Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)
Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ
Первый проректор
(должность)
/С.Н. Щербич/
(подпись, Ф.И.О.)
«30» июня 2019 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ
(наименование дисциплины)

образовательной программы высшего образования –

программы специалитета

«10.05.03 - Информационная безопасность автоматизированных систем»

Направленность (Специализация №7): **«Обеспечение информационной безопасности распределенных информационных систем»**

Форма обучения: очная

Курган 2019

Рабочая программа дисциплины «Теоретические основы криптологии» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» («Обеспечение информационной безопасности распределенных информационных систем»), утвержденным для очной формы обучения 29 августа 2019 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 27 сентября апреля 2019 года, протокол № 2.

Рабочую программу составил:
канд. пед. наук, доцент /Т.А. Никифорова/

Согласовано:

Зав. кафедрой «БИАС»
канд. пед. наук, доцент /Е.Н. Полякова/

Начальник Управления
образовательной деятельности /С.Н. Синицын/

Специалист по учебно-методической
работе учебно-методического отдела /Г.В. Казанкова/

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единиц трудоемкости (108 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр 5
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	48	48
Лекции	16	16
Лабораторные работы	16	16
Практические занятия	16	16
Самостоятельная работа, всего часов в том числе:	60	60
Подготовка к зачету с оценкой	27	27
Другие виды самостоятельной работы (подготовка к практическим, лабораторным занятиям и рубежному контролю)	15	15
Контрольная работа	18	18
Вид промежуточной аттестации	**Зачет с оценкой**	**Зачет с оценкой**
	108	108

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Теоретические основы криптологии» относится к дисциплинам по выбору вариативной части программы специалитета Блока 1.

Краткое содержание. Криптология: криптография и криптоанализ. Криптостойкость. Криптоатака. Математические основы криптологии и криптографии. Классификация методов криптографической защиты информации. Принципы построения и анализа криптографических алгоритмов. Статистический криптоанализ. Алгебраический криптоанализ. Дифференциальный (или разностный) криптоанализ. Линейный криптоанализ.

Изучение дисциплины «Теоретические основы криптологии» основывается на базе таких дисциплин как «Математический анализ», «Алгебра и геометрия», «Дискретная математика», «Языки программирования» и «Технологии и методы программирования». Знания и навыки, полученные при изучении дисциплины «Теоретические основы криптологии», широко используются студентами при изучении общепрофессиональных и специальных дисциплин, связанных с вопросами проектирования, разработки, эксплуатации и внедрения систем защиты информации.

Результаты обучения по дисциплине необходимы для выполнения курсовой работы по дисциплине «Криптографические методы защиты информации», а также выпускной квалификационной работы в части проектирования систем или модулей защиты информации криптографическими методами.

Освоение следующих компетенций на уровне не ниже порогового: способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8); способностью проводить анализ защищенности автоматизированных систем (ПК-3); способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8); способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14).

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины «Теоретические основы криптологии» является формирование общепрофессиональных и специальных компетентностей посредством знакомства студентов с базовыми понятиями криптологии, с математическими основами криптологии, с методами криптоанализа, а также посредством рассмотрения примеров реализации методов криптоанализа на практике. Изучение методов защиты информации от взлома неразрывно связано с изучением возможных атак на алгоритмы и на их реализации.

Задачами освоения дисциплины «Теоретические основы криптологии» являются:

- дать основы системного подхода к организации криптографической защиты информации, передаваемой и обрабатываемой техническими

средствами на основе применения криптографических методов, криптографических алгоритмов и криптографических протоколов;

- изучение основных математических методов, используемых в криптологии: в криптоанализе и в криптографии;

- изучение основных алгоритмов криптографической защиты информации для разработки программных модулей реализации этих алгоритмов.

Компетенции, формируемые в результате освоения дисциплины «Теоретические основы криптологии»:

- способностью к самоорганизации и самообразованию (ОК-8);

- способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);

- способностью проводить анализ защищенности автоматизированных систем (ПК-3);

- способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

- способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

- способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14).

В результате изучения дисциплины «Теоретические основы криптологии» обучающийся должен:

знать:

- виды криптоатак и методы криптоанализа для исследования возможности взлома криптосистем (для ОК-8, ПК-3);

- принципы анализа защищенности автоматизированных систем (для ПК-3);

- новые образцы программных, технических средств и возможности информационных технологий, направленных на защиту информации от криптоатак (для ОПК-8);

- критерии оценки эффективности применяемых криптографических средств защиты информации (для ПК-14);

уметь:

- проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств защиты информации (для ПК-14);

- применять методы криптоанализа для исследования возможности взлома криптосистем (для ОК-8, ПК-3);

- применять криптографические протоколы и криптографические алгоритмы для передачи и хранения данных в распределенных информационных системах (для ПК-9);

владеть:

- способностью к освоению новых образцов программных, технических средств защиты и информационных технологий (для ПК-3, ПК-8);

- способностью участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (для ПК-9);

- методами криптоанализа для исследования возможности взлома криптосистем (для ОК-8, ПК-3);

- способностью проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств защиты информации (для ПК-14).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Лаборатор. работы	Практич. занятия
семестр 5					
Рубеж 1	Тема 1.1	Криптология: криптография и криптоанализ	1	1	-
	Тема 2.	Классификация методов криптографической защиты информации	2	2	-
	Тема 3.	Математические основы криптологии	6	-	12
	Рубежный контроль 1 (*тестирование и защита реферата*)				2
Рубеж 2	Тема 4.	Криптоанализ	6	10	2
	Тема 5.	Принципы построения и анализа криптографических алгоритмов	1	2	-
	Рубежный контроль 2 (*криптоанализ шифротекста*)			1	
Всего за семестр:			**16**	**16**	**16**

4.2. Содержание лекционных занятий

ТЕМА 1. Криптология: криптография и криптоанализ

Криптология: криптография и криптоанализ. История развития криптологии, криптографии, криптоанализа. Виды угроз. Основной объект криптографии. Проблемы безопасности информации: конфиденциальность, целостность, аутентификация и невозможность отказа сторон от авторства.

Шифр. Ключ. Стойкость ключа. Имитостойкость шифра. Атака на шифр. Три уровня криптоатаки по нарастанию сложности. Сложность вскрытия шифра.

ТЕМА 2. Классификация методов криптографической защиты информации

Математические модели открытого текста. Критерии распознавания открытого текста.

Классификация методов шифрования (криптоалгоритмов): по типу ключей: симметричные криптоалгоритмы; асимметричные криптоалгоритмы; по размеру блока информации: потоковые шифры; блочные шифры; по характеру воздействий, производимых над данными: метод замены (перестановки), метод подстановки; аналитические методы, аддитивные методы (гаммирование), комбинированные методы.

Требования к криптосистемам. Основные направления использования криптографических методов.

ТЕМА 3. Математические основы криптологии

Целые числа. Делимость целых чисел. Простые и составные числа. Проверка чисел на простоту.

Теория вычетов. Арифметика остатков. Функция Эйлера. Обобщенный алгоритм вычисления функции Эйлера для произвольного числа n. Малая теорема Ферма. Теорема Эйлера. Цепочка сложений. Взаимообратные числа по модулю m.

Китайская теорема об остатках. Символ Лежандра. Символ Якоби.

Проверка большого числа на простоту (тест на основе малой теоремы Ферма, тест Соловея-Штрассена, тест Рабина-Миллера, тест Пепина и др.). Детерминированные алгоритмы проверки чисел на простоту. Вероятностные методы проверки чисел на простоту.

Построение больших простых чисел (Критерий Люка, на основе теоремы Диемитко, метод Мауэра, на основе чисел Мерсена и др.).

Алгоритмы факторизации целых чисел (алгоритм Полларда, алгоритм Полларда-Штрассена, Метод Полларда-Флойда, Факторизация Ферма, Метод Лемана, Метод Брента, Метод Женга, Метод Макки, Алгоритм Диксона, Метод Крайчика, квадратичное решето, Метод пробного деления и др.).

Сложность алгоритмов. Временная сложность алгоритма. Ёмкостная сложность алгоритма. Оценка сложности линейного алгоритма и разветвляющегося алгоритма. Оценка сложности итерационного алгоритма (циклического алгоритма). Оценка сложности рекурсивного алгоритма.

ТЕМА 4. Криптоанализ

Основные типы криптоаналитического вскрытия: вскрытие с использованием только шифротекста, вскрытие с использованием открытого текста, вскрытие с использованием выбранного открытого текста, адаптивное вскрытие с использованием открытого текста, вскрытие с использованием выбранного шифротекста, вскрытие с использованием выбранного ключа, бандитский криптоанализ. Основные типы криптоатак: криптоатака с использованием только криптограмм (A1); криптоатака с использованием открытых текстов и соответствующих им криптограмм (A2); криптоатака с использованием выбираемых криптоаналитиком открытых текстов и соответствующих им криптограмм (A3); криптоатака с использованием аппаратного воздействия на криптосистему (криптоатака по сторонним каналом) (A4).

Криптоанализ классических шифров.

Методы криптоанализа: статистический криптоанализ, алгебраический криптоанализ, дифференциальный (или разностный) криптоанализ, линейный криптоанализ.

ТЕМА 5. Принципы построения и анализа криптографических алгоритмов

Принципы построения и криптоанализ симметричных систем. Криптоанализ шифров перестановки. Криптоанализ открытых текстов.

Принципы построения и криптоанализ RSA. Атака методом Ферма. Атака повторным шифрованием. Атака на основе китайской теоремы об остатках. Бесключевое чтение.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование лабораторных работ	Норматив времени, час.
5 семестр			
1	Криптология:	*Лабораторная работа №1.* Виды угроз. Атака на	1

	криптография и криптоанализ	шифр. Стойкость ключа. Сложность вскрытия шифра.	
2	Классификация методов криптографической защиты информации	*Лабораторная работа №2.* Классификация методов криптографической защиты информации	1
		Лабораторная работа №3. Дешифрование классических шифров. Дешифрование шифра Атбаш, шифра Полибия, перестановочного шифра, шифра Плейфера.	1
4	Криптоанализ	*Лабораторная работа №4.* Криптоанализ классических шифров. Криптоанализ шифра столбцовой перестановки. Криптоанализ шифра двойной перестановки.	1
		Лабораторная работа №5. Дешифрование шифра Цезаря.	1
		Лабораторная работа №6. Дешифрование шифра простой замены. Криптоанализ шифра простой замены на основе статистических закономерностей языка	1
		Практическая работа №7. Криптоанализ шифротекста методом словаря на примере шифра Виженера	1
		Лабораторная работа №8. Криптоанализ шифра Виженера. Определение количества букв в ключевом слове по тесту Казиски и индексам совпадения. Поиск ключевого слова с использованием взаимного индекса совпадения. Дешифровка	1
		Лабораторная работа №9. Взлом моноалфавитного шифра замены методом частотной атаки при помощи программы	1
		Практическая работа №10. Криптоанализ шифра Хилла.	1
5	Принципы построения и анализа криптографических алгоритмов	*Практическая работа №11.* Принципы построения и криптоанализ асимметричных систем. Алгоритм шифрования с открытым ключом RSA. Атаки на алгоритм RSA	2
4	Криптоанализ	*Лабораторная работа №12.* Атака на алгоритм шифрования RSA посредством метода Ферма	0,5
		Лабораторная работа №13. Атака на алгоритм шифрования RSA методом повторного шифрования	0,5
		Лабораторная работа №14. Атака на алгоритм шифрования RSA методом бесключевого чтения	1
		Лабораторная работа №15. Атака на алгоритм шифрования RSA, основанный на Китайской теореме об остатках	1
	2-ой рубежный контроль. Криптоанализ шифротекста		1
	Всего за семестр		**16**

4.4. Практические занятия

Номер темы	Наименование темы	Наименование практических занятий	Норматив времени, час.
5 семестр			
3	Математические основы крипто-	*Практическая работа № 1, 2.* Сложность алгоритма	4
		Практическая работа № 3. Теоретико-числовые ал-	2

	логии	горитмы в криптографии. Теория чисел. Целые числа. Каноническое разложение числа. Делимость целых чисел. Классический алгоритм Евклида. Расширенный алгоритм Евклида. Бинарный алгоритм Евклида. Теория вычетов. Арифметика остатков. Малая теорема Ферма. Теорема Эйлера. Цепочка сложений. Сравнения первой степени. Китайская теорема об остатках. Символ Лежандра. Символ Якоби.	
		Практическая работа № 4. Методы проверки чисел на простоту. Решето Эратосфена. Метод на основе малой теоремы Ферма. Вероятностный тест Соловея-Штрассена. Вероятностный тест Рабина-Миллера.	2
		Практическая работа № 5. Алгоритмы факторизации целых чисел (алгоритм Полларда, алгоритм Полларда-Штрассена, Метод Полларда-Флойда, Факторизация Ферма, Метод Лемана, Метод Брента, Метод Женга, Метод Макки, Алгоритм Диксона. Метод Крайчика, квадратичное решето, Метод пробного деления и др.)	2
		Практическая работа № 6. Дискретное логарифмирование	2
	Рубежный контроль 1 (*тестирование и защита реферата*)		2
4	Криптоанализ	*Практическая работа № 8.* Методы криптоанализа	2
		Всего за семестр	16

4.5. Контрольная работа

ПРИМЕРНАЯ ТЕМАТИКА КОНТРОЛЬНОЙ РАБОТЫ

1. Используя расширенный алгоритм Евклида, найти:
   a. $d = \text{НОД}(a; b)$;
   b. решить уравнение $a \cdot x + b \cdot y = d$
2. Найти вычет: 3153 mod 23
   a. используя только цепочку сложений;
   b. используя теорему Эйлера.
3. Найти x по Китайской теореме об остатках

$$\begin{cases} x \bmod 13 = 5, \\ x \bmod 23 = 5, \\ x \bmod 17 = 11, \\ x \bmod 19 = 7. \end{cases}$$

4. Даны числа p = 13; q = 41 и секретный ключ n = 3001 для системы RSA:
   а) сгенерировать соответствующий публичный ключ для шифрования;
   б) зашифровать им сообщение K = 13;
   в) расшифровать шифровку X = 7.
5. Три пользователя имеют модули $m_1 = 391$, $m_2 = 493$, $m_3 = 943$. Все пользователи используют экспоненту $n^{-1} = 3$. Всем пользователям было послано некое сообщение K, причем пользователи получили сообщения $X_1 = 158$, $X_2 = 345$, $X_3 = 388$. Восстановить исходное сообщение K.

6. Два пользователя применяют общий модуль m =6499, но разные взаимно простые экспоненты n_1^{-1} =397 и n_2^{-1} =59. Пользователи получили шифртексты X_1 =2308 и X_2 =2785, которые содержат одно и то же сообщение К. Восстановить исходное сообщение К.

7. Дешифровать текст, зашифрованный методом Виженера:

Ключ «ЕВГЕНИЙ_ОНЕГИН»
ООМЕЯИЩРЦЮФИЧЧЕСКОРФПНЫЫП
ЧДПОФЙПМОТЩРЙЛЕФРЩЖОЧНЭЧ
ТЯГЩРЗОАЫЙЛГЦОЮЛЩЕЩОЫ.
РСЦФЮДЦ_СЫНФЧФКИСБМИЧЕА?

8. Расшифровать фразу, зашифрованную столбцевой перестановкой:
ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ

9. Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки)
А) СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН
Б) АИНАЛЖНОЛЕШФ_ЗИ_УАРОЬСНЕ_

10. Имеется криптограмма: УСХТХУЦЖ, полученная шифром Цезаря. Требуется методом полного перебора (brute force attack) определить ключ шифра и прочесть сообщение.

11. Перехвачен шифртекст ЮНХЪШЩНШЪРЬРТИЮРРТУЖЯНС, при этом известно, что к исходному тексту был применен шифр Цезаря. Требуется: взломать шифр методом последовательного и исчерпывающего перебора ключей. Известно, что при шифровании использованы заглавные русские буквы, однако неизвестна кодировка букв: алфавитная, ASCII или Юникод.

12. Используя частотный криптоанализ, расшифровать текст. Известно, что каждой букве алфавита соответствует двузначное число:
58 62 32 39 99 31 29 58 72 62 99 58 13 54 15 56 31 63 39 72 84 15 13 56 77 15 82 56 56 56 58 54 29 77 56 — 39 99 56 31 56 77 32 12 15 54 31 48 76 63 15 52 13 39 72 39 54 16 72 39 32 72 62 58 58 15, 37 62 77 52 39 13 39 72 39 32 39 31 62 54 39 77 84 39 21 31 39 16 72 62 99 58 13 15 54 56 13 46 16 39 58 13 95 16 15 13 62 12 46 31 39 62 72 15 77 54 56 13 56 62 84 31 39 32 56 76 58 63 62 72 33 62 12 39 54 62 33 62 58 52 39 91 99 62 29 13 62 12 46 31 39 58 13 56. 56 31 63 39 72 84 15 82 56 39 31 31 48 6213 62 76 31 39 12 39 32 56 56 16 72 39 33 31 39 54 39 53 12 56 54 37 56 77 31 62 58, 39 37 72 15 77 39 54 15 31 56 62, 16 72 39 56 77 54 39 99 58 13 54 39, 39 13 52 72 48 54 33 62 12 39 54 62 52 95 31 62 37 48 54 15 12 48 62 54 39 77 84 39 21 31 39 58 13 56 16 39 58 52 39 72 39 58 13 56 16 39 12 95 33 62 31 56 29 56 39 37 72 15 37 39 13 52 62 56 31 63 39 72 84 15 82 56 56, 15 13 15 52 21 62 16 39 15 54 13 39 84 15 13 56 77 15 82 56 56 16 72 39 56 77 54 39 99 58 13 54 62 31 31 48 76, 95 16 72 15 54 12 62 31 33 62 58 52 56 76 56 56 31 48 76 16 72 39 82 62 58 58 39 54.

13. Пусть задан некоторый текст зашифрованный шифром Виженера, требуется определить ключевое слово и прочитать открытый текст.
влцдутжбюцхъяррмшбрхцэооэцгбрьцмйфктъъюьмшэсяцпунуящэйтаьэдкцибрьцгбрпачкъуцпъбьсэгкцъгуущарцёэвърюуоюэкааэбрняфукабъарпяъафкъиьжяффнйояфывбнэнфуюгбрьсшьжэтбэёчюъюръегофкбьчябашвёэуъъюаднчжчужцёэвлрнчулбюпцуруньъшсэюъзкцхъяррнрювяспэмасчкпэужьжыатуфуярюравртубурьпэщлафоуфбюацмнубсюкйтаьэдйюнооэгюожбгкбрънцэпотчмёодзцвбцшцвщепчдчдръюьскасэгъппэгюкдойрсрэвоопчщшоказръббнэугнялёкьсрбёуыэбдэулбюасшоуэтъшкредугэфлбубуъчнчтртпэгюкиугюэмэгюккъъпэгяапуфуэзьрадзьжчюрмфцхраююанчёчюъыхьъцомэфъцпоирькнщпэтэузуябащущбаыэйчдфрпэцъърьцъцпоилуфэдцойздятррачкубуфнйтаьэдкцкрнницюабугюуубурьпйюэъжтгюркующоъуфъэгясуоичщщчдцсфырэдщэъуяфшёчцюйрщвяхвмкршрпгюопэуцчйтаьэдкцибрьцыяжтюрбуэтэбдуящэубъибрювъежагибрбагбрымпуноцшяжцечкфодщоъчжшйуъцхчщвуэбдлдъэгясуахзцэбдэул

ькнъщбжяцэьрёдъьвюврнуяфуоухфекьгцчччгэъжтанопчынажпачкъуъмэнкйрэфщэъьбудэндадъярье юэлэтчоубъцэфэвлнёэгфдсэвэёкбсчоукгаутэыпуббцчкпэгючсаъбэнэфъркацхёваетуфяепьрювържадфё жбьфутощоявьъгупчршуитеачйчирамчюфчоуяюонкяжыкгсцбрясшчйотъъжрсщчл

ПРИМЕРНАЯ ТЕМАТИКА РЕФЕРАТОВ

1. Оценка сложности линейного алгоритма и разветвляющегося алгоритма.
2. Оценка сложности итерационного алгоритма (циклического алгоритма).
3. Оценка сложности рекурсивного алгоритма.
4. Арифметика вычетов. Операции с большими числами по модулю p. Возведение числа в степень по модулю p. Нахождение обратных чисел по модулю p. Нахождение квадратичных вычетов. Метод бинарного возведения в степень для сокращения количества умножений. Алгоритм Евклида.
5. Модулярная арифметика или арифметика остатков (Нахождение НОД, НОК, коэффициентов Безу. Использование Малой теоремы Ферма и Эйлера. Решение диофантовых уравнений, сравнений. Решение систем сравнений методом прямой подстановки, с использованием китайской теоремы об остатках). Модульное представление чисел и Китайская теорема об остатках. Метод модулярного умножения по Монтгомери для того, чтобы не выходить из разрядности чисел C, D и N в процессе умножения больше, чем на 1 разряд.
6. Проверка большого числа на простоту (тест на основе малой теоремы Ферма, тест Соловея-Штрассена, тест Рабина-Миллера, тест Пепина, Детерминированные алгоритмы проверки чисел на простоту и др.).
7. Замечание. Простоту целого числа можно определять на основе теоремы Вильсона и использования чисел Мерсенна.
8. Построение больших простых чисел (Критерий Люка, на основе теоремы Диемитко, метод Мауэра, на основе чисел Мерсена и др.).
9. Алгоритмы факторизации целых чисел (алгоритм Полларда, алгоритм Полларда-Штрассена, Метод Полларда-Флойда, Факторизация Ферма, Метод Лемана, Метод Брента, Метод Женга, Метод Макки, Алгоритм Диксона, Метод Крайчика, квадратичное решето, Метод пробного деления и др.) и криптографическая система RSA.
10. Дискретное логарифмирование (Алгоритм перебора, алгоритм Сильвера-Поллига-Хеллмана (алгоритм согласования), Алгоритм Гельфонда, Алгоритм Хеллмана–Рейнери и др.) в конечном поле. Вероятностные методы: Метод Полларда-Флойда, Метод Госпера. Субэкспоненциальный метод: Идеология Крайчика, Алгоритм Адлемана и др. Протокол Диффи-Хеллмана [1, 3, 5, 7].
11. Операции на эллиптических кривых. Дискретное логарифмирование на эллиптических кривых.
12. Построение псевдослучайных последовательностей. Конгруэнтные генераторы ПСП. Генератор ПСП Блюм-Блюма-Шуба (BBS). Генератор последовательностей RSA. Регистры сдвигов с обратной связью.
13. Атака с известным шифртекстом (ciphertext only attack). Разновидности: полный перебор ключей; атака по словарю, перебор ключей по словарю (dictionary attack); частотный криптоанализ.
14. Атака с выбором шифртекста (chosen ciphertext attack).
15. Адаптивная атака с выбором шифртекста (adaptive chosen ciphertext attack).
16. Атака с известным открытым текстом (known plaintext attack).
17. Атака с выбором открытого текста (chosen plaintext attack). Разновидности: временный доступ к шифрующему устройству: использование информации о структуре сообщений или стандартных фразах; перебор ключей по словарю (dictionary attack): получение документа и ЭЦП к нему, сгенерированной с помощью закрытого ключа.
18. Адаптивная атака с выбором открытого текста (adaptive chosen plaintext attack). Разновидности: провоцирование противника на использование в сообщениях определенных слов или фраз; дифференциальный криптоанализ; интегральный криптоанализ; линейный криптоанализ; использование открытых ключей в асиметричных системах.
19. Атака на основе связанных ключей (related key attack).
20. Атака с выбором ключа (chosen key attack).
21. Типовые методы криптоанализа классических алгоритмов: Дифференциальный метод криптоанализа. Линейный метод криптоанализа. Частотный метод криптоанализа. Линейный криптоанализ.
22. Универсальные методы криптоанализа. Принципы криптоанализа, критерии распознавания открытого текста, универсальные методы криптоанализа: Метод встречи посередине. Метод Полларда. Метод грубой силы, математическое ожидание числа опробований при случайном и равновероятном

выборе ключа, распараллеливание при тотальном переборе ключей, метод «вирусов», «Китайская лотерея».

23. Метод «разделяй и побеждай», оценка сложности.
24. Частотный метод криптоанализа для шифров простой замены, метод Якобсена.
25. Дифференциальный криптоанализ, дифференциальный криптоанализ DES и трехраундового DES.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной или практической работе.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения практических работ и лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем перед началом работы.

Преподавателем запланировано применение на практических занятиях и лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на практических занятиях и лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает подготовку к практическим занятиям и лабораторным работам, к рубежным контролям, написание контрольной работы, подготовку к дифференцируемому зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Углубленное изучение разделов, тем дисциплины лекционного курса Изучение разделов, тем дисциплины, не вошедших в лекционный курс, а именно: Построение псевдослучайных последовательностей. Конгруэнтные генераторы ПСП. Генератор ПСП Блюм-Блюма-Шуба (BBS). Генератор последовательностей RSA. Регистры сдвигов с обратной связью Операции на эллиптических кривых. Дискретное логарифмирование на эллиптических кривых.	3
Подготовка к практическим занятиям, лабораторным работам и рубеж-	8

ному контролю (по 0,5 ч на каждое занятие)	
Подготовка к рубежному контролю (по 2 ч на каждый контроль)	4
Контрольная работа	18
Подготовка к экзамену	27
Всего:	**60**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ.
2. Отчеты студентов по лабораторным работам.
3. Отчеты студентов по практическим занятиям.
4. Контрольная работа.
5. Банк тестовых заданий к рубежным контролям № 1, № 2.
6. Вопросы к дифференцируемому зачету.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание							
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	*Распределение баллов, 5 семестр*							
		Вид учебной работы:	Посещение лекций	Выполнение практических работ	Выполнение и защита лабораторных работ	Контрольная работа	Рубежный контроль №1	Рубежный контроль №2	Диф зачет
		Балльная оценка:	$1_б$ x8 = $8_б$	$2_б$ x 8 = $16_б$	$2_б$ x 15 =$30_б$	8	4	4	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета	60 и менее баллов – неудовлетворительно; 61…73 – удовлетворительно; 74… 90 – хорошо; 91…100 – отлично							
3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (диф. зачету) студент должен набрать не менее 50 баллов, выполнить все практические, лабораторные и контрольную работы. Для получения экзаменационной оценки «автоматически» и получить оценку «удовлетворительно» студенту необходимо набрать 68 баллов. По согласованию с преподавателем студенту, набравшему минимум 68 балл, могут быть добавлены дополнительные (бонусные) баллы за активность на практических занятиях и лабораторных работах, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических и лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры							

		и выставлена оценка «хорошо» или «отлично» автоматически.
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае, если к промежуточной аттестации (диф. зачету) набрана сумма менее 50 баллов (не выполнены все задания), необходимо выполнить дополнительные задания, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных практических и лабораторных работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенной практической или лабораторной работы (при невозможности дополнительного проведения работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 10 баллов. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежный контроль № 1 проводятся в форме письменного тестирования.

Рубежный контроль № 2 проводятся в письменной форме.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий рубежного контроля № 1 состоят из 15 вопросов. На тестирование при рубежном контроле студенту отводится 2 академических часа.

Задания рубежного контроля № 2 состоят из 3примеров шифротекстов, которые необходимо взломать. На взлом при рубежном контроле студенту отводится 2 академических часа.

Баллы студенту выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования и результаты решения практических заданий каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Дифференцируемый зачет проводится в форме ответа на вопросы билета. Экзаменационный билет состоит из 2 теоретических вопросов и 1 практического задания. Каждый вопрос оценивается в 10 баллов. Вопросы дифференцированного

зачета доводятся до студентов на последней лекции в семестре. На подготовку ответа студенту отводится 1 астрономический час.

Результаты текущего контроля успеваемости дифференцированного зачета заносятся преподавателем в зачетную ведомость, которые сдаются в орготдел института в день дифференцированного зачета, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей, дифференцируемого зачета

1-ый рубежный контроль

1. *Наибольший общий делитель чисел 165 и 315 равен*

1) 15 2) 5 3) 3465 4) 3

2. Используя расширенный алгоритм Евклида найти $x_0 + y_0$, *где* $(x_0; y_0)$ *целые решения уравнения* $119x + 84y = 7$.

1) 7 2) -2 3) 2 4) 1

3. Функция Эйлера φ(n): количество положительных целых чисел, меньших n и взаимно простых с n. φ(13) равно

1) 0 2) 1 3) 13 4) 12

4. Среди данных чисел, евклидовым является число

1) 5 2) 131 3) 29 4) 55

5. Наименьший положительный вычет 10 mod 3 равен

1) 2 2) 7 3) 1 4) 13

6. Последняя цифра числа 3^{83} равна

1) 7 2) 1 3) 9 4) 3

2-ый рубежный контроль (практические задания)

1. Сообщение (3,1,2), закодированное с помощью ключа {7} по mod m = 33 алгоритмом RSA, имеет вид:

1) (19, 2, 21) 2) (3, 4, 8) 3) (3, 1, 16) 4) (9, 1, 29)

2 Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки):

П_БИРДЛЬНЕВ_ОП_ОПЗДЕВЫГЕА

3. Перехвачен шифртекст, при этом известно, что к исходному тексту был применен шифр Цезаря. Требуется: взломать шифр методом последовательного и исчерпывающего перебора ключей. Известно, что при шифровании использованы заглавные русские буквы.

ИЦРХЭЫЩШШЩРЫЩЦМДРШУРМЮПРЭЪЩЬЭРЪРШШЩТЛЧРШКЭЗЩМЖВШЩРМ ЮЧЛСШЩРЫЩЦМДРШУР

4. Известно, что зашифровано стихотворение Р. Киплинга в переводе С.Я. Маршака. Шифрование заключалось в замене каждой буквы на двузначное число. Отдельные слова разделены несколькими пробелами, знаки препинания сохранены.

29 15 10 17 29 22 25 31 15 33 35 41 43 45 35 57 45 25 17 59 15 10 25 41 25 69, 59 78 29 82 25 78 25 17 15 10 88 90 78 25 62 25 22 10 57 73 79 35 67 78 90 88 29 45 35 29, 54 57 90 31 90 73 22 88

15 88 29 15 17 69 41 25 15, 70 17 90 57 43 59 15 78 15 62 22 25 17 57 25 69 88 15 82 17 25 88 29 45 35…

Криптоанализ шифра простой замены выполните на использовании статистических закономерностей русского языка.

5. Злоумышленнику стал известен шифротекст, полученный по алгоритму шифра Плейфера.

ЙЦЦГЕБЪЦЦКХЗЖЛХНИПОЙИДЪЦ

6. Пусть задан некоторый текст зашифрованный шифром Виженера, требуется определить ключевое слово и прочитать открытый текст.

ВЛЦДУТЖБЮЦХЪЯРРМШБРХЦЭООЭЦГБРЬЦМЙФКТЪЪЮЬМШЭСЯЦПУНУЯЩЭЙТА
ЬЭДКЦИБРЬЦГБРПАЧКЪУЦПЪБЬСЭГКЦЪГУУЩАРЦЁЭВЪРЮУОЮЭКААЭБРНЯФУК
АБЪАРПЯЪАФКЪИЬЖЯФФНЙОЯФЫВБНЭНФУЮГБРЬСШЬЖЭТБЭЁЧЮЪЮРЪЕГОФК
БЬЧЯБАШВЁЭУЪЪЮАДНЧЖЧУЖЦЁЭВЛРНЧУЛБЮПЦУРУНЬЪШСЭЮЪЗКЦХЪЯРРНР
ЮВЯСПЭМАСЧКПЭУЖЬЖЫАТУФУЯРЮРАВРТУБУРЬПЭЩЦЛАФОУФБЮАЦМНУБСЮ
КЙТАЬЭДЙЮНООЭГЮОЖБГКБРЪНЦЭПОТЧМЁОДЗЦВБЦШЩВЩЕПЧДЧДРЪЮЬСКА
СЭГЪППЭГЮКДОЙРСРЭВООПЧЩШОКАЗРЪББНЭУГНЯЛЁКЬСРБЁУЫЭБДЭУЛБЮАС
ШОУЭТЪШКРСДУГЭФЛБУБУЪЧНЧТРТПЭГЮКИУГЮЭМЭГЮККЪЪПЭГЯАПУФУЭЗЬ
РАДЗЬЖЧЮРМФЦХРАЮЮАНЧЁЧЮЪЫХЬЪЦОМЭФЪЦПОИРЬКНЩПЭТЭУЗУЯБАЩУ
ЩБАЫЭЙЧДФРПЭЦЪЬРЬЦЬЦПОИЛУФЭДЦОЙЭДЯТРРАЧКУБУФНЙТАЬЭДКЦКРНЦ
ЮАБУГЮУУБУРЬПЙЮЭЪЖТГЮРКУЮЩОЪУФЪЭГЯСУОИЧЩЩЧДЦСФЫРЭДЩЭЪУ
ЯФШЁЧЦЮЙРЩЦВЯХВМКРШРПГЮООПЭУЦЧЙТАЬЭДКЦИБРЬЦЫЯЖТЮРБУЭТЭБДУЯ
ЩЭУБЪИБРЮВЪЕЖАГИБРБАГБРЫМПУНОЦШЯЖЦЕЧКФОДЩОЪЧЖШЙУЪЦХЧЩВУ
ЭБДЛДЪЭГЯСУАХЗЦЭБДЭУЛЬКНЪЩБЖЯЦЭЬРЁДЪЬВЮВЛРНУЯФУОУХФЕКЬГЦЧЧЧ
ГЭЪЖТАНОПЧЫНАЖПАЧКЪУЪМЭНКЙРЭФЩЭЪЬБУДЭНДАДЪЯРЬЕЮЭЛЭТЧОУБЪЦ
ЭФЭВЛНЁЭГФДСЭВЭЁКБСЧОУКГАУТЭЫПУББЦЧКПЭГЮЧСАЪБЭНЭФЪРКАЦХЁВАЕ
ТУФЯЕПЬРЮВЪРЖАДФЁЖБЬФУТОЩОЯВЬЪГУПЧРШУИТЕАЧЙЧИРАМЧЮФЧОУЯЮ
ОНКЯЖЫКГСЦБРЯСШЧЙОТЪЪЖРСЩЧЛ

Примерная тематика вопросов, выносимых на зачет в 5-ом семестре

1. Криптология: криптография и криптоанализ. История развития криптологии, криптографии, криптоанализа. Основной объект криптографии.
2. Проблемы безопасности информации: конфиденциальность, целостность, аутентификация и невозможность отказа сторон от авторства.
3. Шифр. Ключ. Стойкость ключа. Имитостойкость шифра. Сложность вскрытия шифра.
4. Виды угроз. Атака на шифр. Три уровня криптоатаки по нарастанию сложности.
5. Математические модели открытого текста. Критерии распознавания открытого текста.
6. Классификация методов шифрования (криптоалгоритмов) по типу ключей: симметричные криптоалгоритмы; асимметричные криптоалгоритмы.
7. Классификация методов шифрования (криптоалгоритмов) по размеру блока информации: потоковые шифры; блочные шифры.
8. Классификация методов шифрования (криптоалгоритмов) по характеру воздействий, производимых над данными: метод замены (перестановки), метод подстановки; аналитические методы, аддитивные методы (гаммирование), комбинированные методы.

9. Требования к криптосистемам. Основные направления использования криптографических методов.
10. Основные направления использования криптографических методов.
11. Целые числа. Делимость целых чисел. Простые числа. Проверка чисел на простоту тест на основе малой теоремы Ферма.
12. Простые числа. Проверка чисел на простоту тест на основе теста Соловея-Штрассена и теста Пепина.
13. Теория вычетов. Арифметика остатков. Функция Эйлера. Обобщенный алгоритм вычисления функции Эйлера для произвольного числа n. Малая теорема Ферма. Теорема Эйлера. Взаимообратные числа по модулю m.
14. Цепочка сложений. Китайская теорема об остатках. Символ Лежандра. Символ Якоби.
15. Вероятностные методы проверки чисел на простоту тест Рабина-Миллера.
16. Построение больших простых чисел (Критерий Люка, на основе теоремы Диемитко, метод Мауэра, на основе чисел Мерсена и др.).
17. Алгоритмы факторизации целых чисел (алгоритм Полларда, алгоритм Полларда-Штрассена, Метод Полларда-Флойда, Факторизация Ферма, Метод Лемана, Метод Брента, Метод Женга, Метод Макки, Алгоритм Диксона, Метод Крайчика, квадратичное решето, Метод пробного деления и др.).
18. Сложность алгоритмов. Временная сложность алгоритма. Ёмкостная сложность алгоритма. Оценка сложности линейного алгоритма и разветвляющегося алгоритма. Оценка сложности итерационного алгоритма (циклического алгоритма). Оценка сложности рекурсивного алгоритма.
19. Основные типы криптоаналитического вскрытия: вскрытие с использованием только шифротекста, вскрытие с использованием открытого текста, вскрытие с использованием выбранного открытого текста, адаптивное вскрытие с использованием открытого текста, вскрытие с использованием выбранного шифротекста, вскрытие с использованием выбранного ключа, бандитский криптоанализ.
20. Основные типы криптоатак: криптоатака с использованием только криптограмм (A1); криптоатака с использованием открытых текстов и соответствующих им криптограмм (A2); криптоатака с использованием выбираемых криптоаналитиком открытых текстов и соответствующих им криптограмм (A3); криптоатака с использованием аппаратного воздействия на криптосистему (криптоатака по сторонним каналом) (A4).
21. Криптоанализ открытых текстов.
22. Криптоанализ шифров перестановки.
23. Криптоанализ шифров замены.
24. Криптоанализ шифра Вижинера.
25. Методы криптоанализа. Статистический криптоанализ,
26. Методы криптоанализа. Алгебраический криптоанализ.
27. Методы криптоанализа. Дифференциальный (или разностный) криптоанализ.
28. Методы криптоанализа. Линейный криптоанализ.
29. Криптосистема RSA. Принципы построения и криптоанализ RSA.

30. Атака на RSA методом Ферма.
31. Атака на RSA повторным шифрованием.
32. Атака на RSA на основе китайской теоремы об остатках.
33. Атака на RSA. Бесключевое чтение.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

Основная литература:

1. Фомичев В.М., Мельников Д.А. Криптографические методы защиты информации. Математические аспекты. Учебник. В 2 частях. — М. : Издательство Юрайт, 2016. – 210 с. [Электронный ресурс]. https://urait.ru/book/kriptograficheskie-metody-zaschity-informacii-v-2-ch-chast-1-matematicheskie-aspekty-422364
2. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012. – 400 с. [Электронный ресурс] http://www.aha.ru/~msa/kriptograficheskie.pdf
3. Бабаш А.В. Криптографические методы защиты информации: учебник / А.В. Бабаш, Е.К. Баранова. — М. : КНОРУС, 2016. –190 с.
4. Ерош И.Л. Криптография. Первое знакомство. Учебное пособие. Редакционно-издательский центр ГУАП, 2008. – 84 с. [Электронный ресурс]

Дополнительная литература:

1. Ван Тилборг Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. - М., Мир, 2006, 471 с.
2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / М., МЦНМО, 2003, 328 с
3. Введение в криптографию. Под общей редакцией В. В. Ященко. Издание 4-е, дополненное. МЦНМО, М., 2012. – 315 с.
4. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронно-цифровой подписи на базе асимметричного криптографического алгоритма.
5. ГОСТ Р34.10-01. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
6. Запечников, С. В. Криптографические методы защиты информации : учеб. пособие для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — М. : Издательство Юрайт, 2015. – 309 с

7. Маховенко Е.Б. Теоретико-числовые методы в криптографии. М.:Гелиос АРБ,2006.
8. Ростовцев А.Г. Алгебраические основы криптографии. СПб.: Мир и семья, Интерлайн, 2000. — 354 с : илл
9. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации: Учебное пособие для вузов. 2-е издание, стереотип. - М.: Горячая линия-Телеком, 2014. – 229 с.
10. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. ISBN 5-94057-060-7 М.: МЦНМО, 2002. – 104 с.

Методические материалы

1. Лабораторный практикум «Криптоанализ классических шифров» для студентов специальностей 10.05.03, 10.03.01 по дисциплине «Теоретические основы криптологии» для студентов направлений (специальностей) 10.05.03, 10.03.01. – Курган: КГУ, 2016. – 100 с (на правах рукописи).
2. Методические указания к выполнению лабораторных работ по дисциплине «Теоретические основы криптологии» на тему «Криптоанализ алгоритма RSA» для студентов направлений (специальностей) 10.05.03, 10.03.01. – Курган: КГУ, 2016. – 96 с. (на правах рукописи)
3. Методические указания к выполнению контрольной работы по дисциплине «Теоретические основы криптологии» для студентов направлений (специальностей) 10.05.03, 10.03.01. – Курган: КГУ, 2017. – 20 с. (на правах рукописи)

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Голиков, А. М. Криптографические методы защиты информации: Учебное пособие для специалитета. Курс лекций, компьютерный практикум, задание на самостоятельную работу [Электронный ресурс] / Голиков А. М. – Томск: ТУСУР, 2016. – 97 с. – Режим доступа: https://edu.tusur.ru/publications/6313.
2. Ветров Ю. В. Криптографические методы защиты информации в телекоммуникационных системах [Электронный ресурс]: учебное пособие для вузов. / Ю.В. Ветров, С.Б. Макаров; Санкт-Петербургский государственный политехнический университет. – Электрон. текстовые дан. – Санкт-Петербург, 2011. – Загл. с титул. экрана. – Свободный доступ из сети Интернет. – Текстовый документ. – Adobe Acrobat Reader 7.0. – <URL:http://elib.spbstu.ru/dl/2889.pdf>.
3. Черемушкин А.В. Вычисления в алгебре и теории чисел. – Загл. с титул. экрана. – Свободный доступ из сети Интернет. – Текстовый документ. www.cryptography.ru.
4. Шнайер Б. Прикладная криптография / М., Триумф, 2003, 816 с – Загл. с титул. экрана. – Свободный доступ из сети Интернет. – Текстовый документ. http://www.ssl.stu.neva.ru/psw/crypto.html.

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, LibreOffice.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при выполнении заданий лабораторных работ: Windows XP, LibreOffice, программы, разработанные преподавателем.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet, коммутатор 2-го уровня D-LINK DGS-101D/E1A.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Теоретические основы криптологии»

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем
Направленность: обеспечение информационной безопасности распределенных информационных систем
Форма обучения: очная

Трудоемкость дисциплины: 3 з.е. (108 академических часа)
Семестр: 5 (очная форма обучения)
Форма промежуточной аттестации: экзамен
Содержание дисциплины. Основные разделы.

Криптология: криптография и криптоанализ. Криптостойкость. Криптоатака. Математические основы криптологии и криптографии. Классификация методов криптографической защиты информации. Принципы построения и анализа криптографических алгоритмов. Статистический криптоанализ. Алгебраический криптоанализ. Дифференциальный (или разностный) криптоанализ. Линейный криптоанализ.