МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО Руководитель ОПОП	УТВЕРЖДАЮ Зав. кафедрой ПМИ
_____М.В. Коломина	_____М.В. Коломина
«8» сентября 2022 г.	«8» сентября 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптография»

Составитель	**Станкевич А.С., к.т.н., доцент ФИТиП, ИТМО**
Направление подготовки / специальность	**01.03.02 Прикладная математика и информатика**
Направленность (профиль) ОПОП	**Программирование и искусственный интеллект**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная**
Год приёма	**2023**
Курс	**3**
Семестр(ы)	**6**

Астрахань – 2022

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целью освоения дисциплины «Криптография» является ознакомление студентов с методами информационной безопасности и их использованием в области защиты информации.

1.2. Задачи освоения дисциплины:

- формирование основных понятий и методов криптографии;
- научить отбирать технологии работы с информацией в зависимости от класса задач в области данных;
- сформировать навыки кодирования и шифрования данных;
- сформировать навык применения алгоритмов криптозащиты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина «Криптография» к части, формируемой участниками образовательных отношений (элективным дисциплинам) и осваивается в 6 семестре.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями):

- Дискретная математика
- Линейная алгебра
- Введение в программирование
- Введение в цифровую культуру

Знания: основные понятия дискретной математики, принципы передачи и хранения информации, а также о мерах информации, основных угроз безопасности информации и методов защиты данных

Умения: определять угрозы информационной безопасности, применять математические методы для решения типовых задач, составлять алгоритмы, с использованием основных алгоритмических структур.

Навыки: критического мышления, анализировать сложные проблемы, связанные с безопасностью данных, и находить оптимальные решения

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

Теория кодирования

Проектирование программного обеспечения

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки / специальности:

а) профессиональных (ПК 24)

ПК-24. Способен планировать и организовывать свою деятельность в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта и требований информационной безопасности.

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)

ПК-24.	ИПК-24.1.1. Текущее состояние информационного общества и роль искусственного интеллекта в его развитии ИПК-24.1.2. Классификацию информационных систем и систем искусственного интеллекта, функциональность программного обеспечения для решения задач профессиональной деятельности ИПК-24.1.3. Современное состояние информационно-коммуникационных технологий в мире и перспективы их развития ИПК-24.1.4. Основные методы оценки экономической эффективности применяемого программного и аппаратного обеспечения	ИПК-24.2.1. Анализировать сущность и значение искусственного интеллекта в развитии современного информационного общества ИПК-24.2.2 Выбирать необходимые инструментальные средства анализа для решения поставленных задач ИПК-24.2.3. Формировать и использовать критерии оценки эффективности применения программного и аппаратного обеспечения в профессиональной деятельности	ИПК-24.3.1 Навыками выбора современных технологий и систем искусственного интеллекта для решения задач в профессиональной деятельности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Объём дисциплины составляет 4 зачётных единицы, в том числе 54 часа, выделенных на контактную работу обучающихся с преподавателем (из них 18 часов – лекции, 36 часов – лабораторные работы), и 90 часов – на самостоятельную работу обучающихся.

Таблица 2 – Структура и содержание дисциплины

Раздел, тема дисциплины (модуля)	Семестр	Контактная работа (в часах)			Самост. работа		Форма текущего контроля успеваемости, форма промежуточной аттестации
		Л	ПЗ	ЛР	КР	СР	
Криптография. Основные положения	6	9		18		45	лабораторная работа, домашнее задание
Криптографические и технические методы защиты информации	6	9		18		45	лабораторная работа, домашнее задание
Итого		18		36		90	Диф. зачёт

Таблица 3 – Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции	Общее количество компетенций
		ПК-24	
Криптография. Основные положения	72	+	1
Криптографические и технические методы защиты информации	72	+	1
Итого	144		1

Краткое содержание каждой темы дисциплины (модуля)

1. Криптография. Основные положения

Блочные шифры. Классификация блочных шифров. Режимы использования блочных шифров. Режимы использования блочных шифров. Режим простой замены. Режим шифрования с зацеплением. Режим обратной связи по шифротексту. Режим шифрования с обратной связью по выходу, Поточные шифры. Классификация поточных шифров. Регистр сдвига с линейной обратной связью. Линейная сложность. Алгоритм Берлекэмпа-Мэсси. Нелинейные регистры сдвига с обратной связью. Нелинейная комбинация генераторов. Алгоритм SEAL. Линейное и предварительное шифрование. Методы получения случайных и псевдослучайных чисел. Анализ генераторов псевдослучайных чисел. Гаммирование. Шифр RC 4. Роторные машины, Криптографические средства. Основные понятия криптографии.

Функции, используемые в криптографических системах. Однонаправленные функции, Имитостойкость. Криптографическая стойкость. Практическая криптографическая стойкость

2. Криптографические и технические методы защиты информации

Системы обнаружения утечек, Межсетевое экранирование, Криптографические методы защиты информации, Монитор обращений, Разграничение доступа, Системы обнаружения вторжений, Анализатор сетевого трафика, Симметричные алгоритмы шифрования. DES (Data Encryption Standard). ГОСТ 28147–89 Криптографические алгоритмы с открытым ключом Электронно-цифровая подпись

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

Лекционные занятия

Основной формой реализации теоретического обучения является лекция, которая представляет собой систематическое, последовательное изложение преподавателем-лектором учебного материала теоретического характера. Цель лекции – организация целенаправленной познавательной деятельности студентов по овладению программным материалом учебной дисциплины.

Порядок подготовки лекционного занятия включает в себя выполнение следующих этапов:

- изучение требований программы дисциплины;
- определение целей и задач лекции;
- разработка плана проведения лекции;
- подбор литературы (ознакомление с методической литературой, публикациями периодической печати по теме лекционного занятия);
- отбор необходимого и достаточного по содержанию учебного материала;
- определение методов, приемов и средств поддержания интереса, внимания, стимулирования творческого мышления студентов;
- написание конспекта лекции.

Лекция должна включать следующие разделы:

- формулировку темы лекции;
- указание основных изучаемых разделов или вопросов и предполагаемых затрат времени на их изложение;
- изложение вводной части;
- изложение основной части лекции;
- краткие выводы по каждому из вопросов;
- заключение;
- рекомендации литературных источников по излагаемым вопросам.

Лабораторные занятия

Лабораторное занятие − целенаправленная форма организации педагогического процесса, направленная на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Они развивают научное мышление и речь, позволяют проверить знания студентов и выступают как средства оперативной обратной связи.

Правильно организованные лабораторные занятия ориентированы на решение следующих задач:

- обобщение, систематизация, углубление, закрепление полученных на лекциях и в процессе самостоятельной работы теоретических знаний по дисциплине (предмету);

- формирование практических умений и навыков, необходимых в будущей профессиональной деятельности, реализация единства интеллектуальной и практической деятельности;
- выработка при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Состав заданий для лабораторного занятия должен быть спланирован с расчетом, чтобы за отведенное время они могли быть качественно выполнены большинством учащихся.

Лабораторные занятия должны так быть организованы, чтобы студенты ощущали нарастание сложности выполнения заданий, испытывали бы положительные эмоции от переживания собственного успеха в учении, поисками правильных и точных решений.

Самостоятельная работа

Самостоятельная работа – это вид учебной деятельности, которую студент совершает в установленное время и в установленном объеме индивидуально или в группе, без непосредственной помощи преподавателя (но при его контроле), руководствуясь сформированными ранее представлениями о порядке и правильности выполнения действий.

В учебном процессе образовательного учреждения выделяются два вида самостоятельной работы:

- аудиторная – выполняется на учебных занятиях, под непосредственным руководством преподавателя и по его заданию (выполнение самостоятельных работ; выполнение контрольных и практических работ; решение задач);
- внеаудиторная – выполняется по заданию преподавателя, но без его непосредственного участия (подготовка к аудиторным занятиям; изучение учебного материала, вынесенного на самостоятельную проработку; выполнение домашних заданий разнообразного характера; выполнение индивидуальных заданий, направленных на развитие у студентов самостоятельности и инициативы; подготовка к контрольной работе). Внеаудиторные самостоятельные работы представляют собой логическое продолжение аудиторных занятий, проводятся по заданию преподавателя, который инструктирует студентов и устанавливает сроки выполнения задания.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Лекция

- Лекция – основной вид обучения в вузе.
- В лекции излагаются основные положения теории, ее понятия и законы, приводятся факты, показывающие связь теории с практикой.
- Накануне лекции необходимо повторить содержание предыдущей лекции (а также теорию по изучаемой теме в школьных учебниках геометрии, если эта тема была представлена в них), а затем посмотреть тему очередной лекции по программе (по плану лекций).

Лабораторное занятие

- Лабораторное занятие – наиболее активный вид учебных занятий в вузе. Он предполагает самостоятельную работу над лекциями и учебными пособиями.
- К каждому лабораторному занятию нужно готовиться. Подготовку следует начинать с повторения теории (по записям лекций или по учебному пособию). После этого нужно решать задачи из предложенного домашнего задания.

Организация самостоятельной работы

Самостоятельность в учебной работе способствует развитию заинтересованности студента в изучаемом материале, вырабатывает у него умение и потребность самостоятельно получать знания, что весьма важно для специалиста с высшим образованием. Самостоятельная работа студентов представлена в следующих формах:

- работа с учебной литературой и конспектом лекций с целью подготовки к лабораторным занятиям, составление конспектов тем, выносимых на самостоятельную проработку;
- систематическое выполнение домашних работ.

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер раздела (темы)	Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Раздел 1	Криптография. Основные положения	45	Изучение теоретического материала. Подготовка к лабораторным работам и домашним заданиям
Раздел 2	Криптографические и технические методы защиты информации	45	Изучение теоретического материала. Подготовка к лабораторным работам и домашним заданиям

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины (модуля), выполняемые обучающимися самостоятельно

Домашнее задание:

При выполнении домашнего задания предусмотрено два варианта задач.
Количество задач в каждом варианте: две задачи.
Форма выдачи задания обучающимся: студенты получают задание на электронную почту с комментарием преподавателя и сроком предоставления решения.
Форма представления обучающимися решения задач/домашнего задания: решения задач предоставляются в письменном или электронном виде.

Лабораторные работы выполняются в рамках каждого раздела курса с целью усвоения прослушанного студентом теоретического материала.
Объем выполненной работы: каждая лабораторная работа содержит 3-5 задач.
Срок сдачи работы: работы должны быть сданы в период прочтения курса. Сдача работы представляет собой предоставление отчёта в свободной форме в письменном или электронном виде и, в случае необходимости, устные ответы на уточняющие вопросы по отдельным задачам.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине «Криптография» могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line или off-line в формах.

Таблица 5. Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Криптография. Основные положения	Обзорная лекция	Не предусмотрено	Выполнение лабораторных работ
Криптографические и технические методы защиты информации	Лекция-диалог	Не предусмотрено	Выполнение лабораторных работ

6.2. Информационные технологии

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

- система управления обучением LMS Moodle;
- использование возможностей Интернета в учебном процессе (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т.д.);
- использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источник информации;
- использование возможностей электронной почты;
- использование средств представления учебной информации (электронных учебных пособий, применение новых технологий для проведения занятий с использованием презентаций и т.д.);
- использование интерактивных средств взаимодействия участников образовательного процесса (технологии дистанционного или открытого обучения в глобальной сети);
- использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс).

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Пакет офисных программ
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Google Chrome	Браузер
OpenOffice	Пакет офисных программ

6.3.2. Современные профессиональные базы данных и информационные справоч-ные системы

1. Электронная библиотека «Астраханский государственный университет» собственной генерации на платформе ЭБС «Электронный Читальный зал – БиблиоТех». https://biblio.asu.edu.ru
2. Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента». www.studentlibrary.ru.
3. Электронная библиотечная система издательства ЮРАЙТ, раздел «Легендарные книги». www.biblio-online.ru
4. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем». https://library.asu.edu.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине «Криптография» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе

освоения образовательной программы определяется последовательным освоением дисциплин и прохождением практик, а в процессе освоения дисциплины– последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие разделов, тем дисциплины, результатов обучения по дисциплине и оценочных средств

№ п/п	Контролируемые разделы, темы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1	Криптография. Основные положения	ПК-24	лабораторные работы, домашние задания
2	Криптографические и технические методы защиты информации	ПК-24	лабораторные работы, домашние задания

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задания

7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Домашнее задание

При выполнении домашнего задания предусмотрено два варианта задач.
Количество задач в каждом варианте: две задачи.
Форма выдачи задания обучающимся: студенты получают задание на электронную почту с комментарием преподавателя и сроком предоставления решения.
Форма представления обучающимися решения задач/домашнего задания: решения задач предоставляются в письменном или электронном виде.
Сроки представления решения: решения предоставляются в срок, указанный преподавателем.

Примеры заданий:
Задача 1.

Известно, что три числа a_1, a_2, a_3 были получены следующим образом. Сначала выбрали натуральное число A и нашли числа $A_1 = [A]_{16}, A_2 = [A/2]_{16}, A_3 = [A/4]_{16}$, где $[X]_{16}$ – остаток от деления целой части числа X на 16 (например, $[53/2]_{16} = 10$). Затем было выбрано целое число B такое, что $0 \le B \le 15$. Числа A_1, A_2, A_3 и B записывают в двоичной системе счисления, т.е. представляют каждое из них в виде цепочки из 0 и 1 длины 4, приписывая слева необходимое число нулей. Такие цепочки условимся складывать посимвольно «в столбик» без переносов в следующий разряд согласно правилу: $1+1=0+0=0$ и $0+1=1+0=1$, а саму операцию посимвольного сложения обозначим символом $\oplus$. Например, $3 \oplus 14 = (0011) \oplus (1110) = (1101) = 13$. Положим $a_1 = A_1 \oplus B$, $a_2 = A_2 \oplus B$, $a_3 = A_3 \oplus B$. Найдите все возможные значения числа a_3, если известно, что $a_1 = 10, a_2 = 4$.

Задача 2.

Для прохода в учреждение необходимо предъявить пятизначную комбинацию, состоящую из нулей и единиц. Устройство распознавания представляет собой упрощённую модель нейрона – клетки головного мозга (см. рис. 6).

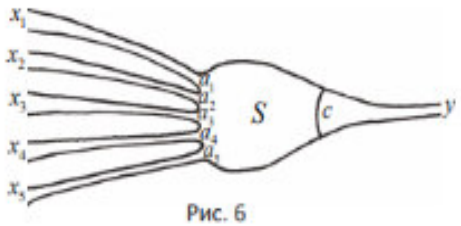

Рис. 6

Пятизначная комбинация x_1, x_2, x_3, x_4, x_5 по пяти каналам поступает в клетку, где её компоненты умножаются на фиксированные целые числа a_1, a_2, a_3, a_4, a_5, и вычисляется сумма $S = a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + a_5x_5$. Проход в учреждение открывается, только если $S \geq c$, где c – некоторое фиксированное целое число. В табл. 1 представлены те комбинации, при предъявлении которых проход открывается, а в табл. 2 – для которых проход закрыт.

Таблица 1

1,0,1,1,0	1,1,0,1,0	1,1,1,1,1

Таблица 2

1,0,1,0,0	0,0,1,1,0	1,1,0,1,1	1,0,1,1,1

Найдите ещё одну комбинацию, открывающую проход в учреждение.

Лабораторная работа 1

Лабораторная работа выполняется в рамках каждого раздела курса с целью усвоения прослушанного студентом теоретического материала.

Объем выполненной работы: каждая лабораторная работа содержит 3-5 задач.

Срок сдачи работы: работы должны быть сданы в период прочтения курса. Сдача работы представляет собой предоставление отчёта в свободной форме в письменном или электронном виде и, в случае необходимости, устные ответы на уточняющие вопросы по отдельным задачам.

Примеры заданий к лабораторной работе «Криптография. Основные положения»

1. Определить частотные характеристики криптограммы, для чего рассчитать значение частоты встречаемости символов j Am в криптограмме.

2. Определить вероятностные характеристики алфавита, для чего вычислить значение логарифма вероятности встречаемости символа log ( ) 1p j для заданного алфавита. Полученные значения свести в таблицу 1.

Таблица 1.

Буква	А	Б	…	Ю	Я
$j \in A_m$					
$\log p_1(j)$					
$\nu_j(Y)$					

3. В соответствии с выражением (1) определить значение логарифма функции правдоподобия l(K) и построить соответствующую графическую зависимость.

4. Определить в соответствии с выражением (1) оценку ключа * k .

5. Дешифровать заданную криптограмму, используя оценку ключа * k . При получении осмысленного текста подготовить отчет и представить его преподавателю.

Порядок предоставления отчета по работе

Отчет по лабораторной работе представляется в печатном виде в формате, предусмотренном шаблоном отчета по лабораторной работе. Время, отводимое на выполнение – 4 часа. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя.

Шаблон отчета по лабораторной работе

Отчет по лабораторной работе № ____

«*Название лабораторной работы*»

1. Цель и задачи лабораторной работы: ____
2. Методика проведения исследования: ____
3. Анализ погрешностей: ____
4. Результаты: ____
5. Выводы: ____

Требования к выполнению лабораторной работы

Отчеты по лабораторным работам должны быть отправлены на электронную почту преподавателя не позднее, чем через две недели после выдачи задания. Полученные выводы и графический материал должны быть информативными и корректными.

Контрольная работа

Контрольная выполняется по вариантам (2 варианта).

Бланки с заданиями (перечнем терминов) выдаются преподавателем на практическом занятии по окончании изучения дисциплины. Студенту необходимо вписать свои ФИО и группу, выполнить задание и сдать преподавателю на проверку.

Время выполнения – 10 минут.

Комплект заданий для контрольной работы:

1. Дайте определение ключа подстановочного шифра
2. Дайте определение модулярного шифра
3. Дайте определение периодического шифра Хилла
4. Сформулируйте последовательность действий при помощи шифрования цифрового сообщения в криптосистеме RSA

Шкала оценивания и критерии оценки:

Лабораторная работа 2

Лабораторная работа выполняется в рамках каждого раздела курса с целью усвоения прослушанного студентом теоретического материала.

Объем выполненной работы: каждая лабораторная работа содержит 3-5 задач.

Срок сдачи работы: работы должны быть сданы в период прочтения курса. Сдача работы представляет собой предоставление отчёта в свободной форме в письменном или электронном виде и, в случае необходимости, устные ответы на уточняющие вопросы по отдельным задачам.

Примеры заданий к лабораторной работе «Криптографические методы защиты информации»

1. Зашифруйте шифром Чейза слово «Криптография».
2. Зашифруйте усложненным шифром Чейза слово «Криптография».
3. Почему использование любого другого числа кроме 9, влечет за собой нестыковки при шифровании?
4. Зашифруйте шифром Порта слово «Криптография» используя произвольный лозунг.
5. Зашифруйте шифром Ришелье слово «Криптография».
6. Зашифруйте слово «Криптография» используя шифр гаммирования с произвольным ключом.

7. Зашифруйте анаграммой словосочетание «Криптостойкий Алгоритм», допустив замену Й на И.
8. Предложите программную реализацию RC4 на известном языке программирования.

Порядок предоставления отчета по работе

Отчет по лабораторной работе представляется в печатном виде в формате, предусмотренном шаблоном отчета по лабораторной работе. Время, отводимое на выполнение – 4 часа. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя.

Шаблон отчета по лабораторной работе

Отчет по лабораторной работе № ____

«*Название лабораторной работы*»

1. Цель и задачи лабораторной работы: ____
2. Методика проведения исследования: ____
3. Анализ погрешностей: ____
4. Результаты: ____
5. Выводы: ____

Требования к выполнению лабораторной работы

Отчеты по лабораторным работам должны быть отправлены на электронную почту преподавателя не позднее, чем через две недели после выдачи задания. Полученные выводы и графический материал должны быть информативными и корректными.

Перечень вопросов, выносимых на дифференцированный зачет

1. Криптографические средства.
2. Функции, используемые в криптографических системах.
3. Однонаправленные функции.
4. Имитостойкость.
5. Криптографическая стойкость.
6. Практическая криптографическая стойкость.
7. Поточные шифры.
8. Классификация поточных шифров.
9. Регистр сдвига с линейной обратной связью.
10. Линейная сложность.
11. Алгоритм Берлекэмпа-Мэсси.
12. Нелинейные регистры сдвига с обратной связью.
13. Нелинейная комбинация генераторов.
14. Алгоритм SEAL.
15. Линейное и предварительное шифрование.
16. Методы получения случайных и псевдослучайных чисел.
17. Анализ генераторов псевдослучайных чисел.
18. Гаммирование.
19. Шифр RC 4.
20. Роторные машины
21. Блочные шифры.
22. Классификация блочных шифров.
23. Режимы использования блочных шифров.
24. Режим простой замены.
25. Режим шифрования с зацеплением.
26. Режим обратной связи по шифротексту.
27. Режим шифрования с обратной связью по выходу.
28. Симметричные алгоритмы шифрования.
29. DES (Data Encryption Standard).
30. ГОСТ 28147–89

31. Криптографические алгоритмы с открытым ключом
32. Электронно-цифровая подпись
33. Криптографические методы защиты информации. Межсетевое экранирование
34. Разграничение доступа.
35. Монитор обращений
36. Системы обнаружения вторжений
37. Анализатор сетевого трафика
38. Системы обнаружения утечек

Порядок формирования билета:
Билеты состоят из 2-х вопросов:
1 вопрос – с 1 по 19 вопрос из перечня вопросов к экзамену;
2 вопрос – с 20 по 38 вопрос из перечня вопросов к экзамену.
Пример билета № 1
1. Вопрос «Однонаправленные функции»
2. Вопрос «Криптографические алгоритмы с открытым ключом»

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-24. Способен планировать и организовывать свою деятельность в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта и требований информационной безопасности				
1.	Задание закрытого типа	*Выберите верный ответ*. Что требуется для восстановления зашифрованного текста? а. ключ б. матрица в. вектор г. пароль	а	1-3
2.		*Выберите верный ответ*. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования? а. 1 б. 2 в. 3 г. 4	а	1-3
3.		*Выберите верный ответ*. Сколько используется ключей в системах с открытым ключом? а. 1 б. 2 в. 3 г. 4	б	1-3
4.		*Выберите верный ответ*. Символы исходного текста складываются с символами некой случайной последовательности - это...	а	1-3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		а. алгоритм гаммирования б. алгоритм перестановки в. алгоритм аналитических преобразований		
5.		*Выберите верный ответ*. Из скольки последовательностей состоит расшифровка текста по таблице Вижинера? а. 2 б. 3 в. 4 г. 5	б	1-3
6.	Задание открытого типа	Дайте определение термину *Шифрование*.	Шифрование - это способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого.	2-5
7.		В чем заключается суть метода перестановки?	Для метода перестановки характерно следующее: символы шифруемого текста представляются по определенным правилам внутри шифруемого блока символов.	2-5
8.		Сформулируйте несколько общепринятых требований для современных криптографических систем защиты информации.	1. Знание алгоритма шифрования не должно влиять на надежность защиты. 2. Структурные элементы алгоритма шифрования должны быть неизменными. 3. Не должно быть простых и легко устанавливаемых зависимостью между ключами последовательно используемых в процессе шифрования. 4. Зашифрованное сообщение должно подаваться чтению только при наличии ключа.	2-5
9.		Дайте краткое определение шифру RC4.	RC4 — потоковый шифр, широко применяющийся в различных системах защиты информации в компьютерных сетях (например, в протоколах SSL и TLS, алгоритмах обеспечения безопасности беспроводных сетей WEP и WPA). Шифр разработан компанией RSA Security, и для его использования требуется лицензия. Алгоритм RC4, как и любой потоковый шифр, строится на основе генератора псевдослучайных битов. На вход генератора записывается ключ, а	5-8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			на выходе читаются псевдослучайные биты. Длина ключа может составлять от 40 до 2048 бит. Генерируемые биты имеют равномерное распределение. Основные преимущества шифра: высокая скорость работы; переменный размер ключа.	
10.		Дайте краткую характеристику алгоритму SEAL.	EAL— симметричный поточный алгоритм шифрования данных, оптимизированный для программной реализации. Разработан в IBM Филом Рогэвеем в 1993 году. Алгоритм оптимизирован и рекомендован для 32-битных процессоров. Для работы ему требуется кэш-память на несколько килобайт и восемь 32-битовых регистров. Скорость шифрования — примерно 4 машинных такта на байт текста. Для кодирования и декодирования используется 160-битный ключ. Чтобы избежать нежелательной потери скорости по причине медленных операций обработки ключа, SEAL предварительно выполняет с ним несколько преобразований, получая в результате три таблицы определённого размера. Непосредственно для шифрования и расшифрования текста вместо самого ключа используются эти таблицы. Алгоритм считается очень надёжным, очень быстрым и защищён патентом США № 5454039 с декабря 1993 года.	8-10
11.	Задание комбинированного типа	*Верно ли утверждение:* Блок-схема алгоритма ГОСТ отличается от блок-схемы DES-алгоритма длиной ключа. *Поясните ответ.*	Утверждение неверно, поскольку блок-схема алгоритма ГОСТ отличается от блок-схемы DES-алгоритма отсутствием начальной перестановки и числом циклов шифрования, а не длиной ключа.	2-5

7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Лабораторные работы*	4/10	40	
2.	*Домашние задания*	3/10	30	
3.	*Контрольная работа*	1/20	20	
Всего			**90**	-
Блок бонусов				
4.	*Посещение занятий*		5	
5.	*Своевременное выполнение всех заданий*		5	
Всего			**10**	-
ИТОГО			**100**	-

Таблица 11 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	Зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	Не зачтено

При реализации дисциплины в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

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

8.1. Основная литература

1. Hopcroft J. E., Motwani R., Ullman J. D. Introduction to Automata Theory, Languages, and Computation (3rd Edition). — Addison-Wesley, Boston, MA, USA, 2006. — 750 с.
2. Шень А. Программирование: теоремы и задачи. — М.: МЦНМО, 2014. — 296 с.
3. Шень А., Верещагин Н. Языки и исчисления. — М.: МЦНМО, 2012. — 240 с.
4. Верещагин, Н. К. Колмогоровская сложность и алгоритмическая случайность [Электронный ресурс] / Н. К. Верещагин, В. А. Успенский, А. Шень. — Электрон. дан. — СПб: Лань, 2013. — 575 с. — Режим доступа: https://e.lanbook.com/book/56395 — Загл. с экрана.

8.2. Учебно-методическое обеспечение для самостоятельной работы обучающихся:

1. Кривцова, И. Е. Основы дискретной математики. Часть 1. Учебное пособие [Электронный ресурс] / И. Е. Кривцова, И. С. Лебедев, А. В. Настека. — Электрон. дан. — СПб: ИТМО, 2016. — 92 с. — Режим доступа: http://books.ifmo.ru/book/1869/osnovy_diskretnoy_matematiki._chast_1._uchebnoe_posobie.htm — Загл. с экрана.

2. Теофили, Т. Глубокое обучение для поисковых систем : руководство / Т. Теофили ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 318 с. — ISBN 978-5-97060-776-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140574

8.3. Дополнительная литература

Вики-конспекты. — http://neerc.ifmo.ru/wiki/index.php?title=Заглавная_страница

8.4. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru
2. Корпоративный проект Ассоциации региональных библиотечных консорциумов (АРБИКОН) «Межрегиональная аналитическая роспись статей» (МАРС): http://mars.arbicon.ru
3. Единое окно доступа к образовательным ресурсам http://window.edu.ru

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для проведения **лекционных занятий**:

1. Используется аудитория, оборудованная необходимым количеством столов, стульев, доской маркерной и электронной.
2. Аудитория должна иметь следующие нормы освещенности
   - СНиП 23-05-95 «Естественное и искусственное освещение» норма освещенности аудиторий ВУЗов 400 Лк.
   - СанПиН 2.2.1/2.1.1.1278-03 «Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий» пункт 3.3.3. «Общее освещение в помещениях общественных зданий должно быть равномерным».
3. Электронная доска должна быть подключена к сети Интернет.

Для проведения **лабораторных занятий**:

1. Лабораторные занятия проводятся с группами или подгруппами не более 15 человек.
2. Аудитория должна быть оснащена необходимым количеством столов, стульев, доской маркерной и электронной.
4. Аудитория должна иметь следующие нормы освещенности
   - СНиП 23-05-95 «Естественное и искусственное освещение» норма освещенности аудиторий ВУЗов 400 Лк.
   - СанПиН 2.2.1/2.1.1.1278-03 «Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий» пункт 3.3.3. «Общее освещение в помещениях общественных зданий должно быть равномерным».
5. В аудитории должно быть не менее 15 компьютеров, находящихся в исправном состоянии.
6. Расположение компьютеров в аудитории должно позволять преподавателю подойти к рабочему месту студента.
7. Компьютеры должны быть соединены локальной сетью со скоростью не менее 1 Гбит/с и подключены к сети Интернет.
8. Компьютеры должны обладать минимальными характеристиками:
   - Объем оперативной памяти 16 Гб
   - Накопитель SDD 500 Гб
   - Процессор 12th Gen Intel(R) Core(TM) i3-12100
   - Видеоадаптер Intel(R) UHD Graphics 730

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).