

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

**ФИЗИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра «Информационные системы и технологии»**

СОГЛАСОВАНО

УТВЕРЖДАЮ

Руководитель образовательной программы

И.о. декана физико-математического
факультета

_____/М.Х. Мальсагов
от «03» марта 2025г.

_____/ Б.С.Кульбужев
от «14» марта 2025г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.05.02 «Основы криптографии»

Направление подготовки

09.03.02 Информационные системы и технологии

Направленность (профиль подготовки)

Информационные системы и технологии

Квалификация выпускника

Бакалавр

Форма обучения

Очная, заочная, очно-заочная

Магас, 2025г.

1. Цели и задачи освоения дисциплины «Основы криптографии»

Целями освоения дисциплины Б1.В.ДВ.05.02 «Основы криптографии» являются формирование у студентов компетенций в области ин-формационной безопасности и применения на практике основ криптографии.

Формируемые дисциплиной знания и умения готовят выпускника данной образовательной программы к выполнению следующих обобщенных трудовых функций (трудовых функций):

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	Код	Наименование	Уровень квалификации	Наименование	Код	Уровень (подуровень) квалификации
06.001 Программист		Разработка требований и проектирование программного обеспечения	6	Анализ требований к программному обеспечению	D/01.6	6
				Разработка технических спецификаций на программные компоненты и их взаимодействие	D/02.6	6
				Проектирование программного обеспечения	D/03.6	6

2. Место учебной дисциплины в структуре основной профессиональной образовательной программы бакалавриата

Дисциплина «Основы криптографии» изучается в блоке 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.

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 правовых норм, имеющих ресурсы и ограничений	УК-2.1.: понимает виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность. УК-2.2.: проводит анализ поставленной цели и	Знать: виды ресурсов ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность. Уметь: проводить анализ поставленной цели и формулировать задачи, которые необходимо ре-

		<p>формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности.</p>	<p>шить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности.</p>
ПК-4	<p>ПК-4. Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности</p>	<p>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;</p> <p>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</p> <p>ПК-4.3: запускает процедуры резервного копирования; мониторинга выполнения процедуры резервного копирования; контроля завершения процедуры резервного 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;</p>	<p>Знать: специальные знания по работе с установленной БД; общие основы решения практических задач по восстановлению БД и проверке корректности восстановленных данных; специальные знания по работе с установленной БД основы управления учетными записями пользователей; специальные знания по работам с установленной БД.</p> <p>Уметь: выполнять регламентные процедуры п резервированию данных; выбирать способ действия и известных; контролировать оценивать и корректировать свои действия; выполнять 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;</p> <p>Владеть навыками: запуск процедуры резервного копирования; мониторинг выполнения процедуры резервного копирования; контроля завершения процедуры резервного копирования; запуска процедуры восстановления БД мониторинга выполнения процедуры восстановления БД контроля завершения процедуры восстановления БД назначения прав доступа пользователей к БД; изменений прав доступ пользователей к БД</p>

		контроля соблюдения 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	<p>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;</p> <p>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;</p>	<p>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;</p> <p>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</p>

4.1. Структура дисциплины «Основы криптографии»

[illegible]

4.2. Содержание дисциплины

№	Название темы	Содержание
1.	Базовые понятия криптографии	Терминология. Криптоанализ. Стойкость алгоритмов. Стеганография. Подстановочные и перестановочные шифры. Простой XOR. Одноразовые блокноты. Компьютерные алгоритмы.
2.	Основные элементы криптографических протоколов	Понятие протокола. Протоколы с посредником. Протоколы с арбитром. Самодостаточные протоколы. Организация связи с помощью симметричной криптографии. Однонаправленные функции. Организация связи с помощью криптографии с открытым ключом. Цифровые подписи. Цифровые подписи плюс шифрование.
3.	Основные криптографические протоколы	Обмен ключами. Аутентификация. Протокол Kerberos. Методы разбиения и разделения секрета. Доказательства с нулевым разглашением.
4	Типы криптографических алгоритмов и режимов шифрования	Блочные и потоковые шифры. Режим электронной кодовой книги. Режим сцепления блоков шифротекста. Самосинхронизирующиеся потоковые шифры. Режим обратной связи по шифротексту. Синхронные потоковые шифры. Режим обратной связи по выходу. Режим счетчика. Рекомендации по выбору режима шифрования. Сравнение блочных и потоковых шифров.
5.	Использование криптографических алгоритмов	Сравнение криптографии с открытым ключом и симметричной криптографии. Шифрование каналов связи. Шифрование данных для хранения. Сравнение аппаратного и программного шифрований. Сжатие, кодирование и шифрование. Уничтожение информации.
6.	Алгоритм DES	Назначение алгоритма. Схема работы алгоритма. Шифрование и расшифрование. Режимы работы алгоритма.
7.	Алгоритм ГОСТ 28147-89	Назначение алгоритма. Схема работы алгоритма. Криптоанализ алгоритма. Основные отличия от алгоритма DES.
8.	Теория проектирования блочных шифров	Проблема избыточности открытого текста сообщения. Методы перемешивания и рассеивания. Сети Фейстеля. Групповая структура. Проектирование S-блоков. Строгий лавинный критерий.
9.	Потоковые шифры	Регистры сдвига с линейной обратной связью и их использование при проектировании потоковых шифров. Алгоритм A5

5. Образовательные технологии

В освоении дисциплины используются следующие образовательные техно-логии:

- Компьютерные классы с набором лицензионного базового программно-го 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 (вирту-альные кабинеты, лаборатории). Гипертекстовая технология (электрон-ные учебники, справочники, словари, энциклопедии) и т.д.

При подготовке бакалавриатов 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 студен-тов. Оценочные средства для текущего контроля успеваемости, промежу-точной аттестации по итогам освоения дисциплины.

6.1 План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Тема 1. Базовые понятия криптографии	Коллоквиум	Подготовиться к кол- локвиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	2
2	Тема 2. Основные элементы криптографических протоколов	Коллоквиум	Подготовиться к кол- локвиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	2

3	Тема 3. Основные 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	2
4	Тема 4. Типы криптографических алгоритмов и режимов шифрования	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	8
5	Тема5. Использование криптографических алгоритмов	Тест	Подготовиться к тесту, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	8
6	Тема 6. 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	4
7	Тема 7. 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	4
8	Тема 8. Теория проектирования блочных шифров	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	10
9	Тема 9. Поточковые 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

6.2 Методические указания по организации самостоятельной работы студентов

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

- а. 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.
- e. К промежуточной аттестации допускаются студенты, выполнившие требования рабочего учебного плана.

6.3. 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

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

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 k_i использовался и учитывался некоторый секретный ключ, причем вычисление числа k_{i+1} по известным предыдущим элементам последовательности k_i 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

6.4 Методические материалы, определяющие процедуры оценивания достижения запланированных результатов обучения по дисциплине

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 проводиться 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.

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 про-читанному и свои сомнения, а также знает, как убедить преподавателя в право-те 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 обнаруживается недостаточное раскрытие 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.

Критерии оценки промежуточной аттестации в форме зачета

Уровень сформированности компетенций	Общие требования к результатам аттестации в форме зачета	Планируемые результаты обучения
--------------------------------------	--	---------------------------------

Высокий уровень	<p>Теоретическое содержание курса освоено полностью без пробелов или в целом, или большей частью, необходимые практические навыки работы с освоенным материалом сформированы или в основном сформированы, все или большинство предусмотренных рабочей программой учебных заданий выполнены, отдельные из выполненных заданий содержат ошибки</p>	<p>Знать:-систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; - точное использование научной терминологии систематически-грамотное и логически правильное изложение ответа на вопросы;</p> <p>Уметь:-ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин;- творческая самостоятельная работа на практических/семинарских/лабораторных занятиях, активное участие в групповых обсуждениях, высокий уровень культуры исполнения заданий;</p> <p>Владеть:-безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; - выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; - полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине;</p>
Базовый уровень	<p>Теоретическое Содержание курса освоено в целом без пробелов, необходимые практические навыки работы с освоенным материалом в основном сформированы, предусмотренные рабочей учебной программой учебные задания выполнены с отдельными</p>	<p>Знать:- достаточно полные и систематизированные знания по дисциплине;</p> <p>Уметь:-ориентироваться в основном теориях, концепциях и направлениях дисциплины и давать им критическую оценку; -использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы,</p>

	неточностями, качество выполнения большинства заданий оценено числом баллов, близким к максимуму.	умение делать обоснованные выводы; Владеть:- владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач; - усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; - самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; - средний уровень сформированности заявленных в рабочей программе компетенций.
Минимальный уровень	Теоретическое содержание курса освоено большей частью, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных рабочей учебной программой учебных заданий выполнены, отдельные из выполненных заданий содержат ошибки.	Знать:- достаточный минимальный объем знаний по дисциплине; - усвоение основной литературы, рекомендованной учебной программой; Уметь:- умение ориентироваться в основных теориях, концепциях и Направлениях по дисциплине и давать им оценку; - использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок; Владеть:- владение инструментарием учебной дисциплины, умение его использовать в решении типовых задач; - умение под руководством преподавателя решать стандартные задачи;- работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий;- достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций.
компетенции, закреплённые за дисциплиной, не сформированы	Теоретическое Содержание курса освоено частично, необходимые навыки работы не	Планируемые результаты обучения не достигнуты

	сформированы или сформированы отдельные из них, большинство предусмотренных рабочей учебной программой заданий не выполнено либо выполнено с грубыми ошибками, качество их выполнения оценено числом баллов, близким к минимуму.	
--	--	--

Перечень вопросов для подготовки к экзамену:

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-Гамала.
17. Шифр RSA.
18. Основные этапы развития теории защиты информации.
19. Наивная криптография.
20. Формальная криптография
21. Алгоритм DES
22. Алгоритм ГОСТ 28147-89
23. Теория проектирования блочных шифров
24. Поточковые шифры
- 25 Типы криптографических алгоритмов и режимов шифрования

7. Учебно-методическое и материально-техническое обеспечение дисциплины «Основы криптографии»

7.1. Учебная литература:

Основная литература:

1. Бабаш А. В., Ларин Д. А. История защиты информ.в за-руб. 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. Лапониная 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

Название ресурса	Ссылка/доступ
Электронная библиотека онлайн «Единое окно к образовательным ресурсам»	http://window.edu.ru
«Образовательный ресурс России»	http://school-collection.edu.ru
Федеральный образовательный портал: учреждения, программы, стандарты, ВУЗы, тесты ЕГЭ, ГИА	http://www.edu.ru
Федеральный центр информационно-образовательных ресурсов (ФЦИОР)	http://fcior.edu.ru
Русская виртуальная библиотека	http://rvb.ru
Кабинет русского языка и литературы	http://ruslit.ioso.ru
Национальный корпус русского языка	http://ruscorpora.ru
Научная электронная библиотека «e-Library»	http://elibrary.ru/defaultx.asp
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru
Электронно-библиотечная система ИнГГУ	https://lib.inggu.ru/
Информационно-правовая система «Гарант»	Сетевая версия, доступна со всех

	компьютеров в корпоративной сети ИнГГУ
--	--

7.3. Программное обеспечение

1.1. Microsoft Windows 7, Windows 8, Windows 8.1, Windows 10

1.2. Microsoft Windows server 2003, 2008, 2012, 2016

1.3. Microsoft Office 2007, 2010, 2016

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 звуко-воспроизведения 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 Б1.В.ДВ.05.02 «Основы криптографии» составлена в соответствии с требованиями ФГОСВО по направлению подготовки 09.03.02 «Информационные системы и технологии», профиль «Информационные системы и технологии» утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 г. № 926(ред. от 08.02.2021г.).

Программу составил: ассистент кафедры «Информационные системы и технологии» Катиева Л.М.

Программа одобрена на заседании кафедры «Информационные системы и технологии»

Протокол №6 от«03»марта 2025года

Программа одобрена Учебно-методической комиссией физико- математического факультета

Протокол №7от«13»марта2025года

Сведения о переутверждении программы на очередной учебный год и регистра-ции изменений

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ

Б1.В.ДВ.07.02 «Основы криптографии»

Направление подготовки

09.03.02 «Информационные системы и технологии»

Направленность(профиль подготовки)

Информационные системы и технологии

Квалификация выпускника

Бакалавр

Форма обучения

Очная, заочная, очно-заочная

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

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 правовых норм, имеющихся ресурсов и ограничений	УК-2.1.: понимает виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, 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.	Знать: виды ресурсов ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную 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	<p>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;</p> <p>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</p> <p>ПК-4.3: запускает процедуры резервного копирования; мониторинга выполнения процедуры резервного копирования; контроля завершения процедуры резервного 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</p>	<p>Знать: специальные знания по работе с установленной БД; общие основы решения практических задач по восстановлению БД и проверке корректности восстановленных данных; специальные знания по работе с установленной БД основы управления учетными записями пользователей; специальные знания по работам с установленной БД.</p> <p>Уметь: выполнять регламентные процедуры по резервированию данных; выбирать способ действия и известных; контролировать оценивать и корректировать свои действия; выполнять регламентные процедуры по восстановлению и проверки корректности восстановленных данных; выбирать способ действия из известных; контролировать, оценивать корректировать свои действия; применять специальные процедуры управления правами доступа пользователей;</p> <p>Владеть навыками: запуск процедуры резервного копирования; мониторинг выполнения процедуры резервного копирования; контроля завершения процедуры резервного копирования; запуска 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</p>
------	--	--	---

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
------	--	--	---

Тестирование по дисциплине «Основы криптографии»

Тест 1:

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

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

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 k_i использовался и учитывался некоторый секретный ключ, причем вычисление числа k_{i+1} по известным предыдущим элементам последовательности k_i 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

Тест 2:

1. **Программа, которая может размножаться, присоединяя свой код к другой программе, называется**
Выберите один ответ.
 - a. Компилятор
 - b. Интернет-черви
 - c. Вирус
2. **Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется**
Выберите один ответ.
 - a. Воздействием (влиянием)
 - b. Потерей
 - c. Силой
3. **Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется**
Выберите один ответ.
 - a. Троянской программой
 - b. Червем
 - c. Вирусом
4. **Уровень риска, который считается доступным для достижения желаемого результата, называется**
Выберите один ответ.
 - a. Устойчивостью
 - b. Терпимостью по отношению к риску
 - c. Независимостью
5. **Компьютер с одним процессором в каждый конкретный момент времени может выполнять команд**
Выберите один ответ.
 - a. Две
 - b. Одну
 - c. Сколько зададут
6. **Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:**
Выберите один ответ.
 - a. Статическими алгоритмами
 - b. Алгоритмы RMS
 - c. Динамическими алгоритмами
7. **Системные файлы, обеспечивающие поддержку структур файловой системы, называются:**
Выберите один ответ.
 - a. Каталоги
 - b. Символьные файлы
 - c. Регулярные файлы

8. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются

Выберите один ответ.

- a. Вирусами
- b. Руткитами
- c. Червями

9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:

Выберите один ответ.

- a. Правилами безопасности
- b. Требованием безопасности
- c. Мерами безопасности

10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:

Выберите один ответ.

- a. Управление риском
- b. Предупреждением рисков
- c. Анализом рисков

11. Компьютерная система, в которой два или более центральных процессоров делят полный доступ к общей оперативной памяти, называется

Выберите один ответ.

- a. Мультипроцессоры типа «хозяин-подчиненный»
- b. Симметричный мультипроцессор
- c. Мультипроцессор с общей памятью

1. Методические материалы, определяющие процедуры оценивания достижения запланированных результатов обучения по дисциплине

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 проводиться 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 собеседования 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.

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:

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

7. 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.

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

9. 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.

10. 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 обнаруживается недостаточное раскрытие 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.

Перечень вопросов для подготовки к экзамену:

1. Объяснить значение следующих терминов: криптография, криптоанализ, криптология, шифрование, расшифрование, дешифрование, атака (пассивная и активная).
2. Перечислить и объяснить задачи, решаемые с помощью криптографии.
3. Что понимается под криптографическим алгоритмом? Что такое ограниченный алгоритм?
4. Объяснить роль ключей в криптографии. Что означает понятие «криптосистема»?
5. Объяснить принцип работы симметричных алгоритмов.
6. Объяснить принцип работы асимметричных алгоритмов.
7. Объяснить назначение криптоанализа. Перечислить основные типы атак, используемых при проведении криптоанализа.
8. Объяснить принцип атаки на основе шифрованного текста.
9. Объяснить принцип атаки на основе открытого текста.
10. Объяснить принцип атаки на основе подобранного открытого текста.
11. Объяснить принцип атаки на основе адаптивно подобранного открытого текста.
12. Объяснить принцип атаки на основе подобранного шифрованного текста.
13. Объяснить принцип атаки на основе подобранного ключа.
14. Привести классификацию сложности взлома алгоритмов.
15. Что означает понятие «стойкость алгоритма»?
16. Что такое стеганография? Приведите примеры использования стеганографии.
17. Что называется подстановочным шифром? Какие типы подстановочных шифров Вы знаете и чём их суть?
18. Что такое перестановочный шифр?
19. Объясните алгоритм работы простого XOR.
20. Объясните суть алгоритма одноразового блокнота.
21. Понятие протокола. Характеристики протокола. Криптографический протокол. Назначение протокола.
22. Объясните работу протокола с посредником.
23. Объясните работу протокола с арбитром.
24. Объясните работу самодостаточного протокола.
25. Объясните принцип организация связи с помощью симметричной криптографии.
26. Что такое однонаправленная функция? Что такое ключевая однонаправленная функция?

27. Что такое однонаправленная хэш-функция? В чём заключается её основная суть?
28. Что такое код проверки подлинности сообщения?
29. Объясните принцип организации связи с помощью криптографии с открытым ключом.
30. Объясните принцип работы смешанной (гибридной) криптосистемы.
31. Для чего используется подпись? Какими свойствами она обладает?
32. Объясните, как происходит подписание документов с помощью симметричных криптосистем и посредника.
33. Объясните, как происходит подписание документов с помощью криптографии с открытым ключом.
34. Для чего нужны метки времени при подписании документов? Объясните, как происходит подписание документов с помощью криптографии с открытым ключом и однонаправленных хэш- функций.
35. Объясните работу протокола цифровой подписи и шифрования.
36. Как организуется повторная отсылка принятого сообщения?
37. Как организуется защита от атаки при повторной отсылке сообщения?
38. Как происходит обмен ключами средствами симметричной криптографии?
39. Как происходит обмен ключами средствами криптографии с открытым ключом?
40. Каким образом срабатывает атака «человек посередине»?
41. Объясните назначение и принцип работы протокола взаимоблокировки.
42. Каким образом можно защититься от атаки «человек посередине» с помощью одновременной передаче ключей и сообщений?
43. Объясните принцип широковещательной рассылки ключей и сообщений.
44. Объясните значение термина «аутентификация».
45. Каким образом осуществляется аутентификация с помощью однонаправленных функций?
46. Каким образом срабатывает атака по словарю? Для чего используются «привязки»?
47. Объясните назначение и принцип работы программы SKEY.
48. Каким образом осуществляется аутентификация с помощью криптографии с открытым ключом?
49. Каким образом можно проверить подлинность сообщения?
50. Аутентификация и обмен ключами. Протокол Kerberos.
51. Разбиение секрета (secret splitting). Разделение (sharing) секрета.
52. Доказательства с нулевым разглашением (zero knowledge proof).

53. Типы алгоритмов и режимов шифрования.
54. Режим электронной кодовой книги (режим простой замены).
55. Режим сцепления (chaining) блоков шифротекста. Рекомендации по выбору режима шифрования. Сравнение блочных и потоковых шифров.
56. Типы алгоритмов и режимов шифрования. Потоковые шифры. Самосинхронизирующиеся потоковые шифры. Режим обратной связи по шифротексту (гаммирование с обратной связью). Рекомендации по выбору режима шифрования. Сравнение блочных и потоковых шифров.
57. Синхронные потоковые шифры. Режим обратной связи по выходу. Режим счётчика. Рекомендации по выбору режима шифрования. Сравнение блочных и потоковых шифров.
58. Шифрование каналов связи. Шифрование данных для хранения. Сравнение аппаратного и программного шифрований. Сжатие, кодирование и шифрование. Уничтожение информации.
59. Алгоритм DES.
60. Алгоритм ГОСТ 28147-89.
61. Теория проектирования блочных шифров. Методы перемешивания и рассеивания. Сети Фейстеля. Групповая структура. Проектирование S-блоков.
62. Потоковые шифры. Регистры сдвига с линейной обратной связью (РСЛОС). Проектирование и анализ потоковых шифров. Потоковые шифры на основе РСЛОС.
63. Алгоритмы с открытым ключом. Алгоритмы на основе задачи об укладке ранца (рюкзак) (haversack).
64. Алгоритмы с открытым ключом. Алгоритм RSA. Типовой билет.

Студент получает 2 вопроса из разных разделов курса.

