы (определение, схема, свойства, достоинства и недостатки). 3. Возможности взлома ас. шифров. Квантовая криптография. 4. Шифр RSA (схема, способы взлома). Обмен ключами Диффи-Хелмана. 5. Шифр Эль Гамала. Шифр Рабина. 6. Хэш-функции (определение, назначение, условия использования). 7. Электронная цифровая подпись. Подпись и проверка подписи. Алгоритмы ЭЦП. 8. Подпись RSA. Подпись DSS. подпись ГОСТ Р 34.10-2001. 9. Хэш протокол MD4 и MDC. 10. Хэш протокол MD5 и RIPEMD.</p> <p>Раздел 4. Криптографические системы с открытым ключом 11. Криптосистема с секретным ключом. Принцип Керкхоффа. Поточные и блочные шифры. 12. Поточные шифры. Генератор ключевого потока. Свойства генератора ключевого потока. Генератор псевдослучайных чисел, основанный на использовании алгебраических свойств M-последовательностей 13. Статистические тесты генераторов ключевого потока. 14. Блочные шифры. Алгоритм DES. Перестановки. Раунды. Алгоритм Фейстеля при шифровании и дешифровании. 15. Сравнение блочных и поточных шифров. Методы организации процедуры исправления ошибок. 16. Статичный ключ. Эфемерный ключ. Распределение ключей. Основные пути решения проблемы распределения ключей. (физические методы, Протоколы с секретным ключом, Протоколы с открытым ключом, современные физические методы). 17. Разделение секрета. Схема порогового разделения секрета. (T, W) - пороговая схема Шамира. 18. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Барроуза. 19. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Нидхейма-Шредера 20. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Отвэй-Риса. 21. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Цербер. 22. Арифметика остатков. Сравнение по модулю. Решение уравнения $ax = b \pmod{N}$. 23. Функция Эйлера. Мультипликативные обратные по модулю N. Теорема Лагранжа. Малая теорема Ферма. Применение в криптографии. 24. Алгоритм Евклида. Китайская теорема об остатках. Расширенный алгоритм Евклида. Применение в криптографии. 25. Криптосистема с открытым ключом. Криптографическая односторонняя функция. Важнейшие криптографические односторонние функции.</p> <p>Раздел 5. Криптографические системы, основанные на физических механизмах защиты информации. 26. Оценка сложности задач. Сложность алгоритма: Полиномиальная, экспоненциальная, субэкспоненциальная Оракул. Сравнительный анализ сложности криптографических алгоритмов (без доказательства). 27. Алгоритм RSA. Шифрование в RSA. Дешифрование в RSA. Доказательство алгоритма.</p>	
6.4. Перечень видов оценочных средств	
тестовое задание;	

отчеты по лабораторным занятиям;
отчеты по практическим работам;
экзаменационные вопросы.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
ЛП.1	Котов Ю. А.	Криптографические методы защиты информации: шифры: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2016	1	http://biblioclub.ru/index.php?page=book&id=576379
ЛП.2	Котов Ю. А.	Криптографические методы защиты информации: стандартные шифры. Шифры с открытым ключом: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2017	1	http://biblioclub.ru/index.php?page=book&id=574782
ЛП.3	Кирпичнико в А. П., Хайбуллина З. М.	Криптографические методы защиты компьютерной информации: учебное пособие	Казань: Казанский научно-исследовательский технологический университет (КНИТУ), 2016	1	http://biblioclub.ru/index.php?page=book&id=560536

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
ЛП.1	Левин М.	Криптография без секретов: Руководство пользователя	Москва: Новый издательский дом, 2005	5	

7.1.3. Методические разработки

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
ЛП.1	Осипян В.О., Осипян К.В.	Криптография в упражнениях и задачах: учебное пособие	Москва: Гелиос АРВ, 2004	15	

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Электронная библиотека БрГУ	http://ecat.brstu.ru/catalog
----	-----------------------------	---

7.3.1 Перечень программного обеспечения

7.3.1.1	Microsoft Windows Professional 7 Russian Upgrade Academic OPEN No Level
7.3.1.2	Microsoft Office Professional Plus 2010 Russian Academic OPEN 1 license No Level

7.3.2 Перечень информационных справочных систем

7.3.2.1	Электронная библиотека БрГУ
7.3.2.2	Электронный каталог библиотеки БрГУ
7.3.2.3	«Университетская библиотека online»

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

A1207	Лаборатория технических средств защиты информации	Учебная мебель Персональный компьютер i5-2500/H67/4Gb/500Gb(Монитор TFT19 Samsung E1920NR), интерактивная доска SMART Board X885ix со встроенным проектором UX 60,комплекс учебно-лабораторного оборудования "Технические средства и методы защиты информации", управляемый коммутатор 2 уровня D-Link DES-3028.
A1203	Лаборатория параллельных вычислений	Персональный компьютер i5-2500/H67/4Gb/500Gb(Монитор TFT19 Samsung E1920NR), интерактивная доска SMART Board X885ix со встроенным проектором UX 60,доска магнитно-маркерная .
2201	читальный зал №1	Учебная мебель Оборудование 10- ПК i5-2500/H67/4Gb (монитор TFT19 Samsung); принтер HP Laser Jet P2055D
2201	читальный зал №1	Учебная мебель Оборудование 10- ПК i5-2500/H67/4Gb (монитор TFT19 Samsung); принтер HP Laser Jet P2055D

A1207	Лаборатория технических средств защиты информации	Учебная мебель Персональный компьютер i5-2500/H67/4Gb/500Gb(Монитор TFT19 Samsung E1920NR), интерактивная доска SMART Board X885ix со встроенным проектором UX 60, комплекс учебно-лабораторного оборудования “Технические средства и методы защиты информации”, управляемый коммутатор 2 уровня D-Link DES-3028.
2201	читальный зал №1	Учебная мебель Оборудование 10- ПК i5-2500/H67/4Gb (монитор TFT19 Samsung); принтер HP Laser Jet P2055D

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающийся должен разработать собственный режим равномерного освоения дисциплины. Подготовка студента к предстоящей лекции включает в себя ряд важных познавательно-практических этапов:

- чтение записей, сделанных в процессе слушания и конспектирования предыдущей лекции, вынесение на поля всего, что требуется при дальнейшей работе с конспектом и учебником;
- техническое оформление записей (подчеркивание, выделение главного, выводов, доказательств);
- выполнение практических заданий преподавателя;
- знакомство с материалом предстоящей лекции по учебнику и дополнительной литературе.

Активная работа на лекции, ее конспектирование, продуманная, целенаправленная, систематическая, а главное - добросовестная и глубоко осознанная последующая работа над конспектом - важное условие успешного обучения студентов.

Практические занятия и лабораторные работы позволяют студенту более глубоко разобраться в теоретическом материале и определить сферы его практического применения. Основная цель – развитие самостоятельности студента.

Наиболее продуктивной является самостоятельная работа в библиотеке, где доступны основные и дополнительные печатные и электронные источники.

При выполнении приведенных выше рекомендаций подготовка к экзамену сведется к повторению изученного и совершенствованию навыков применения теоретических положений и различных методов решения к стандартным и нестандартным заданиям.