МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФИЗИКО- МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

УТВЕРЖДАЮ
Проректор по УР и КО
_____С.А. Льянова
«29» июня 2023г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.05.02 ОСНОВЫ КРИПТОГРАФИИ

Основной профессиональной образовательной программы
академического бакалавриата

09.03.02 «Информационные системы и технологии»

Квалификация выпускника

бакалавр

Форма обучения

очная

Магас, 2023

1. Цели и задачи освоения дисциплины «Основы криптографии»

Цель дисциплины – сформировать компетенции обучающегося в области математического аппарата криптозащиты и криптоанализа, современных криптографических протоколов, практического использования криптографических средств защиты информации.

Задачами преподавания дисциплины являются:

– Рассмотреть наиболее распространённые криптографические протоколы, а также основные методы криптоанализа.;

– Раскрыть принципы математических и вычислительных моделей криптографических процессов, их оптимизация и выработка направлений совершенствования;

– Показать особенности различных криптографических протоколов и возможностей их применения.

Код и наименование профессионального стандарта	**Обобщенные трудовые функции**			**Трудовые функции**		
	Код	**Наименование**	**Уровень квалификации**	**Наименование**	**Код**	**Уровень (подуровень) квалификации**
06.011 Администратор баз данных	D	Обеспечение информационной безопасности на уровне БД	6	Разработка политики информационной безопасности на уровне БД	D/01.6	6
				Контроль соблюдения регламентов по обеспечению безопасности на уровне БД	D/02.6	6
				Оптимизация работы систем безопасности с целью уменьшения нагрузки на работу БД	D/03.6	6
				Разработка регламентов и аудит системы безопасности данных	D/04.6	6
				Подготовка отчетов о состоянии и эффективности системы безопасности на уровне БД	D/05.6	6
				Разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным	D/06.6	6

2. Место учебной дисциплины в структуреосновной профессиональной образовательной программы бакалавриата

Дисциплина «Основы криптографии» изучается в блоке Б1.В и является одной из дисциплин вариативной части, формируемой участниками

образовательных отношений, и имеет соответствующий шифр Б1.В.ДВ.05.02 подготовки бакалавриата по направлению 09.03.02 «Информационные системы и технологии».

Дисциплины и практики, знания и умения, по которым необходимы как "входные" при изучении данной дисциплины	Безопасность жизнедеятельности Информатика
Дисциплины, практики, ГИА, для которых изучение данной дисциплины необходимо как «предшествующее»	Администрирование в информационных системах Управление данными Защита интеллектуальной собственности Корпоративные информационные системы

Формы работы студентов - в ходе изучения дисциплины предусмотрены семинарские занятия, выполнение домашних работ. Самостоятельная работа студентов, предусмотренная учебным планом, выполняется в ходе семестра в форме выполнения домашних заданий. Отдельные темы теоретического курса прорабатываются студентами самостоятельно в соответствии с планом самостоятельной работы и конкретными заданиями преподавателя с учетом индивидуальных особенностей студентов. Виды текущего контроля - проверка домашних заданий, устный опрос, проверка контрольной работы. Форма итогового контроля: 3 курс, 5 семестр –экзамен.

3.Результаты освоения дисциплины «Основы криптографии»:

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Категория (группа) компетенций	**Код и наименование компетенции**	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**
УК-2	**УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих**	УК-2.1.: понимает виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы,	**Знать**: виды ресурсов ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную

	правовых норм, имеющихся ресурсов и ограничений	регулирующие профессиональную деятельность. УК-2.2.:проводит анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности.	деятельность. **Уметь:** проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно правовую документацию в сфере профессиональной деятельности.
ПК-4	**ПК-4. Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности**	ПК-4.1: использует специальные знания по работе с установленной БД; общие основы решения практических задач по восстановлению БД и проверке корректности восстановленных данных; основы управления учетными записями пользователей; ПК-4.2: выполняет регламентные процедуры по резервированию данных; выбирать способ действия из известных; контролировать оценивать и корректировать свои действия; выполнять регламентные процедуры по восстановлению и проверке корректности восстановленных данных; выбирать способ действия из известных; контролировать оценивать и корректировать свои действия; применять специальные процедуры управления правами доступа пользователей ПК-4.3: запускает процедуры резервного копирования; мониторинга выполнения процедуры резервного копирования; контроля завершения процедуры резервного	**Знать:** специальные знания по работе с установленной БД; общие основы решении практических задач по восстановлению БД и проверке корректности восстановлены данных; специальные знаний по работе с установленной БД основы управления учетными записями пользователей; специальные знания по работам с установленной БД. **Уметь:** выполнять регламентные процедуры п резервированию данных; выбирать способ действия и известных; контролировать оценивать и корректировать свои действия; выполнят , регламентные процедуры п восстановлению и проверки корректности восстановлены данных; выбирать способ действия из известных контролировать, оценивать корректировать свои действия применять специальные процедуры управления правами доступа пользователей; **Владеть навыками:** запуск процедуры резервного копирования; мониторинг выполнения процедуры резервного копирования; контроля завершения ; процедуры резервного копирования; запуска

		копирования; запуска процедуры восстановления БД; мониторинга выполнения процедуры восстановления БД; контроля завершения процедуры восстановления БД; назначения прав доступа пользователей к БД изменения прав доступа пользователей к БД; контроля соблюдения прав доступа пользователей к БД	процедуры восстановления БД мониторинга выполнения процедуры восстановления БД контроля завершения процедуры восстановления БД назначения прав доступа пользователей к БД; изменений прав доступа пользователей к БД
ПК-8	**ПК-8. Способность выполнять работы по разработке компонентов системных программных продуктов: компилятор, загрузчиков, сборщиков, системных утилит, драйверов устройств, по созданию инструментальных средств программирования**	ПК-8.1.: понимает синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования; методологии разработки программного обеспечения; методологии и технологии проектирования и использования баз данных; технологии программирования; особенности выбранной среды программирования и системы управления базами данных; компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними; ПК-8.2: применяет выбранные языки программирования для написания программного кода; использовать выбранную среду программирования и средства системы управления базами данных; использовать возможности имеющейся технической и/или программной архитектуры;	**Знать:** синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования; методологии разработки программного обеспечения; методологии и технологии проектирования и использования баз данных; технологии программирования; особенности выбранной среды программирования и системы управления базами данных; компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними; Уметь: применять выбранные языки программирования для написания программного кода; использовать выбранную среду программирования и средства системы управления базами данных; использовать возможности имеющейся технической и/или программной архитектуры

4. Структура и содержание дисциплины «Основы криптографии»

4.1. Структура дисциплины «Основы криптографии»

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Наименование разделов и тем дисциплины (модуля)	семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)									Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*						
			Контактная работа					Самостоятельная работа										
			Всего	Лекции	Практические занятия	Лабораторные занятия	Др. виды контакт.работы	Всего	Курсовая работа(проект)	Подготовка к экзамену	Другие виды самостоятельнойработы	Собеседование	Коллоквиум	Проверка тестов	Проверка контрольн. работ	Проверка реферата	Проверка эссе и иных творческих работ	курсовая работа (проект) лр.
1.	Тема 1. Введение в криптографию. Основные понятия и определения.	5	2	2				4			4							
2.	Тема 2. Математические основы криптографии	5	4	2		2		4			4							
3.	Тема 3. Стойкость криптоалгоритмов	5	4	2		2		4			4							
4.	Тема 4. Поточные шифры	5	4	2		2		4			4							
5.	Тема 5. Блочные шифры	5	4	2		2		4			4							
6.	Тема 6. Криптографические протоколы	5	4	2		2		4			4							
7.	Тема 7. Построение криптографических примитивов	5	4	2		2		4			4							
8.	Тема 8. Симметричные криптосистемы	5	4	2		2		4			4							
9.	Тема 9. Алгоритм DES	5	4	2		2		6			6							
10.	Тема 10. Алгоритм ГОСТ 28147 -89	5	4	2		2		6			6							
11.	Тема 11. Ассиметричные криптосистемы	5	4	2		2		6			6							
12.	Тема 12. Алгоритм RSA	5	4	2		2		6			6							
13.	Тема 13. Электронная цифровая подпись	5	6	4		2		6			6							
14.	Тема 14. Основные криптоаналитические методы	5	4	2		2		6			6							
15.	Тема 15. Дискретное логарифмирование	5	4	2		2		6			6							
16.	Тема 16. Факторизация целых чисел (Поллард)	5	4	2		2		6			6							

17.	Тема 17. Псевдослучайные последовательности. Линейные рекуррентные последовательности как псевдослучайные последовательности	5	4	2		2		5			5							
	Общая трудоемкость, в часах		**180**	**36**		**32**		**85**			**85**							
	Экзамен		27															

5. Образовательные технологии

В освоении дисциплины используются следующие образовательные технологии:

- Компьютерные классы с набором лицензионного базового программного обеспечения для проведения лабораторных занятий;
- Skype, ЭИОС на платформе Moodle для проведения дистанционного обучения и консультаций. Технология мультимедиа в режиме диалога.
- Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории). Гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии) и т.д.

При подготовке бакалариатов используются основные формы проведения учебных занятий:

- интерактивные лекции;
- лекции-пресс-конференции;
- тренинги и семинары по развитию профессиональных навыков;
- практические (семинарские) занятия, групповые дискуссии и обмен мнениями, разбор альтернативных ситуаций;
- индивидуальные консультации;
- самостоятельная работа студентов с учебной литературой и первоисточниками, с интернет-ресурсами;
- экзамен.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых вовремя аудиторной работы. Вовремя

самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

6.1. План самостоятельной работы студентов

№.	Тема	Вид самостоятел. работы	Задание	Рекомендуемаялитература	Количество часов
1	Тема 1. Введение в криптографию. Основные понятия и определения.	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4
2	Тема 2. Математические основы криптографии	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4
3	Тема 3. Стойкость криптоалгоритмов	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4
4	Тема 4. Поточные шифры	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4
5	Тема 5. Блочные шифры	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4
6	Тема 6. Криптографические протоколы	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4
7	Тема 7. Построение криптографических примитивов	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4
8	Тема 8. Симметричные криптосистемы	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4
9	Тема 9. Алгоритм DES	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	6

10	Тема 10. Алгоритм ГОСТ 28147 -89	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	6
11	Тема 11. Ассиметричные криптосистемы	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	6
12	Тема 12. Алгоритм RSA	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	6
13	Тема 13. Электронная цифровая подпись	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	6
14	Тема 14. Основные криптоаналитические методы	Коллоквиум	Подготовиться к тесту, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	6
15	Тема 15. Дискретное логарифмирование	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	6
16	Тема 16. Факторизация целых чисел (Поллард)	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	6
17	Тема 17. Псевдослучайные последовательности. Линейные рекуррентные последовательности как псевдослучайные последовательности	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	5

6.2. Методические указания по организации самостоятельной работы студентов

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные занятия, практические занятия, самостоятельную работу студента, консультации.

a. При изучении тем студентам необходимо повторить лекционный учебный материал, изучить рекомендованную литературу, а также учебный материал, находящийся в указанных информационных ресурсах.

На завершающем этапе изучения каждого модуля необходимо, воспользовавшись предложенными вопросами для самоконтроля, размещенными в электронной информационной образовательной среде (ЭИОС), проверить качество усвоения учебного материала.

В случае затруднения в ответах на поставленные вопросы рекомендуется повторить учебный материал.

b. После изучения каждого модуля дисциплины необходимо ответить на вопросы контрольного теста по данному модулю с целью оценивания знаний и получения баллов.

c. После изучения всех модулей приступить к выполнению контрольной работы, руководствуясь методическими рекомендациями по ее выполнению.

d. По завершению изучения учебной дисциплины в семестре студент обязан пройти промежуточную аттестацию. Вид промежуточной аттестации определяется рабочим

учебным планом. Форма проведения промежуточной аттестации - компьютерное тестирование с использованием автоматизированной системы тестирования знаний студентов в ЭИОС.

е. К промежуточной аттестации допускаются студенты, выполнившие требования рабочего учебного плана.

6.3. Материалы для проведения текущего и промежуточного контроля знаний студентов.

Тематика заданий текущего контроля
Пример тестового задания.

Тестовое задание

Тестирование по дисциплине «Основы криптографии»

1. Что в переводе с греческого языка означает слово «криптография»?

1. шифр
2. тайнопись
3. преобразование
4. расшифровка

2. Для чего предназначен центр сертификации ключей?

1. для регистрации абонентов
2. для изготовления сертификатов открытых ключей
3. для выделения специальных каналов связи абонентам
4. для хранения изготовленных сертификатов
5. для поддержания в актуальном состоянии справочника действующих сертификатов
6. для выпуска списка досрочно отозванных сертификатов

3. Кем было выполнено доказательство существования абсолютно стойких криптографических алгоритмов?

1. Г Вернамом
2. Б Шнайером
3. Б Паскалем
4. К Шенноном

4. Что является целью криптографического преобразования информации?

1. защита информации от несанкционированного доступа, аутентификация и защита от преднамеренных изменений
2. защита информации от случайных помех при передаче и хранении
3. защита информации от всех случайных или преднамеренных изменений
4. сжатие информации

5. Как называется шифр, в котором каждый символ открытого текста заменяется некоторым, фиксированным при данном ключе, символом другого алфавита?

1. шифром одноалфавитной подстановки
2. шифром многоалфавитной подстановки
3. шифром замены
4. шифром Цезаря

6. Что общего имеют все методы шифрования с закрытым ключом?

1. в них для шифрования информации используется один ключ, а для расшифрования – другой ключ
2. в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов
3. в них производится сложение символов исходного текста и ключа по модулю, равному числу букв в алфавите
4. в них для шифрования и расшифрования информации используется один и тот же ключ

7. Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования?

1. возведение в степень
2. замена бит по таблице замен
3. нахождение остатка от деления на большое простое число
4. перестановка бит
5. сложение по модулю 2

8. Как называется однозначное преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины?

1. Коллизия
2. хеширование
3. Гаммирование
4. перестановка
5. Сложение по модулю 2

9. Какова цель использования генераторов псевдослучайных чисел при поточном шифровании?

1. защита информации от случайных помех при передаче и хранении
2. защита информации от всех случайных или преднамеренных изменений
3. получение "бесконечной " гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа
4. сжатие информации
5. формирование открытых ключей

10. Какими свойствами должен обладать генератор псевдослучайных чисел (ГПСЧ) для использования в криптографических целях?

1. вероятности порождения различных значений ключевой последовательности должны быть равны
2. ГПСЧ при каждом включении должен создавать одну и ту же последовательность битов
3. порождаемая последовательность должна быть «почти» неотличима от действительно случайной

4. для того, чтобы только законный получатель мог расшифровать сообщение, необходимо, чтобы при получении потока ключевых битов ki использовался и учитывался некоторый секретный ключ, причем вычисление числа ki+1 по известным предыдущим элементам последовательности ki без знания ключа должно быть сложной задачей

11. Алгоритмы шифрования с открытым ключом по-другому называются

1. асимметричными алгоритмами шифрования
2. симметричными алгоритмами шифрования
3. односторонними алгоритмами шифрования
4. помехоустойчивыми алгоритмами шифрования

12. Как называется совокупность заранее оговоренных способов преобразования
исходного секретного сообщения с целью его защиты?

1. алгоритм
2. ключ
3. протокол
4. шифр

13. Как называется натуральное число, которое не имеет делителей, кроме самого себя
и единицы?

1. простое число
2. составное число
3. каноническое число
4. криптографическое число

14. Какой шифр называется совершенным?

1. шифр называется совершенным, если знание шифротекста сообщения предоставляет некоторую информацию относительно соответствующего открытого текста
2. шифр называется совершенным, если в алгоритме шифрования используется не более четырех простейших операций
3. шифр называется совершенным, если анализ зашифрованного текста не может дать никакой информации об открытом тексте, кроме, возможно, его длины

15. Как называется преобразование информации с целью обнаружения и коррекции
ошибок при воздействии помех при передаче данных?

1. компрессия
2. эффективное кодирование
3. шифрование
4. помехоустойчивое кодирование

16. Как называется способ шифрования, в котором шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите?

1. гаммирование
2. одноалфавитная подстановка
3. перестановка

17. Какие требования предъявляются в настоящее время к блочным шифрам?

1. зашифрованное сообщение должно поддаваться чтению только при наличии ключа
2. знание алгоритма шифрования может влиять на надежность защиты
3. любой ключ из множества возможных должен обеспечивать надежную защиту информации
4. алгоритм шифрования должен допускать только аппаратную реализацию

18. Какие части имеются в составе сдвигового регистра с обратной связью?

1. арифметико-логическое устройство
2. регистр памяти
3. регистр сдвига
4. устройство генерации функции обратной связи

19. Гарантирование невозможности несанкционированного изменения информации - это:

1. обеспечение целостности
2. обеспечение конфиденциальности
3. обеспечение аутентификации
4. обеспечение шифрования

20. Рассмотрим источник информации, формирующий сообщение из конечного множества возможных символов (дискретный источник информации) Чему равно минимальное количество символов, образующих алфавит?

1. 1
2. 2
3. 3

21. В чем заключается общая идея помехоустойчивого кодирования?

1. из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
2. из всех допустимых кодовых слов считаются возможными не все, а лишь некоторые
3. производится преобразование информации с целью сокрытия ее смысла
4. уменьшается избыточность передаваемых сообщений

22. Как называется способ реализации криптографического метода, при котором все процедуры шифрования и расшифрования выполняются специальными электронными схемами по определенным логическим правилам?

1. аппаратный
2. программный
3. ручной
4. электромеханический

23. Что является особенностью систем шифрования с открытым ключом по сравнению
с симметричными системами шифрования?

1. возможность шифрования как текстовой, так и графической информации
2. высокая скорость процессов шифрования/расшифрования
3. использование малого количества вычислительных ресурсов
4. отсутствие необходимости предварительной передачи секретного ключа по надёжному каналу связи

24. Выберите правильное определение термина «криптография»

1. криптография – это наука о преодолении криптографической защиты информации
2. криптография – это наука, занимающаяся шифрованием данных при передаче по
открытым каналам связи
3. криптография изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия
4. криптография изучает способы защиты информации, основанные на попытке скрыть от противника сам факт наличия интересующей его информации

25. Какая наука разрабатывает методы «вскрытия» шифров?

1. криптография
2. криптоанализ
3. теория чисел
4. тайнопись

Вопросы для промежуточной аттестации по дисциплине:

1. Управление открытыми ключами.
2. Проблемы передачи информации и их комплексное решение.
3. Помехоустойчивое кодирование.
4. Принципы сжатия данных.
5. Предмет и задачи криптографии. Основные термины.
6. Приведите известные вам классификации криптосистем.
7. Общая схема симметричного шифрования.
8. Криптография с открытым ключом.
9. Криптографические протоколы.
10. Шифры с секретным ключом.
11. Криптосистемы на эллиптических кривых.
12. Случайные числа в криптографии.
13. Сжимающее кодирование.
14. Электронная цифровая подпись.
15. Шифр Шамира.
16. Шифр Эль-Гамаля.
17. Шифр RSA.
18. Основные этапы развития теории защиты информации.

19. Наивная криптография.
20. Формальная криптография.

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

1.Итоговый контрольный тест доступен студенту только во время тестирования, согласно расписанию занятий или в установленное деканатом время.
2.Студент информируется о результатах текущей успеваемости.
3.Студент получает информацию о текущей успеваемости и допуске к процедуре итогового тестирования от преподавателя или в ЭИОС.
4.Производится идентификация личности студента.
5.Студентам, допущенным к промежуточной аттестации, открывается итоговый контрольный тест.
6.Тест закрывается студентом лично по завершении тестирования или автоматически по истечении времени тестирования.

Опрос устный

Опрос устный - диалог преподавателя со студентом, цель которого - систематизация и уточнение имеющихся у студента знаний, проверка его индивидуальных возможностей усвоения материала.

Устный опрос по основным терминам может проводится в начале/конце лекционного или практического занятия в течение 15 -20 мин. Либо устный опрос проводится в течение всего практического занятия по заранее выданной тематике. Выбранный преподавателем студент может отвечать с места либо у доски.

Критериями оценки устного опроса являются: правильность ответа на вопросы, степень раскрытия сущности вопроса.

Оценка **«отлично»** — дан полный, всесторонний ответ на вопрос. Точность в определениях. Приведение примеров из практики.

Оценка **«хорошо»** — дан неполный ответ на вопрос. Допущены неточности при ответе. Допущены неточности в основных определениях.

Оценка **«удовлетворительно»** — имеются существенные недочеты при ответе. Вопрос раскрыт частично. Незнание базовых определений курса.

Оценка **«неудовлетворительно»** — вопрос не раскрыт или дан неверный ответ.

Тесты

Тесты - инструмент, с помощью которого педагог оценивает степень достижения студентом требуемых знаний, умений, навыков. Составление теста включает в себя создание выверенной системы вопросов, собственно процедуру проведения тестирования и способ измерения полученных результатов.

Критерии оценки теста: Оценка **«отлично»** выставляется при условии правильного ответа студента не менее чем 85 % тестовых заданий;

Оценка **«хорошо»** выставляется при условии правильного ответа студента не менее чем 70 % тестовых заданий;

Оценка **«удовлетворительно»** выставляется при условии правильного ответа студента не менее 51 %; .

Оценка **«неудовлетворительно»** выставляется при условии правильного ответа студента менее чем на 50 % тестовых заданий.

Контрольная работа

Контрольная работа - средство промежуточного контроля остаточных знаний и умений, состоит из вопросов или заданий, которые студент должен решить, выполнить. Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в этой теме.

Критерии оценки контрольной работы для студентов заочного отделения:
Оценка «зачтено» ставится за полные ответы на все вопросы.

Оценка «не зачтено» ставится, если освещены не все вопросы требуемого материала или не описано главное в содержании вопросов, или письменная работа не сдана.

Коллоквиум(в переводе с латинского «беседа, разговор») – форма текущего контроля знаний студентов, которая проводится в виде собеседовании преподавателя и студента по самостоятельно подготовленной студентом теме.

Он применяется для проверки знаний по определенному разделу (или объемной теме) и принятия решения о том, можно ли переходить к изучению нового материала. Коллоквиум — это беседа со студентами, целью которой является выявление уровня овладения новыми знаниями. В отличие от семинара главное на коллоквиуме — это проверка знаний с целью их систематизации.

Целью коллоквиума является формирование у студента навыков анализа теоретических проблем на основе самостоятельного изучения учебной и научной литературы.

На коллоквиум выносятся крупные, проблемные, нередко спорные теоретические вопросы. Коллоквиум может проводиться по вопросам, обсуждавшимся на семинарах. Конкретные вопросы для коллоквиума студентам не сообщаются, однако заранее формулируются преподавателем. Предполагаемый объем ответа не должен быть большим (примерно 1,5-2 минуты), чтобы преподаватель мог успеть опросить всех студентов.

От студента требуется:

- владение изученным в ходе учебного процесса материалом, относящимся к рассматриваемой проблеме;
- наличие собственного мнения по обсуждаемым вопросам и умение его аргументировать.

Коллоквиум — это не только форма контроля, но и метод углубления, закрепления знаний студентов, так как в ходе собеседования преподаватель разъясняет сложные вопросы, возникающие у студента в процессе изучения данного источника.

Задача коллоквиума добиться глубокого изучения отобранного материала, пробудить у студента стремление к чтению дополнительной экономической литературы.

Подготовка к проведению коллоквиума.

Подготовка к коллоквиуму предполагает несколько этапов:

1. Подготовка к коллоквиуму начинается с установочной консультации преподавателя, на которой он разъясняет развернутую тематику проблемы, рекомендует литературу для изучения и объясняет процедуру проведения коллоквиума.

2. Как правило, на самостоятельную подготовку к коллоквиуму студенту отводится 3–4 недели. Подготовка включает в себя изучение рекомендованной литературы и (по указанию преподавателя) конспектирование важнейших источников.

3. Коллоквиум проводится в форме индивидуальной беседы преподавателя с каждым студентом или беседы в небольших группах (3–5 человек).

4. Преподаватель задает несколько кратких конкретных вопросов, позволяющих выяснить степень добросовестности работы с литературой, контролирует конспект. Далее более подробно обсуждается какая-либо сторона проблемы, что позволяет оценить уровень понимания.

5. По итогам коллоквиума выставляется дифференцированная оценка, имеющая большой удельный вес в определении текущей успеваемости студента.

Особенности и порядок сдачи коллоквиума. Студент может себя считать готовым к сдаче коллоквиума по избранной работе, когда у него есть им лично составленный и обработанный конспект сдаваемой работы, он знает структуру работы в целом, содержание работы в целом или отдельных ее разделов (глав); умеет раскрыть рассматриваемые проблемы и высказать свое отношение к прочитанному и свои сомнения, а также знает, как убедить преподавателя в правоте своих суждений.

Проведение коллоквиума позволяет студенту приобрести опыт работы над первоисточниками, что в дальнейшем поможет с меньшими затратами времени работать над литературой по курсовой работе и при подготовке к экзаменам.

Экзамен

Экзамен - итоговая форма оценки знаний.

Проводится в заданный срок, согласно графику учебного процесса.

Критерии оценки при проведении экзамена:

Оценка "отлично" ставится, если студент обнаружил полное знание учебно-программного материала, успешно выполняет предусмотренные в программе задания, усвоил основную литературу, рекомендованную в программе. Ответ полный и правильный на основании изученного материала. Выдвинутые положения аргументированы и иллюстрированы примерами. Материал изложен в определенной логической последовательности, осознанно, литературным языком, с использованием современных научных терминов; ответ самостоятельный.Студент уверенно отвечает на дополнительные вопросы

Оценка «хорошо» ставится в том случае, когда студент обнаруживает полное знание учебного материала, демонстрирует систематический характер знаний по дисциплине. Ответ полный и правильный, подтвержден примерами; но их обоснование не аргументировано, отсутствует собственная точка зрения. Материал изложен в определенной логической последовательности, при этом допущены 2-3 несущественные погрешности, исправленные по требованию экзаменатора. Студент испытывает незначительные трудности в ответах на дополнительные вопросы. Материал изложен осознанно, самостоятельно, с использованием современных научных терминов, литературным языком.при этом могут допускаться некоторые погрешности в ответе на зачете, если студент обладает необходимыми знаниями для их устранения под руководством преподавателя.

Оценка «удовлетворительно» ставится в том случае, когда студент обнаруживает знание основного программного материала по дисциплине, но допускает погрешности в ответе. Ответ недостаточно логически выстроен, самостоятелен. Основные понятия употреблены правильно, но обнаруживаетсянедостаточноераскрытие теоретического материала. Выдвигаемые положения недостаточно аргументированы и не подтверждены примерами; ответ носит преимущественно описательный характер. Студент испытывает достаточные трудности в ответах на вопросы. Научная терминология используется недостаточно.

Оценка «неудовлетворительно» выставляется студенту, обнаружившему проблемы в знаниях основного учебного материала по дисциплине. При ответе обнаружено непонимание студентом основного содержания теоретического материала по дисциплине. При ответе обнаружено непонимание студентом основного содержания теоретического материала или допущен ряд существенных ошибок, которые студент не может исправить при наводящих вопросах экзаменатора. Студент подменил научное обоснование проблем рассуждением бытового плана. Ответ носит поверхностный характер; наблюдаются неточности в использовании научной терминологии.

7. Учебно-методическое и материально-техническое обеспечение дисциплины«Методы и средства защиты информации»

7.1. Учебная литература:

Основная литература:

1. Бабаш А. В., Ларин Д. А. История защиты информ. В заруб.странах: Уч.пос./А.В.Бабаш- ИЦ РИОР,НИЦ ИНФРА-М,2016-283с (ВОБакалавр.(о); Высшая школа - Москва, 2021. - 627 с.
2. Петраков А. В. Основы практической защиты информации; РадиоСофт - М., 2020. - 504 с.
3. Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации. Учебное пособие; Ленанд - М., 2018. - 248 с.
4. Лапонина О. Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия; Интернет-университет информационных технологий, Бином. Лаборатория знаний - М., 2019. - 536 с.

Дополнительная литература:

1. Мельников Д. А. Информационная безопасность открытых систем: моногр. ; Флинта, Наука - М., 2019. - 448 с.
2. Партыка Т. Л., Попов И. И. Информационная безопасность; Форум - М., 2022. - 432 с.
3. Проскурин В. Г. Защита в операционных системах. Учебное пособие; Гостехиздат - Москва, 2022. - 192 с.
4. Хорев П. Б. Программно-аппаратная защита информации; Форум - М., 2020. - 352 с.

7.2. Интернет-ресурсы

1. Электронная информационно-образовательная среда АНО ВО "СЗТУ" (ЭИОС СЗТУ) [Электронный ресурс]. - Режим доступа:http: //edu.nwotu.ru/
2. Учебно-информационный центр АНО ВО "СЗТУ" [Электронный ресурс].- Режим доступа:http://lib.nwotu.ru:8087/iirbis2/
3. Электронно-библиотечная система IPRbooks[Электронный ресурс]. - Режим доступа:http: //www.iprbookshop. ru/
4. Информационная система "Единое окно доступа к образовательным ресурсам" [Электронный ресурс]. - Режим доступа:http: //window.edu.ru/
5. Информационная системы доступа к электронным каталогам библиотек сферы образования и науки (ИС ЭКБСОН)[Электронный ресурс]. - Режим доступа:http: //www.vlibrary.ru/

7.3. Программное обеспечение

При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:

Internet- технологии:

WWW(англ.WorldWideWeb- Всемирная Паутина) - технология работы в сети с гипертекстами;

FTP(англ. FileTransferProtocol- протокол передачи файлов) - технология передачи по сети файлов произвольного формата;

IRC(англ.InternetRelayChat- поочередный разговор в сети, чат) - технология ведения переговоров в реальном масштабе времени, дающая возможность разговаривать с другими людьми по сети в режиме прямого диалога;

ICQ(англ.Iseekyou- я ищу тебя, можно записать тремя указанными буквами) - технология ведения переговоров один на один в синхронном режиме.

1. Дистанционное обучение с использованием ЭИОС на платформе Moodle.
2. Технология мультимедиа в режиме диалога.
3. Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории).
4. Гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии) и т.д.

Программное обеспечение: ППП MSOffice2010

7.4. Материально-техническое обеспечение

Описание материально-технической базы, необходимой для изучения модуля

Перечень материально-технического обеспечения

№ п/п	Вид занятий	Вид и наименование оборудования
1	Лекционные занятия	Аудитории с мультимедийными средствами, средствами звуковоспроизведения и имеющие выход в сеть «Интернет». Помещения для проведения аудиторных занятий, оборудованные учебной мебелью
2	Лабораторные работы	Компьютерный класс с комплексом программных средств, позволяющих каждому студенту разрабатывать программные реализации практических задач в ходе выполнения лабораторных работ
3	Самостоятельная работа	Библиотека, имеющая рабочие места для студентов. Аудитории, оснащенные компьютерами с доступом к сети «Интернет»
4	Практика	Компьютерный класс с комплексом программных средств, позволяющих каждому студенту разрабатывать программные реализации практических задач в ходе выполнения лабораторных работ

Рабочая программа дисциплины **«Основы криптографии»** составлена в соответствии с требованиями ФГОСВО по направлению подготовки 09.03.02 - «Информационные системы и технологии», утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 г. № 926.

Программу составили: старший преподаватель кафедры «Информационные системы и технологии» _____/Цуроев И.М.

Программа одобрена на заседании кафедры «Информационные системы и технологии»

Протокол №10 от «21» июня 2023 года

Программа одобрена Учебно-методическим советом физико-математического факультета

Протокол №10 от «23» июня 2023 года

Программа рассмотрена на заседании Учебно-методического совета университета

Протокол №10 от «28» июня 2023 года

Сведения о переутверждении программы на очередной учебный год

и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедрой