

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИЖЕВСКАЯ ГОСУДАРСТВЕННАЯ СЕЛЬСКОХОЗЯЙСТВЕННАЯ АКАДЕМИЯ»



УТВЕРЖДАЮ

Проректор по учебной работе:

/П.Б. Акмаров/

04 2017 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине «Кодирование и защита информации»

Специальность: «Экономическая безопасность»

Квалификация выпускника: экономист

Форма обучения - очная, заочная

Ижевск 2017

1. Цели и задачи дисциплины

Дисциплина «Кодирование и защита информации» предполагает ознакомление с основными понятиями и теоретическими основами теории защиты информации - методов передачи, хранения и защиты информации по различным каналам связи, а именно: теории кодов, исправляющих ошибки в каналах связи с шумами; криптологии, состоящей из криптографии и криптоанализа; а также сжатия данных (передачи информации по каналам связи без шума).

Задачи дисциплины. 1. В части курса, посвященной теории кодирования, предлагается ознакомление с базовыми понятиями теории линейных кодов (основные понятия, кодирование и декодирование линейных кодов, границы объемов кодов, методы построения кодов), а также теории циклических кодов (кольцо многочленов над полем Галуа, определение циклического кода, необходимое и достаточное условие существования циклического кода с порождающим многочленом $g(x)$, кодирование и декодирование циклических кодов, коды Хэмминга, коды Боуза-Чоудхури-Хоквингема (БЧХ-коды), коды Рида-Соломона). Эти классы кодов наиболее часто применяются на практике. Теория кодирования самым тесным образом связана с дискретным анализом, теорией групп, теорией Галуа, конечными геометриями, теорией графов, теорией блок-схем (design theory), криптографией. 2. Вторая часть курса посвящена введению в криптологию, здесь излагаются основные стандарты шифрования данных (DES, AES, российский стандарт шифрования данных ГОСТ 28147-89), теорема Шеннона о существовании совершенно секретных шифров, а также основные криптосистемы с открытыми ключами: криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма, криптосистема Шамира, криптосистема, основанная на эллиптических кривых, цифровые подписи, базирующиеся на основных криптосистемах. Здесь же рассматриваются вопросы применения теории кодирования в криптографии (кодовые асимметричные криптосистемы, проблемы аутентификации, блочные шифры, проблемы распределения секретов). 3. В третьей части курса, посвященной сжатию данных излагаются основные методы сжатия данных – методы побуквенного кодирования (коды Фано, Хаффмена, Шеннона), критерий однозначности кодирования, теорема Шеннона; основные методы адаптивного кодирования (методы Лемпела-Зива, код “стопка книг”, арифметический код).

2. Место дисциплины в структуре ООП

Дисциплина изучается во взаимосвязи с материалом других дисциплин по практическому решению задач на персональных компьютерах и обеспечивает внедрение информационных технологий в научно-исследовательский процесс. Умения и навыки приобретаются студентами в процессе занятий и в процессе самоподготовки.

В рамках дисциплины студенты должны освоить современные информационные технологии, базирующиеся на применении электронно-вычислительной техники, математического, программного и информационного обеспечения, а также средств и систем связи, уметь использовать электронные и сетевые ресурсы для решения прикладных пользовательских задач и проведения научных исследований.

Содержательно-логические связи дисциплины «Кодирование и защита информации»

Код дисциплины	Содержательно-логические связи
	коды и название учебных дисциплин, практик
	на которые опирается содержание данной учебной дисциплины
Кодирование и защита информации	История
	Которым предшествует изучение дисциплины
	Экономическая безопасность Научно-исследовательская работа

3. Компетенции обучающегося, формируемые в результате освоения дисциплины « Кодирование и защита информации»

(перечень планируемых результатов обучения по дисциплине)

В процессе освоения дисциплины студент должен развивать и овладевать следующими компетенциями:

- способностью использовать закономерности и методы экономической науки при решении профессиональных задач (ОПК-2);
- способностью применять методы проведения прикладных научных исследований, анализировать и обрабатывать их результаты, обобщать и формулировать выводы по теме исследования (ПК-47);
- способность выявлять и использовать взаимосвязь и взаимозависимость экономических и правовых явлений в профессиональной деятельности (ПСК-2).

В результате изучения дисциплины студент должен:

Иметь представление об области применимости методов передачи, хранения и защиты информации для исследования различных явлений и процессов. Знать методы теории кодирования для решения задач передачи информации по каналам связи с шумами; знать криптографические методы защиты информации от несанкционированного доступа для передачи информации с использованием как криптосистем с секретными ключами, так и криптосистем с открытыми ключами; уметь создавать цифровые подписи, используя основные криптосистемы Эль-Гамала, RSA, криптосистемы на эллиптических кривых; знать методы теории информации для решения задач передачи информации по каналам связи без шума. Уметь оценить возможности применения и применять методы передачи, хранения и защиты информации для решения конкретных прикладных задач (в частности создания цифровых подписей, защиты паролей в банках). Владеть основными методами теории помехоустойчивого кодирования для передачи информации по каналам связи с помехами такими как методы кодирования и декодирования линейных кодов, методы кодирования и декодирования циклических кодов (кодов БЧХ, Рида-Соломона); владеть основными методами теории сжатия данных – методы кодирования для стационарных источников, адаптивные методы кодирования, универсальные методы; владеть основными методами теории защиты информации от несанкционированного доступа – владеть методами защиты информации как с помощью криптосистем с секретными ключами, так и с помощью криптосистем с открытыми ключами, владеть методами построения цифровых подписей на основе криптосистем Эль-Гамала, RSA, криптосистем, основанных на эллиптических кривых.

3.1 Перечень компетенций

Номер/индекс компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины студент должен:		
		Знать	Уметь	Владеть
ОПК-2	способностью использовать закономерности и методы экономической науки при решении профессиональных задач	Основные законы в области защиты информации	Разрабатывать технологии кодирования и защиты информации	Законными способами получения и защиты информации
ПК-47	способностью применять методы проведе-	Способы извлечения и восстановления науч-	Пользоваться электронными система-	Законными технологиями полу-

	ния прикладных научных исследований, анализировать и обрабатывать их результаты, обобщать и формулировать выводы по теме исследования	ной информации, передачи ее по каналам связи	ми получения информации и ее анализа	чения и использования экономической информации
ПСК-2	способность выявлять и использовать взаимосвязь и взаимозависимость экономических и правовых явлений в профессиональной деятельности	Нормативно-правовые акты в сфере защиты информации	Оформлять документацию ограниченного доступа	Средствами электронной защиты информации

4. Структура и содержание дисциплины

Общая трудоемкость составляет 3 зач.ед. (108 часов).

Вид учебной работы, часов	Очная форма	Заочная форма
	Семестр	
	3	3
1.Аудиторная работа, всего:	52	12
Лекции	18	6
Лабораторные занятия	34	6
2.Самостоятельная работа студентов (СРС):	29	87
-рефераты		
- контрольная работа	4	30
-самоподготовка (самостоятельное изучение разделов, проработка и повторение лекционного материала, учебников и учебно-методических пособий, подготовка к практическим занятиям и пр.)	25	53
Промеж.аттестация: экзамен	27	9
Общая трудоемкость дисциплины	108	108

4.1 Структура дисциплины (очная форма обучения)

№ п/п	Семестр	Недели семестра	Раздел дисциплины (модуля), темы раздела	Виды учебной работы, включая СРС и трудоемкость (в часах)						Форма: -текущего контроля успеваемости, СРС (по неделям семестра); -промежуточной аттестации (по семестрам)
				всего	лекция	лабораторные занятия	Практические занятия	семинары	СРС	
1	3	1	Кодирование информации	20	4	12			13	2КР

2	3	2	Сжатие информации	12	4	4			4	СР
3	3	4	Элементы криптологии	24	6	14			4	2КР, СР
4	3	6	Цифровая подпись	8	2	2			4	СР
5	3	8	Защита информации	8	2	2			4	СР
6	3		Промежуточная аттестация Экзамен	27						Экз.
Итого				108	18	34			29	

4.2 Структура дисциплины (заочная форма обучения)

№ п/п	Семестр	Недели семестра	Раздел дисциплины (модуля), темы раздела	Виды учебной работы, включая СРС и трудоемкость (в часах)						СРС	Форма: -текущего контроля успеваемости, СРС (по неделям семестра); -промежуточной аттестации (по семестрам)
				всего	лекция	лабораторные занятия	Практические занятия	семинары	СРС		
1	2	1	Кодирование информации	24	2	2				20	2КР
2	2	2	Сжатие информации	19	1	1				16	СР
3	2	4	Элементы криптологии	19	1	1				16	2КР, СР
4	2	6	Цифровая подпись	19	1					16	СР
5	2	8	Защита информации	18	1	2				19	СР
6	2		Промежуточная аттестация Экзамен	9						9	Экз.
Итого				108	6	6				96	

4.3 Матрица формируемых дисциплиной компетенций

Разделы и темы дисциплины	Количество часов	Компетенции			
		ОПК-2	ПК-47	ПСК-2 ...	общее количество компетенций
Кодирование информации	20	*		*	2
Сжатие информации	12	*			1
Элементы криптологии	24		*	*	2
Цифровая подпись	8	*		*	2
Защита информации	8	*			1
Промежуточная аттестация Экзамен	36	*	*	*	3
Итого	108				3

4.4 Содержание разделов дисциплины

№№ п/п	Название раздела	Содержание раздела
1.	Кодирование информации	Кодирование в двоичном симметричном канале - Модель канала связи, скорость кода, пропускная способность. Теорема Шеннона (без доказательства). Вероятность ошибки декодирования. Стандартное расположение. Синдром. - Поле Галуа, его свойства, примеры полей Галуа. - Линейные коды. Кодирование и декодирование. Общие свойства линейных кодов.
2.	Сжатие информации	Сжатие информации - Разделимые и префиксные коды. Стоимость кодирования. Неравенство Крафта-Макмиллана. Теорема Крафта. Теорема МакМиллана. - Оптимальное кодирование. Метод Хаффмена. Метод Фано. - Энтропия. Метод Шеннона для бернуллиевских источников.
3	Элементы криптологии	Элементы криптологии - Введение в криптологию. Секретность и имитостойкость. Основные идеи. Криптография и криптоанализ. - Криптографические системы с секретными ключами. Подстановки. Перестановки. Полиалфавитные шифры. Шифр с бегущим ключом. Криптографические системы коды. - Теорема Шеннона о существовании совершенно секретных шифров. - Стандарт шифрования данных (криптосистема AES, криптосистема ГОСТ, криптосистема DES). - Криптографические системы с открытыми ключами.
4	Цифровая подпись	Цифровая подпись. Законодательство. Техническая реализация
5	Защита информации	Защита от несанкционированного использования. Защита от вирусов. Защита от помех

4.5 Лабораторные занятия (очная форма обучения)

№ п/п	№ раздела дисциплины	Тематика лабораторных занятий	Трудоемкость (час.)
1	1.	Линейные коды. Кодирование и декодирование. Методы построения новых кодов из заданных. Комбинирование кодов. Совершенные коды. Коды Хэмминга над $GF(q)$, способы задания, кодирование, декодирование, единственность. Конструкция кодов Васильева, Циклические коды. Кодирование и декодирование циклических кодов. Модель канала связи, скорость кода, пропускная способность. Стандартное расположение. Примеры полей Галуа. -	12
2	2.	Сжатие текстовой и графической информации. Способы сжатия. Плотность сжатия	4
3	3	Секретность и имитостойкость. Криптографические системы с секретными ключами. Подстановки. Перестановки. Полиалфавитные шифры. Шифр с бегущим ключом. Криптографические системы коды. Криптографические системы с открытыми ключами. Односторонняя функция с лазейкой. “Шарады” Меркля. - Криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма. - Криптосистема Шамира. - Криптосистема RSA. Криптосистема Меркля-Хэллмана, основанная на задаче об укладке ранца. - Кодированные системы Мак Эллиса и Нидеррайтера.	14
4	4	Формирование и анализ цифровой подписи	2
5	5	Законы и нормативно-правовые акты. Антивирусы. Помехозащитные коды	2

4.6 Лабораторные занятия (заочная форма обучения)

№ п/п	№ раздела дисциплины	Тематика лабораторных занятий	Трудоемкость (час.)
1	1.	Линейные коды. Кодирование и декодирование. Методы построения новых кодов из заданных. Комбинирование кодов. Совершенные коды. Коды Хэмминга над $GF(q)$, способы задания, кодирование, декодирование, единственность. Конструкция кодов Васильева, Циклические коды. Кодирование и декодирование циклических кодов. Модель канала связи, скорость кода, пропускная способность. Стандартное расположение. Примеры полей Галуа. -	2
2	2.	Сжатие текстовой и графической информации. Способы сжатия. Плотность сжатия	2
3	3	Секретность и имитостойкость. Криптографические системы с секретными ключами. Подстановки. Перестановки. Полиалфавитные шифры. Шифр с бегущим ключом. Криптографические системы коды. Криптографические системы с открытыми ключами.	2

		Односторонняя функция с лазеркой. “Шарады” Меркля. - Криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма. - Криптосистема Шамира. - Криптосистема RSA. Криптосистема Меркля-Хэллмана, основанная на задаче об укладке ранца. - Кодированные системы Мак Эллиса и Нидеррайтера.	
4	4	Формирование и анализ цифровой подписи	2
5	5	Законы и нормативно-правовые акты. Антивирусы. Помехозащитные коды	2

4.7 Содержание самостоятельной работы и формы ее контроля (очная форма обучения)

№ п/п	Раздел дисциплины , темы раздела	Всего часов	Содержание самостоятельной работы	Форма контроля
1.	Кодирование информации	4	Работа с учебной литературой. Решение задач и выполнение контрольной работы	2КР
2.	Сжатие информации	4	Работа с учебной литературой.	СР
3.	Элементы криптологии	4	Решение задач и выполнение контрольных работ	2КР, СР
4.	Цифровая подпись	4	Работа с учебной литературой	СР
5.	Защита информации	4	Работа с учебной литературой, решение задач	СР

4.8 Содержание самостоятельной работы и формы ее контроля (заочная форма обучения)

№ п/п	Раздел дисциплины , темы раздела	Всего часов	Содержание самостоятельной работы	Форма контроля
1.	Кодирование информации	20	Работа с учебной литературой. Решение задач и выполнение контрольной работы	2КР
2.	Сжатие информации	16	Работа с учебной литературой.	СР
3.	Элементы криптологии	16	Решение задач и выполнение контрольных работ	2КР, СР
4.	Цифровая подпись	16	Работа с учебной литературой	СР
5.	Защита информации	15	Работа с учебной литературой, решение задач	СР

5 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Применение мультимедийного оборудования на лекциях. компьютерных программ MICROSOFT OFFICE, справочно- информационных систем для самостоятельной работы.

5.1 Интерактивные образовательные технологии, используемые в аудиторных занятиях

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
	ЛР	Обмен зашифрованной информацией	8
	ЛР	Расшифровка кодированной информации передаваемой между обучающимися	6
	ЛР	Выявление помех в пересылаемых сообщениях	4
Итого:			18

6 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6.1 Виды контроля и аттестации, формы оценочных средств

№ п/п	Виды контроля и аттестации (ВК, ТАт, ПрАт) ¹	Наименование раздела учебной дисциплины	Оценочные средства*	
			Форма	Количество вопросов в задании
1.	Текущая (Тат)	1,2,3	Тест	99
2.	Текущая (Тат)	4,5	Задачи	30
3.	Промежуточная (ПрАт)	1,2,3,4,5	Вопросы и задача	30

*Фонд оценочных средств для обучающихся по дисциплине «Кодирование и защита информации» приведен в приложении к рабочей программе.

Контрольные вопросы к экзамену

1. Кодирование в двоичном симметричном канале - Модель канала связи, скорость кода, пропускная способность.
2. Теорема Шеннона (без доказательства).
3. Вероятность ошибки декодирования. Стандартное расположение.
4. Синдром. - Поле Галуа, его свойства, примеры полей Галуа. - Линейные коды.
5. Кодирование и декодирование.
6. Общие свойства линейных кодов.
7. Теорема о связи проверочной и порождающей матриц. - Теорема Глаголева.
8. Границы объема кода: граница Синглтона, граница Хэмминга, граница Варшавова-Гилберта.
9. Методы построения новых кодов из заданных. Комбинирование кодов.
10. Теорема Плоткина.
11. Каскадная конструкция. - Совершенные коды.
12. Теорема о существовании совершенных кодов (без доказательства).
13. Коды Хэмминга над $GF(q)$, способы задания, кодирование, декодирование, единственность.
14. Конструкция кодов Васильева, Оценки снизу и сверху числа совершенных кодов. - Циклические коды. Кольцо многочленов над полем Галуа.
15. Определение циклического кода.
16. Теорема о необходимом и достаточном условии существования циклического кода с порождающим многочленом $g(x)$.
17. Кодирование и декодирование циклических кодов.
18. Примеры циклических кодов: коды Хэмминга, коды Боуза-Чоудхури-Хоквингема (БЧХ-коды), коды Рида-Соломона.
19. Сжатие информации - Разделимые и префиксные коды.
20. Стоимость кодирования. Неравенство Крафта-Макмиллана. Теорема Крафта.
21. Теорема МакМиллана. - Оптимальное кодирование.
22. Метод Хаффмена. Метод Фано. - Энтропия. Метод Шеннона для бернуллиевских источников.
23. Теорема Шеннона (с доказательством). - Критерий разделимости побуквенного кодирования.
24. Теоремы Маркова.
25. Алгоритм распознавания разделимости кода. - Универсальное кодирование, теорема Фитингофа. - Код Левенштейна.

26. Код “стопка книг”. - Адаптивные методы сжатия данных.
27. Методы Лемпела-Зива и их модификации. - Адаптивный метод Хаффмена. - Арифметический код.
28. Элементы криптологии - Введение в криптологию.
29. Секретность и имитостойкость. Основные идеи.
30. Криптография и криптоанализ.
31. Криптографические системы с секретными ключами.
32. Подстановки. Перестановки. Полиалфавитные шифры.
33. Шифр с бегущим ключом.
34. Криптографические системы коды. - Теорема
35. Шеннона о существовании совершенно секретных шифров.
36. Стандарт шифрования данных (криптосистема AES, криптосистема ГОСТ, криптосистема DES).
37. Криптографические системы с открытыми ключами.
38. Односторонняя функция с лазейкой. “Шарады” Меркля.
39. Криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма. Криптосистема Шамира.
40. Криптосистема RSA и проблема разложения числа на простые сомножители. - Криптосистема Меркля-Хэллмана, основанная на задаче об укладке ранца.
41. Кодированные системы Мак Эллиса и Нидеррайтера.
42. Цифровая подпись
43. Законы и нормативно-правовые акты.
44. Антивирусы.
45. Помехозащитные коды.

7 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Основная литература

№ п/п	Наименование	Автор(ы)	Год и место издания	Количество экземпляров	
				в библиотеке	на кафедре
1	Кодирование и защита информации : учебное пособие	Акмаров П.Б.	Ижевская ГСХА, 2016	ЭБС «Рукопт» http://rucont.ru/	

7.2 Дополнительная литература

№ п/п	Наименование	Автор(ы)	Год и место издания	Количество экземпляров	
				в библиотеке	на кафедре
1	Основы работы в Excel	Левин Л.А	Красноярск.: КГТИ, 2002	ЭБС»Рукопт» http://rucont.ru/	

7.3 Перечень Интернет-ресурсов

1. Интернет-портал ФГБОУ ВО «Ижевская ГСХА» (<http://portal/izhgsha.ru>);

7.4 Методические указания по освоению дисциплины

Перед изучением дисциплины студенту необходимо ознакомиться с рабочей программой дисциплины, размещенной на портале и просмотреть основную литературу, приведенную в рабочей программе в разделе «Учебно-методическое и информационное обеспечение дисциплины». Книги, размещенные в электронно-библиотечных системах доступны из любой точки, где имеется выход в «Интернет», включая домашние компьютеры и устройства, позволяющие работать в сети «Интернет». Если выявили проблемы доступа к указанной литературе, обратитесь к преподавателю (либо на занятиях, либо через портал академии).

Для изучения дисциплины необходимо иметь чистую тетрадь, объемом не менее 48 листов для выполнения заданий. Перед началом занятий надо бегло повторить материал

из курсов дисциплин «Информатика», «Информационные технологии в экономике». Для изучения 3-го раздела дисциплины необходимо найти в справочно-консультационной системе «Консультант-плюс» (доступ свободный с портала академии) Федеральные законы «О защите информации», «О государственной тайне» и ознакомиться с ними.

Для эффективного освоения дисциплины рекомендуется посещать все виды занятий в соответствии с расписанием и выполнять все домашние задания в установленные преподавателем сроки. В случае пропуска занятий по уважительным причинам, необходимо подойти к преподавателю и получить индивидуальное задание по пропущенной теме.

Полученные знания и умения в процессе освоения дисциплины студенту рекомендуется применять для решения своих задач, не обязательно связанных с программой дисциплины. Например, передать в закодированном виде какое-либо письмо своим друзьям по электронной почте, а потом, при необходимости, помочь декодировать это сообщение. Также консультируйте знакомых пользователей вычислительной техники по вирусам и антивирусным программам.

Владение компетенциями дисциплины в полной мере будет подтверждаться Вашим умением ставить конкретные задачи по кодированию и защите информации, а также выявлять существующие проблемы.

Полученные при изучении дисциплины знания, умения и навыки рекомендуется использовать при выполнении курсовых и дипломных работ(проектов), а также на учебных и производственных практиках.

7.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Поиск информации в глобальной сети Интернет

Работа в электронно-библиотечных системах

Работа в ЭИОС вуза (работа с порталом и онлайн-курсами в системе moodle.izhgsha.ru)

Мультимедийные лекции

Работа в компьютерном классе

При изучении учебного материала используется комплект лицензионного программного обеспечения следующего состава:

1. Операционная система: Microsoft Windows 10 Professional. Подписка на 3 года. Договор № 9-БД/19 от 07.02.2019. Последняя доступная версия программы. Astra Linux Common Edition. Договор №173-ГК/19 от 12.11.2019 г.

2. Базовый пакет программ Microsoft Office (Word, Excel, PowerPoint). Microsoft Office Standard 2016. Бессрочная лицензия. Договор №79-ГК/16 от 11.05.2016. Microsoft Office Standard 2013. Бессрочная лицензия. Договор №0313100010014000038-0010456-01 от 11.08.2014. Microsoft Office Standard 2013. Бессрочная лицензия. Договор №26 от 19.12.2013. Microsoft Office Professional Plus 2010. Бессрочная лицензия. Договор №106-ГК от 21.11.2011. Р7-Офис. Договор №173-ГК/19 от 12.11.2019 г.

Обучающимся обеспечен доступ (удаленный доступ) к следующим современным профессиональным базам данных и информационным справочным системам:

1. Информационно-справочная система (справочно-правовая система) «Консультант-Плюс». Соглашение № ИКП2016/ЛСВ 003 от 11.01.2016 для использования в учебных целях бессрочное. Обновляется регулярно. Лицензия на все компьютеры, используемые в учебном процессе.

8. Материально-техническое обеспечение дисциплины

Тип аудитории	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы
Лекции и практики	Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (лаборатория). Компьютерный класс, укомплектованный специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: компьютеры с необходимым программным обеспечением, выходом в «Интернет» и корпоративную сеть ВУЗа.
Самостоятельная работа	Помещение для самостоятельной работы. (читальный зал) Помещение оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.
Общее помещение для хранения и профилактического обслуживания учебного оборудования	Помещение для хранения и профилактического обслуживания учебного оборудования.

**ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ**

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Таблица 1.1 – Паспорт фонда оценочных средств

Название раздела	Код контролируемой компетенции (или её части)	Оценочные средства для проверки знаний (1-й этап)	Оценочные средства для проверки умений (2-й этап)	Оценочные средства для проверки владений (навыков) (3-й этап)
Кодирование информации	ОПК-2	Компьютерный тест по адресу http://vssoh2.ucoz.ru	Задания 1-8	Задания 17-25
	ПСК-2	Тесты 1-17 Вопросы 1-18	Задания 9-16	Задания 17-25
Сжатие информации	ОПК-2	Вопросы 19-27	Задания 33-34	Задания 35-36
Элементы криптологии	ПК-47 ПСК-2	Вопросы 33-38 Вопросы 28-40	Задания 37-38	Задание 39
Цифровая подпись	ПСК-2	Вопросы 36-43, 45	Задание 44	Задание 45
Защита информации	ОПК-2	Вопросы 43-45	Задания 26-28	Задания 29-32

2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 2.1 – Перечень компетенций

Номер/индекс компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины студент должен:		
		Знать	Уметь	Владеть
ОПК-2	способностью использовать закономерности и методы экономической науки при решении профессиональных задач	Основные законы в области защиты информации	Разрабатывать технологии кодирования и защиты информации	Законными способами получения и защиты информации
ПК-47	способностью применять методы проведения прикладных научных исследований, анализировать и обрабатывать их результаты, обобщать и формулировать выводы по теме исследования	Способы извлечения и восстановления научной информации, передачи ее по каналам связи	Пользоваться электронными системами получения информации и ее анализа	Законными технологиями получения и использования экономической информации
ПСК-2	способность выявлять и использовать взаимосвязь и взаимозависимость экономических и правовых явлений в профессиональной деятельности	Нормативно-правовые акты в сфере защиты информации	Оформлять документацию ограниченного доступа	Средствами электронной защиты информации

3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

3.1 Описание показателей, шкал и критериев оценивания компетенций

Показателями уровня освоенности компетенций на всех этапах их формирования являются:

1-й этап (уровень знаний):

- Умение отвечать на основные вопросы и тесты на уровне понимания сути – удовлетворительно (3).
- Умение грамотно рассуждать по теме задаваемых вопросов – хорошо (4)
- Умение формулировать проблемы по сути задаваемых вопросов – отлично (5)

2-й этап (уровень умений):

- Умение решать простые задачи с незначительными ошибками - удовлетворительно (3).
- Умение решать задачи средней сложности – хорошо (4).
- Умение решать задачи повышенной сложности, самому ставить задачи – отлично (5).

3-й этап (уровень владения навыками):

- Умение формулировать и решать задачи из разных разделов с незначительными ошибками - удовлетворительно (3).
- Умение находить проблемы, решать задачи повышенной сложности – хорошо (4).
- Умение самому ставить задачи, находить недостатки и ошибки в решениях – отлично (5).

3.2 Методика оценивания уровня сформированности компетенций в целом по дисциплине

Уровень сформированности компетенций в целом по дисциплине оценивается на основе результатов текущего контроля знаний в процессе освоения дисциплины – как средний балл результатов текущих оценочных мероприятий в течение семестра;

на основе результатов промежуточной аттестации – как средняя оценка по ответам на вопросы экзаменационных билетов и решению задач;

по результатам участия в научной работе, олимпиадах и конкурсах.

Оценка выставляется по 4-х бальной шкале – неудовлетворительно (2), удовлетворительно (3), хорошо (4), отлично (5).

4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

4.1 Задания

1. Дана кодовая таблица азбуки Морзе:

А • -	Л • - • •	Ц - • - •
Б - • • •	М ---	Ч ---- •
В • - -	Н - •	Ш ---- -
Г - - •	О ----	Щ - - • -
Д - • •	П • - - •	Ъ • - - • - •
Е •	Р • - •	Ы - • - -
Ж • • • -	С • • •	Ь - • • -
З - - • •	Т -	Э • • - • •
И • •	У • • -	Ю • • - -
Й • - - -	Ф • • - •	Я • - • -
К - • -	Х • • • •	

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

----- •----- ••----- ••----- •-----

- Закодируйте с помощью азбуки Морзе слова ИНФОРМАТИКА, ДАННЫЕ, АЛГОРИТМ.
- Закодируйте с помощью азбуки Морзе свое имя и фамилию.
- Мальчик заменил каждую букву своего имени ее номером в алфавите. Получилось 46151. Как зовут мальчика?
- Зашифрованная пословица.
Чтобы рубить дрова, нужен 14, 2, 3, 2, 7, а чтобы полить огород - 10, 4, 5, 1, 6.
Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.
Самый колючий зверь в лесу - это 12, 13.
А теперь прочитайте пословицу: 1, 2, 3, 4, 5, 1, 6 7, 8, 9, 10, 11 9, 4, 7, 4, 13, 12, 14
- Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: "Я УМЕЮ КОДИРОВАТЬ ИНФОРМАЦИЮ". Что необходимо предусмотреть, чтобы зашифрованный текст был записан без пропусков?
- Дана кодировочная таблица (первая цифра кода - номер строки, вторая - номер столбца)

	1	2	3	4	5	6	7	8	9
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	"				

Рис. 1.

. С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ РАБОТАТЬ С ИНФОРМАЦИЕЙ! А ТЫ?

Используя кодировочную таблицу на рис. 1, расшифруйте текст:
25201538350304053835111503040038.

8. Придумайте свою кодировочную таблицу и зашифруйте с ее помощью свой домашний адрес.

9 "Шифр Цезаря". Этот шифр реализует следующее преобразование текста: каждая буква исходного текста заменяется третьей после нее буквой в алфавите, который считается написанным по кругу. Используя этот шифр, зашифруйте слова ИНФОРМАЦИЯ, КОМПЬЮТЕР, ЧЕЛОВЕК.

10. Расшифруйте слово НУЛТХСЁУГЧЛВ, закодированное с помощью шифра Цезаря.

11 "Шифр Виженера". Это шифр представляет шифр Цезаря с переменной величиной сдвига. Величину сдвига задают ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв исходного текста: 31913191и т.д. Используя в качестве ключевого слово ВАГОН, закодируйте слова: АЛГОРИТМ, ПРАВИЛА, ИНФОРМАЦИЯ.

12. Слово НССРХПЛСГХСА получено с помощью шифра Виженера с ключевым словом ВАЗА. Восстановите исходное слово.

13 "Шифр перестановки". Кодирование осуществляется перестановкой букв в слове по одному и тому же общему правилу. Восстановите слова и определите правило перестановки: ЛБКО, ЕРАВШН, УМЫЗАК, АШНРРИ, РКДЕТИ.

14 Зашифруйте, используя "шифр перестановки", слова ИНФОРМАЦИЯ, ПРАВИЛА, АЛГОРИТМ.

15 Придумайте свой шифр перестановки и с его помощью зашифруйте свое имя и фамилию.

16 Какому или каким из перечисленных ниже слов соответствует код Х0:\$=+0=?
Слова: орнамент, доминион, рифление, строение, смекалка.

17 Правило кодирования: после каждой гласной буквы вставляется буква А, а после согласной - Т. Расшифруйте слова: иантфтоартмтааттиактаа, птртиантттеарт.

18 Угадайте правило шифровки и расшифруйте слова: ткафетра, ткнитсни, тицартна, ланигиро.

19 Пользуясь правилом из задачи 15 зашифруйте фразу: ИНФОРМАТИКА - ЭТО НАУКА О СПОСОБАХ ПОЛУЧЕНИЯ, НАКОПЛЕНИЯ, ОБРАБОТКИ, ПЕРЕДАЧИ И ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИИ.

20 Определите правило шифровки и расшифруйте слова:
АКРОЛДИИТРБОФВНАЗНГИЦЕШ
ЩИКНГФЗОЕРУМЦАЫЦГИХИ

21 Для точности передачи сообщений и ликвидации "шумов" в сообщениях используется принцип двукратной последовательной передачи каждого символа. В результате сбоя при передаче информации приемником принята символьная последовательность: "пррраоссптоо". Какое осмысленное сообщение передавалось?

22 Для шифрования каждой буквы используются двузначные числа. Известно, что буква «е» закодирована числом 20. Среди слов «елка», «полка», «поле», «пока», «кол» есть слова, кодируемые последовательностями цифр 11321220, 20121022.

Выясните код слова «колокол».

23 Для пяти букв алфавита заданы их двоичные коды (для некоторых букв – из двух бит, для некоторых – из трех). Эти коды представлены в таблице:

a	b	c	d	e
000	110	01	001	10

Определите, какой набор букв закодирован двоичной строкой 1100000100110.

24 Вася пригласил друга Колю в гости, но не сказал ему код подъезда, а прислал сообщение: «в последовательности цифр 8, 4, 9, 3, 6 все четные цифры разделить на два, а из всех нечетных вычесть 1, затем удалить из последовательности полученных цифр первую и третью». Выполнив действия, указанные в сообщении, какой код цифрового замка получил Коля?

25 Маша забыла пароль для входа в WINDOWS XP, но помнила алгоритм его получения из символов «КВМAM9КВК» в строке подсказки. Если все последовательности символов «МAM» заменить на «RP», а «КВК» на «1212», а из получившейся строки удалить 3 последних символа, то полученная последовательность будет паролем. Назовите пароль

26 Для кодирования сообщения, состоящего только из букв А, В, С, D и Е, используется неравномерный по длине двоичный код:

А	В	С	D	Е
000	11	01	001	10

Какое (только одно!) из четырех полученных сообщений было передано без ошибок и может быть декодировано:

- 1) 110000010011110
- 2) 110000011011110
- 3) 110001001001110
- 4) 110000001011110

27 Для кодирования сообщения, состоящего только из букв О, К, Л, М и Б, используется неравномерный по длине двоичный код:

О	К	Л	М	Б
00	01	11	010	0110

Какое (только одно!) из четырех полученных сообщений было передано без ошибок и может быть декодировано:

- 1) 110001001001110
- 2) 10000011000111010
- 3) 110001001101001
- 4) 1000110001100010

28 На первом месте в цепочке стоит одна из бусин А, Б, В. На втором - одна из бусин Б, В, Г. На третьем месте - одна из бусин А, В, Г, не стоящая в цепочке на первом или втором месте. Задание: выписать все такие цепочки.

29 Для составления цепочек разрешается использовать 5 бусинок, помеченных буквами А Б Е Ж И. Каждая цепочка должна состоять из 4 бусинок, при этом должны соблюдаться правила:

- 1) любая цепочка начинается буквой А
- 2) после гласной буквы не может снова идти гласная, а после согласной - согласная.
- 3) буквы в цепочке не должны повторяться

Задание: выписать все допустимые цепочки.

30 Для составления цепочек разрешается использовать 6 бусинок, помеченных буквами А Б Е Ж И К. Каждая цепочка должна состоять из всех 6 бусинок, при этом должны соблюдаться правила:

- 1) любая цепочка начинается гласной буквой
- 2) после гласной буквы не может снова идти гласная, а после согласной - согласная.
- 3) буквы в цепочке не должны повторяться

Задание: сколько всего существует таких цепочек?

31 Имеется (неизвестное нам) слово из 8 букв. Оно подвергается шифрованию по следующим правилам:

1. На 1-м этапе буквы попарно меняются местами по следующей схеме: 1«3 2«5 4«7 6«8 (то есть меняются местами 1 и 3 буквы, 2 и 5 и так далее).

2. На 2-м этапе для получившейся строки из 8 букв смотрим: если крайние буквы различны по гласности (одна из них - гласная, другая - согласная), то результат шифрования является окончательным, в противном случае получившуюся на предыдущем этапе строку преобразуем по схеме $1 \oplus 2 \oplus 3 \oplus 4 \oplus 5 \oplus 6 \oplus 7 \oplus 8 \oplus 1$ (выполняем циклический сдвиг вправо, то есть первая буква ставится на место второй, вторая - на место третьей, ... последняя - на место первой), после чего снова выполняем этапы 1 - 2. Таким образом, для некоторых исходных слов этапы 1-2 могут повторяться многократно, пока на этапе 1 не получится окончательный результат шифрования.

Задание: в результате шифрования получена строка БИЛКРАКО.

Каким было исходное слово?

32 Имеется исходный набор 8-буквенных слов:

КАРАНДАШ МАРЦИПАН МАРГАРИН МАРТЫШКА ТРЯПОЧКА

Выбрать из этого набора 8-буквенных слов два слова (по своему усмотрению) и зашифровать их по правилам, указанным в задаче 28

33. Выполнить сжатие информации методом RLE по заданию преподавателя, вычислить контрольные суммы и коэффициент сжатия.

34. Выполнить сжатие информации методом Шеннона-Фано, построить кодовое дерево и определить коэффициент сжатия методом Шеннона-Фано

35. Выполнить сжатие информации методом Хаффмана, построить кодовое дерево и определить коэффициент сжатия методом Хаффмана

36. Исследовать эффективность сжатия файлов различных форматов С помощью стандартного архиватора (WinZip, WinRar, 7-Zip и т.п.) выполнить сжатие различных документов, В качестве текстового документа нужно взять файл, который не содержит рисунков. Число символов должно быть более 3000 знаков.

37. Расшифруйте латинскую поговорку, зная, что она зашифрована шифром Цезаря с ключом $k = 5$ (пробелы и запятые - остаются без изменений):

XN ANX UFHJR, UFWF GJQQZR

38. Определите ключ шифра сдвига, которым зашифровано одно из, возможно самых знаменитых, изречений Гая Юлия Цезаря:

MVEZ MZUZ MZTZ

39. Неизвестный русский последователь Цезаря, не ищущий легких путей, использует для шифрования преобразование:

$$C_i = (M_i * k + n) \bmod 32$$

где k и n - натуральные числа, M_i и C_i - коды i -ых символов исходного текста и шифротекста соответственно.

Шифруются только прописные русские буквы, остальные символы остаются без изменений. В частности, при $k = 2$ и $n = 0$ был получен шифротекст:

ВИДРЖ. АИИРЪЪК ЮАКЪВААОЪДАЪРК.

К сожалению, получатель шифротекста так и не смог **правильно** его расшифровать :(При внимательном рассмотрении оказалось, что все дело в выборе параметра k . Найдите все значения параметра k из диапазона $[1, 31]$, использование которых создает нерасшифровываемые шифры.

40. Шифр Цезаря.

Используя шифр Цезаря, зашифруйте свои данные: Фамилию Имя Отчество.

41 Алгоритм шифрования ГОСТ 28147-89.

Выполните первый цикл алгоритма шифрования ГОСТ 28147 89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.

42. Задание №3. Алгоритм шифрования RSA.

Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

43. Функция хеширования.

Найти хеш-образ своей Фамилии, используя хеш-функцию _____, где $n = pq$, p, q взять из Задания №3.

44. Электронная цифровая подпись.

Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA.

45. Используя хеш-образ текстового документа не менее 10 страниц, вычислите электронную цифровую подпись по схеме RSA.

3.2 Тесты

1. Сколько существует в коде Морзе различных последовательностей из точек и тире, длина которых равна 3 символа? _____
2. В алфавите языка племени «тамба-амба» две буквы: Й и Ы.
Сколько различных 5-буквенных слов можно образовать в этом языке? _____
3. Сколько существует различных последовательностей из символов «точка» и «тире» длиной от 2 до 3 символов (включительно)? _____
4. В некоторой стране автомобильный номер длиной 5 символов составляется из заглавных букв (всего используется 5 букв) и десятичных цифр в любом порядке. Каждый символ кодируется одинаковым и минимально возможным количеством битов, а каждый номер — одинаковым и минимально возможным количеством байтов. Сколько байт памяти необходимо для хранения 40 автомобильных номеров? _____
5. Отметьте все префиксные коды (для которых выполняется условие Фано).
 - А-00, Б-01, В-10, Г-11
 - А-00, Б-01, В-1, Г-011
 - А-0, Б-10, В-11, Г-101
 - А-00, Б-10, В-110, Г-111
 - А-0, Б-10, В-110, Г-111
6. Для 5 букв латинского алфавита заданы их двоичные коды: А-000, В-01, С-100, D-10, Е-011. Определите, какой набор букв закодирован двоичной строкой 0110100011000. В ответе запишите цепочку символов без пробелов, например ABCDE. _____
7. Для кодирования некоторой последовательности, состоящей из букв А, Б, В, Г и Д, решили использовать неравномерный двоичный код, позволяющий однозначно декодировать двоичную последовательность, появляющуюся на приёмной стороне канала связи. Использовали код: А-111, Б-110, В-100, Г-0. Укажите, каким кодовым словом может быть закодирована буква Д. Код должен удовлетворять свойству однозначного декодирования. Если можно использовать более одного кодового слова, укажите кратчайшее из них.
 - 001
 - 00
 - 101
 - 10
8. Для кодирования сообщений, состоящих только из букв А, В, С, D и Е, используется неравномерный код: А-00, В-11, С-01, D-010, Е-0110. Определите, какое из приведённых сообщений было передано правильно и может быть декодировано.
 - 110001001001110
 - 10000011000111010
 - 110001001101001



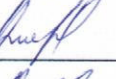


- 1000110001100010
9. Как называется сигнал, который в любой момент времени может принимать любые значения в заданном диапазоне? В ответе введите прилагательное в единственном числе. _____
 10. Каким термином называют представление единого объекта в виде множества отдельных элементов? _____
 11. Какова основная причина перехода от аналоговых сигналов к дискретным в современной технике?
 - надежность передачи данных
 - экономия электроэнергии
 - удобство для пользователя
 - дешевизна электронных устройств
 - упрощение разработки схем
 12. Отметьте все правильные утверждения.
 - дискретизация необходима для хранения данных в памяти компьютера
 - в памяти компьютера можно хранить аналоговые данные
 - при дискретизации, как правило, происходит потеря информации
 - дискретизация не приводит к потере информации
 - органы чувств человека воспринимают дискретные сигналы
 13. Отметьте все утверждения, справедливые для алфавитного подхода к измерению количества информации.
 - количество информации зависит от длины сообщения
 - количество информации зависит от её новизны для получателя
 - учитывается, что одни символы встречаются чаще, а другие - реже
 - количество информации зависит от количества используемых символов
 - чем больше мощность алфавита, тем больше количество информации
 14. Слово TOP закодировано с использованием алфавита из 256 символов. Определите количество информации в этом сообщении в байтах. _____
 15. Слово КИТ закодировано с использованием алфавита из 32 символов. Определите количество информации в этом сообщении в битах. _____
 16. Дан текст из 500 символов. Известно, что символы берутся из таблицы размером 16×16 , в которой все ячейки заполнены разными символами. Определите информационный объём текста в байтах. _____
 17. Для кодирования секретного сообщения используются 12 специальных знаков. При этом символы кодируются одним и тем же минимально возможным количеством битов. Определите информационный объём (в байтах) сообщения длиной в 256 символов? _____

3.3 Вопросы

46. Кодирование в двоичном симметричном канале - Модель канала связи, скорость кода, пропускная способность.
47. Теорема Шеннона (без доказательства).
48. Вероятность ошибки декодирования. Стандартное расположение.
49. Синдром. - Поле Галуа, его свойства, примеры полей Галуа. - Линейные коды.
50. Кодирование и декодирование.
51. Общие свойства линейных кодов.
52. Теорема о связи проверочной и порождающей матриц. - Теорема Глаголева.
53. Границы объема кода: граница Синглтона, граница Хэмминга, граница Варшамова-Гилберта.
54. Методы построения новых кодов из заданных. Комбинирование кодов.
55. Теорема Плоткина.
56. Каскадная конструкция. - Совершенные коды.
57. Теорема о существовании совершенных кодов (без доказательства).

58. Коды Хэмминга над $GF(q)$, способы задания, кодирование, декодирование, единственность.
59. Конструкция кодов Васильева, Оценки снизу и сверху числа совершенных кодов. - Циклические коды. Кольцо многочленов над полем Галуа.
60. Определение циклического кода.
61. Теорема о необходимом и достаточном условии существования циклического кода с порождающим многочленом $g(x)$.
62. Кодирование и декодирование циклических кодов.
63. Примеры циклических кодов: коды Хэмминга, коды Боуза-Чоудхури-Хоквингема (БЧХ-коды), коды Рида-Соломона.
64. Сжатие информации - Разделимые и префиксные коды.
65. Стоимость кодирования. Неравенство Крафта-Макмиллана. Теорема Крафта.
66. Теорема МакМиллана. - Оптимальное кодирование.
67. Метод Хаффмена. Метод Фано. - Энтропия. Метод Шеннона для бернуллиевских источников.
68. Теорема Шеннона (с доказательством). - Критерий разделимости побуквенного кодирования.
69. Теоремы Маркова.
70. Алгоритм распознавания разделимости кода. - Универсальное кодирование, теорема Фитингофа. - Код Левенштейна.
71. Код “стопка книг”. - Адаптивные методы сжатия данных.
72. Методы Лемпела-Зива и их модификации. - Адаптивный метод Хаффмена. - Арифметический код.
73. Элементы криптологии - Введение в криптологию.
74. Секретность и имитостойкость. Основные идеи.
75. Криптография и криптоанализ.
76. Криптографические системы с секретными ключами.
77. Подстановки. Перестановки. Полиалфавитные шифры.
78. Шифр с бегущим ключом.
79. Криптографические системы коды. - Теорема
80. Шеннона о существовании совершенно секретных шифров.
81. Стандарт шифрования данных (криптосистема AES, криптосистема ГОСТ, криптосистема DES).
82. Криптографические системы с открытыми ключами.
83. Односторонняя функция с лазейкой. “Шарады” Меркля.
84. Криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма. Криптосистема Шамира.
85. Криптосистема RSA и проблема разложения числа на простые сомножители. - Криптосистема Меркля-Хэллмана, основанная на задаче об укладке ранца.
86. Кодрующие системы Мак Эллиса и Нидеррайтера.
87. Цифровая подпись
88. Законы и нормативно-правовые акты.
89. Антивирусы.
90. Помехозащитные коды.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номер измененного листа	Дата внесения изменения и номер протокола	Подпись ответственного за внесение изменений
1	10-23	29.08.2018 №1	
2	10-23	30.08.2019 №1	
3	10-23	28.08.2020 №1	
4	12-13	20.11.2020 №3	
5	12-13	31.08.2021 №1	
6			