



Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



«УТВЕРЖДАЮ»

Проректор по учебно-методической работе

Н.В. Бабина

«28» апреля 2020 г.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

**ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«ТЕОРИЯ ИНФОРМАЦИИ»

Направление подготовки: 10.03.01 Информационная безопасность

**Профиль: Информационно-аналитические системы
финансового мониторинга**

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

Автор: к.в.н., доцент Воронов А.Н. Рабочая программа дисциплины: «Теория информации». – Королев МО: «Технологический университет», 2020.

Рецензент: к.в.н., доцент Соляной В.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания кафедры	Протокол № 8 от 26.03.2020			

Рабочая программа согласована:

Руководитель ОПОП ВО

к.в.н., доцент Воронов А.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания УМС	№ 7 от 28.04.2020			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является:

Формирование у студентов специализированной базы знаний по основам теории информации и кодирования сообщений и получение первичных навыков по анализу состояния информационных систем в соответствии с требованиями защиты информации.

Общепрофессиональные компетенции:

- ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач.

Профессиональные компетенции:

- ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.

Основными **задачами** дисциплины являются:

- ознакомление студентов с основными положениями теории информации и кодирования, а также с основными методами определения, свойств, характеристик и параметров систем защиты информации;
- формирование у студентов способности самостоятельно определять информационные потери в каналах связи, строить оптимальные коды, обнаруживать и исправлять ошибки при различных методах обработки и передачи информации;
- проводить анализ состояния и перспектив развития систем защиты информации с помощью современных методов, и средств в различных организационных структурах.

После завершения освоения данной дисциплины студент должен:

Знать:

- основные методологические принципы теории информации и кодирования сообщений;
- основные положения теорем Шеннона для информационных каналов, их следствия и практическое применение;
- порядок формирования и использования статистических моделей каналов связи и их особенности;
- порядок обнаружения и исправления ошибок в обрабатываемых и передаваемых сообщениях;

- основные методы и средства линейного и структурного кодирования информации и особенности их применения;
- особенности защиты и кодирования информации на объектах различного профиля.

Уметь:

- правильно применять на практике структурные, статистические и семантические меры информации и оценивать их результаты;
- осуществлять классификацию статистических и математических моделей каналов связи и передачи информации, анализировать их параметры и характеристики;
- обнаруживать и исправлять ошибки при передаче и обработке информации на стандартной аппаратуре;
- правильно применять методы и средства линейного и структурного кодирования информации в целях её защиты;
- использовать существующие теоретические подходы информационной безопасности при выборе соответствующих способов и средств защиты, а также при расчётах их характеристик и основных показателей;

Владеть:

- методикой выявления и анализа основных параметров вероятностной схемы оценки информации и сообщений;
- последовательностью применения основных методик обнаружения и исправления ошибок при передаче и обработке информации;
- методикой грамотного применения на практике оптимального кодирования и сжатия обрабатываемой и передаваемой информации в ходе её защиты.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Теория информации» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность», профиль: «Информационно-аналитические системы финансового мониторинга».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Безопасность жизнедеятельности», «Экономика предприятия и организация производства», «Документоведение» и компетенциях: ОК-2,4,7, ОПК-5,6, ПК-7.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Техническая защита информации», «Методы защиты на рынке корпоративного контроля», «Национальная система по противодействию легализации преступных доходов и финансированию терроризма», прохождения практики, государственной

итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 4 зачетных единицы, 1454 часов.

Таблица 1

Виды занятий	Всего часов	Семестр 3	Семестр 4	Семестр ...	Семестр ...
Общая трудоемкость	144	144			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	96	96			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	T1; T2	T1; T2			
КСР	-	-			
Вид итогового контроля	Зачёт с оценкой	Зачёт с оценкой			

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час Очное	Занятия в интерактивной форме, час	Код компетенций
Тема 1. Основы теории информации.	2	4	2	ОПК-2, ПК-11
Тема 2. Основные параметры вероятностной схемы информационной системы и их характеристика.	2	4	2	ОПК-2, ПК-11
Тема 3. Обзор теорем Шеннона для каналов связи и	2	4	2	ОПК-2, ПК-11

информации.				
Тема 4. Характеристика статистических моделей каналов связи.	2	4	2	ОПК-2, ПК-11
Тема 5. Оптимальное кодирование информации и обнаружение ошибок в сообщениях.	2	4	2	ОПК-2, ПК-11
Тема 6. Линейное кодирование информации и циклические коды.	2	4	2	ОПК-2, ПК-11
Тема 7. Декодирование циклических кодов и методика исправления ошибок при обработке и обмене информацией.	2	4	3	ОПК-2, ПК-11
Тема 8. Сжатие и структурное кодирование информации.	2	4	3	ОПК-2, ПК-11
Итого:	16	32	18	

4.2. Содержание тем дисциплины

Тема 1. Основы теории информации.

Краткая историческая справка о развитии теории информации и систем передачи сообщений (систем связи). Понятие информации и информационных метрик. Структурные меры информации и их характеристика. Особенности геометрической и комбинаторной мер информации, порядок их применения в теории информации.

Тема 2. Основные параметры вероятностной схемы информационной системы и их характеристика.

Энтропия, как мера степени неопределённости защищаемой системы. Основные единицы измерения энтропии и их характеристика. Основные свойства энтропии простой информационной системы и их особенности. Понятие энтропии и математического ожидания в теории информации и связи.

Тема 3. Обзор теорем Шеннона для каналов связи и информации.

Понятие количества информации в дискретном сообщении. Дискретные источники сообщений без памяти и с памятью. Характеристика избыточности дискретного источника сообщений. Прямая и обратная теоремы Шеннона для канала связи без шума и порядок их доказательства. Практическое применение и следствия теоремы Шеннона для дискретного постоянного канала с шумом. Характеристика и особенности применения метода Фано.

Тема 4. Характеристика статистических моделей каналов связи.

Общая схема передачи информации. Понятие каналов связи их классификация и особенности. Источники и потребители информации. Особенности непрерывных каналов связи и их основные параметры. Особенности дискретных каналов связи и их основные параметры. Влияние шумов на пропускную способность дискретного канала связи.

Тема 5. Оптимальное кодирование информации и обнаружение ошибок в сообщениях.

Понятие оптимальных безизбыточных кодов и их характеристика. Префиксные коды, методика их формирования и особенности применения. Понятие квазиоптимальных кодов, характеристика кодов Хаффмана. Доказательство неравенства Крафта и его основные теоремы. Информационная избыточность и границы для средней длины кодов. Понятие абсолютной и относительной корректирующей избыточности и порядок их определения.

Тема 6. Линейное кодирование информации и циклические коды.

Особенности линейного кодирования информации. Основные свойства помехоустойчивых кодов и порядок их применения при передаче сообщений. Параметры помехоустойчивых кодов и как их определить, граничные соотношения между параметрами помехоустойчивых кодов. Классификация помехоустойчивых кодов. Основные параметры и свойства линейных кодов и кода Хэмминга, порядок их применения.

Тема 7. Декодирование циклических кодов и методика исправления ошибок при обработке и обмене информацией.

Методика применения кодов, исправляющих одиночную ошибку в передаваемых сообщениях. Основные требования к декодированию циклических кодов. Методика применения кодов, обнаруживающих трёхкратные ошибки в сообщениях. Особенности построения и применения циклических кодов (кодов BCH), исправляющих две и большее количество ошибок при обмене информацией.

Тема 8. Сжатие и структурное кодирование информации.

Понятие сжатия информации в соотношении с кодированием данных, определение сжатого кода, основные цели его использования. Основные методы сжатия информации и их характеристика. Примеры сжатия информации различными методами. Суть и особенности применения метода Лавинского для сжатия информации в памяти персональных компьютеров. Основные понятия структурного кодирования данных и условные особенности применения этого типа кодирования. Понятия последовательных структур данных и характеристика их элементов. Однонаправленные и двунаправленные строки в памяти компьютера, понятие однонаправленных и двунаправленных списков.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине.

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Теория информации» приведена в Приложении 1.

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

Основная литература:

1. Анисимов А.А. Менеджмент в сфере информационной безопасности. Учебное пособие. – М.: Интернет – Университет информационных технологий / БИНОМ. Лаборатория знаний, 2010.
2. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность. Учебное пособие. – М.: «ФОРУМ», 2011.
3. Воронов А.Н. Теоретические основы защиты информации. Учебное пособие. – Королёв МО: КИУЭС, 2011.
4. Баранова Е.К. Основы информатики и защиты информации. Учебное пособие. – М.: РИОР: «ИНФРА-М», 2013.

Дополнительная литература:

1. Белов В.М., Новиков С.Н., Солонская О.И. Теория информации. Курс лекций. Учебное пособие для вузов. – М.: «Горячая линия – Телеком», 2012.
2. Гохберг Г.С., Зафиевский А.В., Короткин А.А. Информационные технологии. Учебник. – М.: Издательский центр «Академия», 2012.

Рекомендуемая литература:

1. Духин А.А. Теория информации. Учебное пособие. – М.: «Гелиос-АРВ», 2007.
2. Лидовский В.В. Теория информации. Учебное пособие. – М.: «Спутник», 2004.
3. Цымбал В.П. Теория информации и кодирование. Учебник. – Киев:«Выща школа», 1992.

Электронные книги:

1. Управление информационной безопасностью. Практические правила.

http://www.100balov.com/data/ukr/IInfo_dlya_stydena_12/1_1743.doc

2. Обеспечение информационной безопасности бизнеса.

<http://detectivebooks.ru/author/76454196/>

3. Управление информационной безопасностью.

http://romangamma.ucoz.ru/_ld/0/5____.pdf

4. Политики безопасности компании при работе в Интернет

http://bookz.ru/authors/sergei-petrenko/politiki_424/1-politiki_424.html

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
2. <http://informika.ru/> – образовательный портал.
3. <http://www.academy.it.ru/> – академия АЙТИ.

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice, PowerPoint.
- **Информационные справочные системы:**
 1. Ресурсы информационно-образовательной среды.
 2. Рабочая программа и методическое обеспечение по дисциплине: «Теория информации»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

***ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО
ДИСЦИПЛИНЕ**

**«ТЕОРИЯ ИНФОРМАЦИИ»
(Приложение 1 к рабочей программе)**

Направление подготовки: 10.03.01 «Информационная безопасность»

**Профиль: Информационно-аналитические системы
финансового мониторинга**

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

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

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач	Тема:1,2,3,4,5,6,7,8	<ul style="list-style-type: none"> • основные методологические принципы теории информации и кодирования сообщений; • основные положения теорем Шеннона для информационных каналов, их следствия и практическое применение; • порядок формирования и использования статистических моделей каналов связи и их особенности; • порядок обнаружения и исправления ошибок в обрабатываемых и передаваемых сообщениях; 	<ul style="list-style-type: none"> • правильно применять на практике структурные статистические и семантические меры информации и оценивать их результаты; • осуществлять классификацию статистических и математических моделей связи и передачи информации анализировать их параметры и характеристики; • обнаруживать и исправлять ошибки при передаче и обработке информации на стандартной аппаратуре; 	<ul style="list-style-type: none"> • методикой выявления и анализ основных параметров вероятностной схемы оценки информации сообщений; • последовательностью применения основных методик обнаружения и исправления ошибок при передаче и обработке информации;
2.	ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.	Тема:1,2,3,4,5,6,7,8	<ul style="list-style-type: none"> • основные методы и средства линейного и структурного кодирования информации и особенности их 	<ul style="list-style-type: none"> • правильно применять методы и средства линейного и структурного кодирования информации в целях её защиты; • использовать 	<ul style="list-style-type: none"> • методикой грамотного применения на практике оптимального кодирования и сжатия обрабатываемой и передаваемой информации в ходе её защиты.

				<p>применения;</p> <ul style="list-style-type: none"> • особенности защиты и кодирования информации на объектах различного профиля. 	<p>ать существующие теоретические подходы информационной безопасности при выборе соответствующих способов и средств защиты, а также при расчётах их характеристик и основных показателей;</p>	
--	--	--	--	--	---	--

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-2, ПК-11	Доклад в форме презентации	<p>А) полностью сформирована 5 баллов</p> <p>В) частично сформирована 3-4 балла</p> <p>С) не сформирована 2 балла</p>	<p>Проводится устно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <p>1. Соответствие представленной презентации заявленной тематике (1 балл).</p> <p>2. Качество источников и их количество при подготовке доклада и разработке презентации (1 балл).</p> <p>3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).</p> <p>4. Качество самой представленной презентации (1 балл).</p> <p>5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).</p> <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.</p>

3. 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

Примерная тематика докладов в форме презентации:

1. Сравнение значений энтропии соответствующих вероятностных схем, реализующихся при извлечении одного сообщения из каждого ансамбля сообщений.
2. Определение энтропии вероятностной схемы, вероятности исходов которой определяются распределением Пуассона.
3. Расчёт величины энтропии дискретной вероятностной схемы если максимальное значение вероятностей исходов сообщений уменьшается.

4. Сравнение значений энтропий для трёх вероятностных схем, вероятностные распределения которых заданы различными плотностями.
5. Исследование энтропии непрерывной вероятностной схемы как выпуклой вверх функции в области всех функций плотности вероятности.
6. Определение математического ожидания и дисперсии количества символов, порождённых неким источником сообщений без памяти.
7. Определение минимального среднего числа символов на сообщение для источника без памяти при кодировании их двоичными последовательностями.
8. Определение условий построения двоичного префиксного кода для заданных длин кодовых слов источника без памяти и будет ли такой код однозначно декодируемым?
9. Исследование двоичного префиксного кода со 100 кодовыми словами, у которого длина каждого слова определена, будет ли такой код оптимальным?
10. Условия применения неравенства Крафта для источников с бесконечным алфавитом и конечной энтропией.
11. Методика построения двоичного кода сообщения с использованием алгоритма Фано для источника без памяти и определение средней длины кода.
12. Методика построения двоичного кода сообщения с использованием алгоритма Шеннона для источника без памяти и определение средней длины кода.
13. Методика построения двоичного кода сообщения с использованием алгоритма Хаффмана для источника без памяти и определение средней длины кода.
14. Методика построения троичного префиксного кода сообщения с использованием алгоритма Хаффмана для источника без памяти и определение средней длины кода.
15. Определение вероятности ошибки декодирования сообщений при передаче по двоичному симметричному каналу равновероятных кодовых слов линейного кода, задаваемого порождающей матрицей.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Теория информации» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов

Согласно учебному плану	тестирование	ОПК-2, ПК-11	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Согласно учебному плану	тестирование	ОПК-2, ПК-11	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно учебному плану	Зачёт с оценкой	ОПК-2, ПК-11	3 вопроса	Зачёт с оценкой проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачёта	Критерии оценки: « Отлично »: <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных

					<p>теорий, изучаемых предметов;</p> <ul style="list-style-type: none"> • ответ на вопросы билета. <p>«Хорошо»:</p> <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание <p>«Удовлетворительно»:</p> <ul style="list-style-type: none"> • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практически
--	--	--	--	--	---

					<p>х занятиях; «Неудовлетворительно»:</p> <ul style="list-style-type: none"> • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.
--	--	--	--	--	--

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один или несколько вариантов ответа.

1. Что понимают под теорией информации?

– это наука, изучающая способы и закономерности шифрования информационных сообщений;

– это наука, изучающая количественные закономерности защиты информации и информационных объектов;

– это наука, изучающая количественные закономерности, связанные с получением, обработкой, передачей и хранением информации;

2. Кто и когда впервые применил телеграф для передачи информации?

– американский изобретатель Алмон Строуджер в 1889 году;

– русский учёный электротехник Шиллинг в 1832 году;

– немецкие учёные Карл Гаусс и Вильгельм Вебер в 1833 году;

- английский изобретатель Дэвид Юз в 1855 году.
3. Кто и когда впервые изобрёл первую конструкцию телефона?
- немецкий физик Иоганн Филипп Рейс в 1861 году;
 - английский физик Максвэлл в 1867 году;
 - американский изобретатель Александр Грэм Белл в 1876 году;
 - немецкий физик Артур Корн в 1904 году.
4. Кто впервые осуществил приём радиоволн с использованием антенного устройства?
- итальянский радиотехник Маркони;
 - английский физик Максвэлл;
 - русский физик А. С. Попов;
 - немецкий физик Артур Корн.
5. В какой стране впервые была осуществлена телепередача цветного подвижного изображения?
- в Германии;
 - в России;
 - во Франции.
 - в Америке;
6. Кому принадлежит определение информации как соотношения между сообщением и его потребителем, как способ передачи сведений от одного субъекта к другому?
- Хартли;
 - Винеру;
 - Колмогорову;
 - Котельникову.
7. В каких формах существует информация?
- символы;
 - сведения;
 - коды;
 - сообщения.
8. Выберите знаменитых учёных, которые внесли существенный вклад в развитие теории информации:
- А. Н. Колмогоров;
 - Альберт Эйнштейн;
 - Клод Шеннон;
 - Ральф Хартли.
9. Выберите основные признаки информации:

- количественный;
- функциональный;
- детерминированный;
- качественный.

10. Кто и когда сформулировал основополагающий принцип, положенный в основу теории информации;

- Франциск Скорина в XVI веке;
- Самуэль Фенли Близ Морзе в 1832 году;
- Франклин Фишер в 1921 году;
- Гарри Найквист в 1924 году.

11. Какие направления включает теория по определению количества информации?

- структурное;
- вероятностное;
- статистическое;
- семантическое.

12. Что такое метрика?

– это категория, выражающая единство качества и количества объекта и указывающая на предел, за которым изменение количества влечёт за собой изменение качества;

– это средство, на основании которого производится оценка, определение или классификация чего-либо, как мерило оценки.

– это соразмерность, которая лежит в основе измерения ритма и гармонии окружающего нас мира.

– это математический термин, определяющий формулу или правило для определения расстояния между двумя любыми точками (элементами) данного пространства (множества);

13. Кто явился основоположником семантической теории определения количества информации?

- Шеннон;
- Хартли;
- Харкевич;
- Бернулли.

14. Какие меры подсчёта количества информации применяют при структурном подходе в теории информации?

- геометрическая;
- комбинаторная;
- аддитивная;
- статистическая.

15. В каких случаях применяют комбинаторную меру определения количества информации?

- в случаях, когда количество информации сводится к измерению длины, площади или объёма геометрической модели информационной системы;
- в случаях, когда оценку информационных систем осуществляют с учётом статистических характеристик информации;
- в случаях, когда необходимо оценить возможность передачи информации при помощи различных сочетаний информационных элементов;
- в случаях, когда оценка информации осуществляется по тому эффекту, который она оказывает на результат управления в системах управления.

16. Что понимается под энтропией в теории информации по Шеннону?

- это мера вероятности пребывания системы в заданном состоянии;
- это мера степени неопределённости состояний физической системы;
- это степень взаимозависимости системы, состоящей из множества элементов;
- это математическое ожидание апостериорной вероятности состояний элементов физической системы.

17. Выберите приемлемые единицы измерения энтропии дискретного сигнала в теории информации:

- биты;
- ваты;
- ниты;
- диты.

18. Где используют понятие условная энтропия в теории информации?

- при определении взаимозависимости между символами кодируемого алфавита;
- при ранжировании символов в кодовом сообщении;
- при определении метода сжатия информации для размещения её в памяти ПК.
- для определения потерь при передаче информации по каналам связи;

19. Что такое энтропия объединения сообщений?

- это среднее количество информации, приходящееся на каждый символ отправляемого сообщения ансамбля «А» или ансамбля «В»;
- это среднее значение полученных адресатом сообщений ансамбля «В», при условии, что передавались сообщения ансамбля «А»;
- это среднее количество информации при совместном появлении символов ансамблей «А» и «В» в принятом сообщении.

20. Выберите типы источников информации, рассматриваемые в теории информации:

- марковские;
- резидентурные;
- бернуллиевские;
- комбинаторные.

21. Что понимается под сообщением в теории информации?

- форма представления элемента с помощью физической величины;
- информационный процесс, в отношении которого необходимо обеспечить соответствующую защиту;
- порция информации, передаваемой в системе с коммутацией данных;
- совокупность элементов, узлов и блоков, объединённых в общую законченную конструкцию.

22. Выберите типы сигналов, рассматриваемые в теории информации:

- аналоговые;
- дискретизированные;
- квантованные;
- генетические.

23. Существует ли эргодический источник информации?

- да;
- нет.

24. Чем можно измерить количество информации, содержащееся в дискретном сообщении по Шеннону?

- произведением длительности сигнала, полосы пропускания и логарифма уровня помех;
- суммой логарифмов априорной и апостериорной вероятностей того, что принятый сигнал содержит передаваемое сообщение;
- произведением объёма импульсов, способных принимать некоторое значение и градации уровня передаваемого сигнала;
- разностью логарифмов апостериорной и априорной вероятностей того, что принятый сигнал содержит передаваемое сообщение.

25. Что показывает искусственно созданная избыточность информации для источника сообщений?

- сколько дополнительных компонентов источника может быть задействовано с целью повышения надёжности и работоспособности системы;
- каково максимальное число символов кода в сообщениях источника;
- какую долю максимально возможной неопределённости символов при заданном объёме алфавита не использует источник сообщений;

– какова степень близости неравномерных состояний источника к оптимальному значению.

26. Первая теорема Шеннона рассматривает кодирование информации и передачу сообщений в канале связи с помехами?

- да;
- нет.

27. Что понимается под эффективностью кода?

- величина, характеризующая среднюю избыточность кода по отношению к передаваемому сообщению;
- величина, характеризующая абсолютную недогруженность источника на каждый символ кодируемого сообщения;
- величина, характеризующая разрешённые кодовые комбинации с постоянным соотношением символов в передаваемом сообщении.
- величина, характеризующая степень близости неравномерного статистического кода к оптимальному;

28. Учитывает ли вторая теорема Шеннона вероятность ошибки кодирования информации при передаче сообщений по дискретному постоянному каналу?

- да;
- нет.

29. На какие типы делят каналы связи в зависимости от характера сигналов, передаваемых по ним?

- статистические;
- дискретные;
- комбинаторные;
- аналоговые.

30. Каковы пределы полосы пропускания частот, воспринимаемые человеческим ухом?

- 300 – 3400 Гц;
- 16 Гц – 20 КГц;
- 50 – 300 Гц;
- 100 Гц – 10 КГц.

31. Полоса пропускания является характеристикой непрерывных каналов связи?

- да;
- нет.

32. Что понимают под белым шумом в каналах связи?

- если мощность помех в канале является непрерывной случайной величиной, подчиняющаяся нормальному статистическому распределению;
- если отношение средних мощностей помехи и сигнала в канале связи является величиной неизменной при передаче сигнала;
- если в пределах полосы пропускания канала средняя мощность помех оказывается одинаковой на всех её частотах, а вне этой полосы она равна нулю;
- если средняя мощность помех в канале связи оказывается достаточно мала и стремится к нулю, а вне полосы пропускания она максимальна.

33. Что понимается под пропускной способностью Гауссовского канала передачи информации?

- удельная скорость передачи информации в нормированной полосе пропускания канала;
- максимально достижимая скорость передачи информации при заданном качестве;
- среднее количество передаваемой информации на одно сообщение;
- отношение энергии передаваемого сигнала к спектральной плотности некоторого порогового нормального шума сигнала.

34. Когда дискретный канал называют однородным каналом?

- когда влияние помех всё время одинаково;
- когда отсутствует корреляция знаков в сообщении;
- когда задано время одного элементарного сигнала;
- когда пропускная способность канала не изменяется.

35. Как определить степень загрузки канала связи с помехами?

- вычислением логарифма количества элементарных сигналов в сообщении;
- вычислением разности числа контрольных разрядов и числа информационных знаков в сообщении;
- вычислением отношения количества информации в сообщении к длительности сигнала в канале связи;
- вычислением отношения производительности источника сообщений к пропускной способности канала связи.

4.2 Типовые вопросы, выносимые на зачёт с оценкой

1. Определение дискретных ансамблей и источников сообщений.
2. Количество информации в дискретном сообщении, особенности его определения.
3. Обоснование логарифмической меры в определении количества информации и особенности её применения.
4. Определение и свойства энтропии ансамбля дискретных сообщений.

5. Определение совместной энтропии ансамблей дискретных сообщений, основные её свойства и условия применения.
6. Особенности энтропии дискретного стационарного источника сообщений и энтропии объединения.
7. Определение и характеристики избыточности и безизбыточности источника дискретных сообщений.
8. Определение кодирования информации, понятие эффективного кодирования сообщений.
9. Постановка задачи равномерного кодирования источника и характеристика её основных этапов.
10. Теорема о высоковероятных множествах дискретного источника без памяти, условия её доказательства.
11. Определение типичных и нетипичных множеств для дискретных источников сообщений без памяти, особенности их применения.
12. Особенности определения энтропии источника сообщений без памяти как скорости создания информации.
13. Понятие неравномерного кодирования сообщений с однозначным декодированием и особенности его применения.
14. Понятие оптимальных неравномерных двоичных кодов и особенности их применения, префиксные коды и их характеристика.
15. Характеристика метода Шеннона-Фано и особенности его применения при кодировании информации.
16. Характеристика метода Хаффмана при кодировании информации и особенности его применения.
17. Определение каналов связи их основные характеристики и классификация.
18. Понятие количества информации, передаваемое по каналу связи и его характеристика.
19. Понятие взаимной информации, её основные свойства и характеристики.
20. Информационные характеристики системы передачи дискретных сообщений и порядок их определения.
21. Понятие пропускной способности канала связи и особенности его определения.
22. Порядок кодирования источника сообщений в симметричном канале без помех.
23. Определение двоичного симметричного канала связи со стиранием информации и порядок определения пропускной способности симметричного канала без памяти.
24. Постановка задачи кодирования информации в дискретном канале с помехами и характеристика её основных этапов.
25. Прямая теорема Шеннона для кодирования информации в дискретных каналах без памяти и особенности её применения.
26. Обратная теорема Шеннона для кодирования информации в дискретных каналах без памяти и особенности её применения.
27. Основные ограничения возможности использования оптимального кодиро-

- вания на практике и их характеристика.
28. Характеристика принципов помехоустойчивого кодирования блоками конечной длины.
 29. Понятия непрерывных ансамблей сообщений и источников информации, основные особенности их применения.
 30. Информационные характеристики непрерывных ансамблей сообщений, порядок их определения.
 31. Определение пропускной способности непрерывного канала связи и особенности её применения.
 32. Основные теоремы кодирования информации для непрерывного канала без памяти с дискретным временем, условия их применения.
 33. Понятие эффективности систем передачи информации и их предельные возможности по Шеннону.
 34. Понятия критериев качества воспроизводимых сообщений, порядок их определения.
 35. Общее определение энтропии и её основные возможности.
 36. Порядок использования энтропии гауссовского источника информации без памяти.
 37. Понятие квантования непрерывной случайной величины и особенности её применения.
 38. Особенности отображения ансамбля сообщений множеством значений на числовой оси.
 39. Характеристика теоремы «Закон больших чисел в форме Чебышева» и особенности её применения.
 40. Определение теоремы Котельникова и порядок её применения в теории информации.
 41. Порядок доказательства неравенства Крафта и условия его применения.
 42. Понятие дискретных во времени цепей Маркова и особенности их применения.
 43. Особенности использования конечных дискретных Марковских источников информации с памятью.
 44. Основные понятия арифметического кодирования и особенности его применения.
 45. Характеристика методики кодирования Лемиеля-Зива и особенности его применения.
 46. Основные определения кодов Хэмминга и особенности их применения.
 47. Основные определения БЧХ кодов и особенности их применения.
 48. Понятие порождающая матрица в теории информации и особенности её применения.
 49. Основные понятия и определения циклических кодов, особенности их применения в теории информации.
 50. Основные понятия и определения структурного кодирования и сжатия информации, особенности их применения.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

***ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО
ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**«ТЕОРИЯ ИНФОРМАЦИИ»
(Приложение 2 к рабочей программе)**

Направление подготовки: 10.03.01 «Информационная безопасность»

**Профиль: Информационно-аналитические системы
финансового мониторинга**

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Общие положения

Цель дисциплины:

Формирование у студентов специализированной базы знаний по основам теории информации и кодирования сообщений и получение первичных навыков по анализу состояния информационных систем в соответствии с требованиями защиты информации.

Задачи дисциплины:

- ознакомление студентов с основными положениями теории информации и кодирования, а также с основными методами определения, свойств, характеристик и параметров систем защиты информации;
- формирование у студентов способности самостоятельно определять информационные потери в каналах связи, строить оптимальные коды, обнаруживать и исправлять ошибки при различных методах обработки и передачи информации;
- проводить анализ состояния и перспектив развития систем защиты информации с помощью современных методов, и средств в различных организационных структурах.

2. Указания по проведению практических занятий

Тема 1. Основы теории информации.

Практическое занятие 1.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки систем и процессов управления информационной безопасностью

Учебные вопросы:

1. Особенности аддитивной меры информации и порядок её применения для защиты сообщений.
2. Особенности статистической меры информации и порядок её применения для защиты сообщений.
3. Особенности семантической меры информации и порядок её применения для защиты сообщений.

Время проведения занятия – 4 ч.

Тема 2. Основные параметры вероятностной схемы информационной системы и их характеристика.

Практическое занятие 2.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки о политике безопасности отдельных структур

Учебные вопросы:

1. Понятие условной энтропии и порядок её применения в теории информации и связи.
2. Понятие энтропии объединения и порядок её применения в теории информации и связи.
3. Применение энтропии в каналах связи с влиянием помех или нормального шума.

Время проведения занятия – 4 ч.

Тема 3. Обзор теорем Шеннона для каналов связи и информации.

Практическое занятие 3.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в организационно-кадровых и технических аспектах управления информационной безопасностью

Учебные вопросы:

1. Статистический анализ случайных последовательностей и особенности его применения.
2. Энтропийные характеристики случайных последовательностей и порядок их определения.
3. Другие информационные характеристики случайных последовательностей и порядок их определения.

Время проведения занятия – 4 ч.

Тема 4. Характеристика статистических моделей каналов связи.

Практическое занятие 4.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки оценки эффективности управления ИБ

Учебные вопросы:

1. Основные качественные показатели систем передачи информации и их особенности.
2. Скорость передачи информации в дискретных и непрерывных каналах при наличии помех и как её определить
3. Понятие пропускной способности систем передачи информации и как её определить.

Время проведения занятия – 4 ч.

Тема 5. Оптимальное кодирование информации и обнаружение ошибок в сообщениях.

Практическое занятие 5.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки оценки эффективности управления ИБ

Учебные вопросы:

1. Методика обнаружения и исправления ошибок в сообщениях.
2. Основные условия обнаружения одиночной ошибки в сообщениях.
3. Идея коррекции ошибок в сообщениях и методика её применения.
4. Понятие нижней границы Хэмминга и понятие верхней границы Варшамова-Гильберта в методике коррекции ошибок.

Время проведения занятия – 4 ч.

Тема 6. Линейное кодирование информации и циклические коды.

Практическое занятие 6.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки оценки эффективности управления ИБ

Учебные вопросы:

1. Определение и свойства двоичных циклических кодов в передаче сообщений.
2. Особенности применения систематических циклических кодов.
3. Методика обнаружения пакетов ошибок с помощью циклических кодов.

Время проведения занятия – 4 ч.

Тема 7. Декодирование циклических кодов и методика исправления ошибок при обработке и обмене информацией.

Практическое занятие 7.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки оценки эффективности управления ИБ

Учебные вопросы:

1. Методика обнаружения и исправления ошибок при передаче и обработке информации на телефонной аппаратуре.
2. Методика обнаружения и исправления ошибок при передаче и обработке информации на телеграфной аппаратуре.

3. Методика обнаружения и исправления ошибок при передаче и обработке информации на персональных компьютерах и в сети.
4. Особенности применения комбинированного инверсного кода для исправления одиночных и двойных ошибок в передаваемых комбинациях сообщений.
Время проведения занятия – 4 ч.

**Тема 8. Сжатие и структурное кодирование информации.
Практическое занятие 8.**

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки оценки эффективности управления ИБ

Учебные вопросы:

1. Основные параметры данных, представленных в памяти компьютера и степень эффективности хранения данных в форме таблиц.
2. Характеристика способа логических шкал для экономии памяти и особенности его применения.
3. Особенности применения кольцевых структур в организации памяти персонального компьютера и кодировании данных.

Время проведения занятия – 4 ч.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

- 1) расширить представление в области существующих современных аппаратных средств вычислительной техники;
- 2) привить навыки самостоятельного решения нестандартных задач в области аппаратных средств вычислительной техники.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	Очная форма обучения
	Всего академических часов
Всего часов на самостоятельную работу	96
Вопросы, выносимые на самостоятельное изучение	70
Подготовка к практическим занятиям	8
Подготовка к лабораторным занятиям	-
Подготовка докладов	10
Выполнение практических заданий	8

**Вопросы, выносимые на самостоятельное изучение:
для очной формы обучения:**

1. Исследование верхней и нижней границы оценки для взаимной информации через расстояние по вариации для случайных величин, принимающих конечное число значений.
2. Исследование асимптотики эpsilon-энтропии сфер и шаров в хэмминговом пространстве, в предположении, что размерность пространства стремится к бесконечности.
3. Анализ асимптотических границ для кратных упаковок информации в пространстве “q-ичных” последовательностей длины “n” и особенности их поведения.
4. Обзор вероятностных характеристик случайных упаковок информации евклидова пространства и их особенности.
5. Определение пропускной способности квантового произвольно меняющегося канала, необходимые и достаточные условия положительной пропускной способности.
6. Методика применения асимптотически оптимальных недвоичных кодов для передачи информации по каналу с ошибками и бесшумной обратной связью.
7. Анализ условий, при которых отдельные классы кодов с простой структурой и свободные от перекрытий являются оптимальными при передаче информации.

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	70	Изучение открытых источников
2.	Подготовка к практическим занятиям	8	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	-	
4.	Тематика докладов	10	1. Внутренние аппаратные средства персонального компьютера 2. Внешние периферийные устройства персонального компьютера
5.	Выполнение практических	8	Разработка аппаратного средства

	заданий		вычислительной техники по заданным характеристикам
--	---------	--	--

Примерные темы докладов

1. Исследование границы Грея-Рэнкина для двоичных кодов и анализ суще
2. кодов, достигающих этой границы.
3. Анализ конструкции многочленов кодированной информации, модуль три
4. суммы которых достигает границы Вейля.
5. Обзор современных аналитических методов исследования при выработке нестационарных решений в модифицированной модели Клейрока.
6. Анализ новых подходов в описании и построении отслеживающих кодов и особенности их применения.
7. Анализ новых алгоритмов списочного декодирования кодов Рида-Маллера
8. и особенности их применения в условиях частично-ошибочных и неизвестных данных.
9. Определение и условия применения эргодических источников информации, доказательство теоремы Мак-Миллана.
10. Методика построения линейных двоичных кодов, достигающих границы Варшамова-Гилберта и особенности их применения.
11. Методика построения и условия применения в теории информации алгебро-геометрических кодов сообщений.

5. Указания по проведению контрольных работ

Не предусмотрено учебным планом

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Анисимов А.А. Менеджмент в сфере информационной безопасности. Учебное пособие. – М.: Интернет – Университет информационных технологий / БИНОМ. Лаборатория знаний, 2010.
2. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность. Учебное пособие. – М.: «ФОРУМ», 2011.
3. Воронов А.Н. Теоретические основы защиты информации. Учебное пособие. – Королёв МО: КИУЭС, 2011.
4. Баранова Е.К. Основы информатики и защиты информации. Учебное пособие. – М.: РИОР: «ИНФРА-М», 2013.

Дополнительная литература:

1. Белов В.М., Новиков С.Н., Солонская О.И. Теория информации. Курс лекций. Учебное пособие для вузов. – М.: «Горячая линия – Телеком», 2012.
2. Гохберг Г.С., Зафиевский А.В., Короткин А.А. Информационные технологии. Учебник. – М.: Издательский центр «Академия», 2012.

Рекомендуемая литература:

1. Духин А.А. Теория информации. Учебное пособие. – М.: «Гелиос-АРВ», 2007.
2. Лидовский В.В. Теория информации. Учебное пособие. – М.: «Спутник», 2004.
3. Цымбал В.П. Теория информации и кодирование. Учебник. – Киев: «Выща школа», 1992.

Электронные книги:

1. Управление информационной безопасностью. Практические правила.

http://www.100balov.com/data/ukr/IInfo_dlya_stydena_12/1_1743.doc

2. Обеспечение информационной безопасности бизнеса.

<http://detectivebooks.ru/author/76454196/>

3. Управление информационной безопасностью.

http://romangamma.ucoz.ru/_ld/0/5____.pdf

4. Политики безопасности компании при работе в Интернет

http://bookz.ru/authors/sergei-petrenko/politiki_424/1-politiki_424.html

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
2. <http://informika.ru/> – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. <http://www.academy.it.ru/> – академия АЙТИ.
7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации
8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации.

9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности
<http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине «Теория информации».