

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Смирнов Сергей Николаевич  
Должность: врио ректора  
Дата подписания: 16.10.2023 21:45:02  
Уникальный программный ключ:  
69e375c64f7e975d4e8830e7b4fcc2ad1bf35f08

Министерство науки и высшего образования Российской Федерации  
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:  
Руководитель ООП  
Н.А. Семькина  
*Семькина*  
«4» 09  
МАТЕМАТИЧЕСКИЙ  
ФАКУЛЬТЕТ  
УНИВЕРСИТЕТ

Рабочая программа дисциплины (с аннотацией)  
**Алгоритмы кодирования информации**

Специальность  
**10.05.01 Компьютерная безопасность**

Специализация  
*Математические методы защиты информации*

Для студентов 5 курса очной формы обучения

Составитель:

*Л. Чагу*

к.ф.м.н., доцент  
*Чагурова Л.А.*

## I. Аннотация

### 1. Наименование дисциплины

Алгоритмы кодирования информации.

### 2. Цели и задачи дисциплины

Целями освоения дисциплины являются: получение представлений о подходах к кодированию информации, а также о связи между способом кодирования информации и сложностью последующей обработки кодов.

Дисциплина «Алгоритмы кодирования информации» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует фундаментализации образования, формированию мировоззрения и развитию логического мышления.

### 3. Место дисциплины в структуре ООП подготовки специалиста

Дисциплина относится к вариативной части математического и естественнонаучного цикла.

Предварительные знания, необходимые для освоения дисциплины, — это знания, полученные в курсе «Математическая логика и теория алгоритмов», «Теория алгоритмов», «Дискретная математика», «Математический анализ», «Алгебра».

Знания, полученные при изучении дисциплины, помогают обучаемым глубже понимать проблемы, связанные с цифровым представлением различных задач.

### 4. Объём дисциплины:

3 зачётные единицы, 108 академических часов, в том числе

**контактная работа:** лекции 30 часов, практические занятия 15 часов,

**самостоятельная работа:** 63 часа.

### 5. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
<b>Базовый уровень</b> <b>ПК-5.</b> Способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.	<b>Владеть:</b> навыками конфигурирования и администрирования ОС; методиками анализа системного трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками настройки межсетевых экранов. <b>Уметь:</b> формулировать и настраивать политику безопасности основных ОС, а так же локальных компьютерных сетей, построенных на их основе; использовать средства обнаружения вторжений для защиты информации в сетях. <b>Знать:</b> механизмы реализации атак в сетях, реализующих протоколы Интернет транспортного и сетевого уровня; принципы формирования комплекса мер по обеспечению информационной безопасности; защитные механизмы и средства обеспечения сетевой безопасности; защита в ОС; средства и методы предотвращения и обнаружения вторжений; способы и средства защиты информации от утечки по техническим каналам.
<b>Базовый уровень</b> <b>ПК-10.</b> Способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.	<b>Владеть:</b> необходимыми теоретическими знаниями в областях, связанных с оценкой эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах. <b>Уметь:</b> проводить анализ эффективности и надежности защиты в ОС; выявлять уязвимости в защите ОС; планировать политику безопасности ОС; пользоваться средствами защиты, предоставляемыми ОС. <b>Знать:</b> требования к защищенным ОС; критерии оценки эффективности и надежности средств защиты ОС; защитные механизмы и средства обеспечения безопасности современных операционных систем.

<p><b>Базовый уровень</b>  <b>ПК-18.</b> Способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.</p>	<p><b>Владеть:</b> практическими навыками установки, наладки, тестирования и обслуживания современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем.  <b>Уметь:</b> производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем.  <b>Знать:</b> современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем, включая средства криптографической защиты информации.</p>
--	---

**6. Формы промежуточной аттестации**  
зачёт.

**7. Язык преподавания** – русский.