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
«__»_____ 202__ г.	«__»_____ 202__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптография»

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 и осваивается в 6 семестре.

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) общепрофессиональных (ОПК 4)

ОПК-4. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ОПК-4.1. Знает современные информационные-коммуникационные технологии необходимые для решения задач профессиональной деятельности, основные требования информационной безопасности. ОПК-4.2. Умеет решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-4.3. Владеет навыками применения существующих информационно-коммуникационных технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	современные способы использования информационных технологий в области (областях) профессиональной деятельности, стандарты и нормативы проектной документации, требования информационной безопасности	выбирать и применять в профессиональной деятельности современные цифровые технологии, анализировать и разрабатывать проектную документацию, технические и (или) деловые регламенты, применяя стандарты и нормативы в сфере профессиональной деятельности	навыками использования информационно-коммуникационных технологий, в том числе специальных методов, программного обеспечения, компьютерного оборудования и технологий искусственного интеллекта

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
		ОПК-4	
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.

№	Формы	Описание
1	Лекция-дискуссия	Лекция-дискуссия специально не назначается, а возникает достаточно спонтанно на большинстве лекций. Студенты устно высказываю своѐ мнение по ходу лекции, дискутируют как с лектором, так и между собой. Также дискуссии иногда возникают при защите лабораторных работ.
2	Исследовательские методы в обучении	Дает возможность учащимся самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения.
3	Самостоятельная работа	Работа с ресурсами Internet, подготовка к лабораторным работам

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).

Перечень информационных справочных систем:

1. Электронная библиотека «Астраханский государственный университет» собственной генерации на платформе ЭБС «Электронный Читальный зал – БиблиоТех». https://biblio.asu.edu.ru
2. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем».
3. https://library.asu.edu.ru
4. Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента». www.studentlibrary.ru
5. Электронная библиотечная система издательства ЮРАЙТ, раздел «Легендарные книги». www.biblio-online.ru, https://urait.ru/
6. Электронная библиотечная система IPRbooks. www.iprbookshop.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 5 – 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	ОПК-4	лабораторные работы, домашние задания
2	Криптографические и технические методы защиты информации	ОПК-4	лабораторные работы, домашние задания

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

Таблица 6 – 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 7 – 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)

Типовые контрольные задания, необходимые для оценки достижения запланированных результатов обучения приведены в таблице планирования результатов обучения по дисциплине (БаРС) (Приложение 1)*.

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).

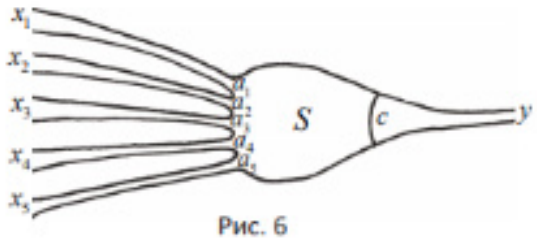

Рис. 6

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 $S \ge c$, 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.

Шкала оценивания и критерии оценки:

Критерий	Максимальное количество баллов	Минимальное количество баллов
Выбор подхода к решению задач	**6**	**0**
Правильность выполняемых операций	**6**	**0**
Правильность полученного ответа	**8**	**0**
Итого:	**20**	**0**

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.

Шкала оценивания и критерии оценки (на примере одной лабораторной работы):

№ п/п	Показатели	Оценка (уровень)		
		высокий	средний	низкий
1	Уровень оформления отчета	5	3	0
2	Навыки представления результатов работы	5	3	0
3	Умение применять полученные знания в новом окружении или для новых задач	5	3	0
4	Умение обосновывать принятые решения, анализировать ограничения их применимости	5	3	0
	Итого:	**20**	**12**	**0**

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:

Максимальное количество баллов — 20 баллов

Каждая правильно решённая задача оценивается в 5 баллов. Оценка снижается при отсутствии развёрнутого решения, наличия доказательных и вычислительных ошибок.

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.

Шкала оценивания и критерии оценки (на примере одной лабораторной работы):

№ п/п	Показатели	Оценка (уровень)		
		высокий	средний	низкий
1	Уровень оформления отчета	5	3	0
2	Навыки представления результатов работы	5	3	0
3	Умение применять полученные знания в новом окружении или для новых задач	5	3	0
4	Умение обосновывать принятые решения, анализировать ограничения их применимости	5	3	0
	Итого:	**20**	**12**	**0**

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

ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Зачет

Формат проведения зачета – устный опрос в формате ответов на вопросы билета. При необходимости преподаватель имеет возможность задать 2-3 дополнительных вопроса по темам практических и лекционных занятий.

Перечень вопросов:

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»

Шкала оценивания и критерии оценки:

Критерии оценки	Минимальное количество баллов	Максимальное количество баллов
Уровень усвоения материала, предусмотренного программой	0	2
Умение выполнять задания, предусмотренные программой	0	2
Уровень знакомства с основной литературой, предусмотренной программой	0	2
Уровень знакомства с дополнительной литературой	0	2
Уровень раскрытия причинно-следственных связей	0	2
Уровень раскрытия междисциплинарных связей	0	2

Качество ответа (его общая композиция, логичность, убежденность, общая эрудиция)	0	3
Ответы на вопросы: полнота, аргументированность, убежденность, умение использовать ответы на вопросы для более полного раскрытия содержания вопроса	0	3
2Деловые и волевые качества докладчика: ответственное отношение к работе, стремление к достижению высоких результатов, готовность к дискуссии, контактность	0	2
Итого баллов:	0	20

Оценка	Минимальное количество баллов	Максимальное количество баллов
Зачтено	60	100
Не зачтено	0	60

Знания, умения и навыки обучающихся при промежуточной аттестации в форме зачета определяются «зачтено», «не зачтено».

«Зачтено» – обучающийся знает курс на уровне лекционного материала, базового учебника, дополнительной учебной, научной и методологической литературы, умеет привести разные точки зрения по излагаемому вопросу.

«Не зачтено» – обучающийся имеет пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий.

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.

8.3. Дополнительная литература

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

8.4. Перечень ресурсов информационно-телекоммуникационной сети “Интернет”, необходимый для освоения дисциплины

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 используется аудитория, оборудованная современной презентационной техникой (проектор, экран, ноутбук).

Для выполнения лабораторных работ используются компьютерные классы с установленным в них необходимым программным обеспечением.

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для обучения с применением дистанционных образовательных технологий. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).