МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 71B13ADF852F0D849D78875814FBEF47
Владелец: Баранов Юрий Александрович
Действителен: с 15.10.2025 до 08.01.2027

УТВЕРЖДЕНО

Заместитель директора,
совмещающий обязанности директора
филиала КузГТУ в г. Новокузнецке

_____Баранов Ю.А.

«29» мая 2026г.

Рабочая программа дисциплины

Методы и средства криптографической защиты информации

Направление подготовки 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация «Специалист по защите информации»

Формы обучения: очная

Год набора 2026

Новокузнецк 2026 г.

Рабочая программа обсуждена на заседании учебно-методического совета филиала КузГТУ в г. Новокузнецке

Протокол № 6 от 29.05.2026

Зав. Кафедрой ИТиЭД _____ В. В. Шарлай
подпись

СОГЛАСОВАНО:

Заместитель директора по УР _____ Т. А. Евсина
подпись

1 Перечень планируемых результатов обучения по дисциплине "Методы и средства криптографической защиты информации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-10 - Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Знает национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения.

Результаты обучения по дисциплине:

Знать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах.

Умеет применять математические модели для оценки стойкости СКЗИ, использовать СКЗИ в автоматизированных системах.

Владеть методами криптоанализа простейших шифров.

2 Место дисциплины "Методы и средства криптографической защиты информации" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Безопасность операционных систем, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Нормативные требования по защите информации, Классификация защищаемой информации и информационных систем.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Методы и средства криптографической защиты информации" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Методы и средства криптографической защиты информации" составляет 4 зачетных единицы, 144 часа.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 3/Семестр 5			
Всего часов	144		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	32		
Лабораторные занятия	32		
Практические занятия	16		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	6		
Самостоятельная работа	22		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Методы и средства криптографической защиты информации", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	**Трудоемкость в часах**
	ОФ
1. Введение	
История криптографии: исторические шифры, история отечественной криптографии, средства защиты информации в период перехода от древности к современности, шифры Виженера, модели шифров по К. Шеннону, обобщенная модель шифра, понятие симметричной криптосистемы, системы шифрования с открытыми ключами, блочные и поточные шифры, простейшие шифры и их свойства, композиции шифров, стойкость шифра, однонаправленные функции, современная классификация известных шифров, простые методы криптоанализа известных шифров. Характер криптографической деятельности. Виды информации, подлежащие закрытию, их модели и свойства. Модели нарушителя и безопасных систем. Модель Долева-Яо. Принципы построения криптографических алгоритмов. Понятие криптографического протокола. Протокол Нидхема-Шредера. Понятия аутентификации сущности и аутентификации сообщений. Модели шифров. Основные требования к шифрам. Программные реализации шифров. Особенности использования вычислительной техники в криптографии.	6
2. Математические основы криптографии	
Понятие сложности алгоритма, сложность некоторых известных алгоритмов. Недетерминированное полиномиальное время. Гипотеза P=NP. Алгоритм быстрого возведения в степень, обобщенный алгоритм Евклида. Модулярная арифметика. Теоремы Эйлера, Лагранжа, Ферма. Китайская теорема об ос-татках. Квадратичные вычеты и невычеты. Вычисление квадратного корня в модулярной арифметике по простому и по составному модулям. Понятие о конечных полях по неприводимым многочленам. Методы получения случайных и псевдослучайных последовательностей.	6
3. Симметричные криптосистемы	
Шифры замены, перестановки, шифры гаммирования. композиционные шифры, сети Файстеля. Блочные шифры: проблема выравнивания, требования к по-строению блочных шифров. Поточные шифры: синтез поточных шифров, тре-бования к поточным шифрам, режимы использования поточных шифров, син-хронизация поточных шифров, опознавание, контроль целостности данных, управление ключами. Криптосистемы DES и отечественного ГОСТа. Стандарт криптографической защиты AES-Rijndael. Криптографическая стойкость шифров. Основные атаки на симметричные шифры. Совершенные шифры. Теоретико-информационный подход к оценке криптостойкости шифров. Вопросы практической стойкости. Имитостойкость и помехоустойчивость шифров. Различие между программными и аппаратными реализациями. Криптографические параметры узлов и блоков шифраторов. Синтез шифров	8
4. Асимметричные криптосистемы	

Вопросы организации сетей засекреченной связи. Ключевые системы. Схема открытого распределения ключей Диффи-Хеллмана. K5A. Криптосистема Рабина. криптосистема Эль Гамаль. Сравнение двух классов криптосистем, гиб-ридные криптосистемы. Принципы криптоанализа, критерии распознавания от-крытого текста, универсальные методы криптоанализа: Дифференциальный криптоанализ, дифференциальный криптоанализ DES и трехраундового DES. Битовая стойкость алгоритма RSA. Понятие оракула четности. Битовая стойкость дискретного логарифма	6
5. Криптографические средства контроля целостности	
Симметричные средства. Криптографические хеш-функции. Электронная цифровая подпись, цифровая подпись на основе RSA, криптосистемы Рабина и Эль Гамаля. Существующие уязвимости системы Эль-Гамаля.	6
Итого	**32**

4.2. Лабораторные занятия

Наименование работы	**Трудоемкость в часах**
	ОФ
1. Классические криптосистемы	8
2. Методы генерации больших простых чисел	8
3. Симметричные схемы. DES	4
4. Алгоритм Advance Encryption System (AES)	4
5. Ассиметричные алгоритмы шифрования	4
6. Симметричные средства. Криптографические хеш-функции. Электронная цифровая подпись, цифровая подпись на основе RSA, криптосистемы Рабина и Эль Гамаля. Существующие уязвимости системы Эль-Гамаля.	4
Итого	**32**

4.3 Практические (семинарские) занятия

Тема занятия	**Трудоемкость в часах**
	ОФ
1. Классические криптосистемы	4
2. Методы генерации больших простых чисел	4
3. Симметричные схемы. DES	2
4. Алгоритм Advance Encryption System (AES)	2
5. Ассиметричные алгоритмы шифрования	2

6. Симметричные средства. Криптографические хеш-функции. Электронная цифровая подпись, цифровая подпись на основе RSA, криптосистемы Рабина и Эль Гамаля. Существующие уязвимости системы Эль-Гамаля.	2
Итого	**16**

4.4 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Вид СРС	**Трудоемкость в часах**
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	10
Оформление отчетов по практическим и(или) лабораторным работам	6
Подготовка к промежуточной аттестации	6
Итого	**22**
Самостоятельная работа под руководством преподавателя	6
Экзамен	36

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Методы и средства криптографической защиты информации"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)
Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	**Компетенции, формируемые в результате освоения дисциплины (модуля)**	**Индикатор(ы) достижения компетенции**	**Результаты обучения по дисциплине (модулю)**	**Уровень**
Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-10	Знает национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения	**Знать** основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах. **Умеет** применять математические модели для оценки стойкости СКЗИ, использовать СКЗИ в автоматизированных системах. **Владеть** методами криптоанализа простейших шифров.	Высокий или средний

Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции** - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции** - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.

5.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

Опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины

Обучающийся отвечает на 2 вопроса, либо отвечает на 10 тестовых заданий.

Например:

1. Ассиметричные методы защиты целостности. Электронная цифровая подпись. Подпись RSA.

2. Цифровая подпись Эль-Гамаля. Потенциальные уязвимости.

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Критерии оценивания при тестировании:

- 100 баллов – при правильном и полном ответе на 10 вопросов;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Примерный перечень контрольных вопросов:

1. Введение

1. Что такое шифрование?
2. Что такое кодирование?
3. Что изучает криптография?
4. Когда были известны первые алгоритмы шифрования?
5. Что такое криптостойкость?

2. Математические основы криптографии

1. Какую математическую функцию относительно легко вычислить, но трудно найти соответствующее значение аргумента?

2. Какие из разделов математики легли в основу современных методов криптографии?

3. Как называется наука, предметом которой являются математические способы преобразования информации с целью ее защиты от несанкционированных пользователей?

4. С каким алфавитом принято работать в теоретической криптографии ?

5. Какие виды математических последовательностей используются в криптографии?

3. Симметричные криптосистемы

1. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования?

2. Какой алгоритм, использует симметричный ключ и алгоритм хэширования?

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

4. Какой размер ключа в отечественном стандарте симметричного шифрования?

5. Какие методы криптоанализа применяются для симметричных шифров?

4. Асимметричные криптосистемы

1. В чем основные преимущества и недостатки асимметричных криптосистем?

2. Сколько используется ключей в асимметричных криптосистемах для шифрования и дешифрования?

3. Какими свойствами секретности должны обладать ключи в асимметричных системах шифрования?

4. Какие шифры (механизмы обмена ключами) относятся к асимметричным?

5. Какая связь существует между двумя ключами в асимметричной криптографии?

5. Криптографические средства контроля целостности

1. Протоколы контроля целостности. Разновидности и краткая характеристика.

2. Какие два основные понятия лежат в основе криптографического контроля целостности?

3. Каков механизм контроля целостности информации на основе криптозащиты, используемый в РФ?

4. От чего зависит алгоритм выработки проверочной комбинации (кода аутентификации), добавляемой к основному сообщению в криптографических методах контроля целостности?

5. Какие требования предъявляются к кодам аутентификации, служащим для проверки целостности сообщения?

Примерный перечень тестовых заданий:

1. Введение

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

шифр
тайнопись
преобразование
расшифровка

2. Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?

шифр Маркова
шифр Цезаря
шифр Энигма
шифр Бэбиджа

3. Выберите правильное определение термина «криптография»

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

2. Математические основы криптографии

1. Математическая функция, которую относительно легко вычислить, но трудно найти по

значению функции соответствующее значение аргумента, называется в криптографии

функцией Диффи-Хеллмана
односторонней функцией
функцией Эйлера
криптографической функцией

2. Какой тип алгоритмов шифрования больше основан на свойствах математических функций:

асимметричные
симметричные

3. На чем из перечисленного базируется криптография с открытым ключом?

дискретного логарифмирования
классической теории чисел
диофантовых линейных уравнениях
интегрального логарифмирования

3. Симметричные криптосистемы

1. Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:

1
2
3

2. Алгоритм, использующий симметричный ключ и алгоритм хэширования:

HMAC
3DES
ISAKMP-OAKLEY
RSA

3. Какие операции применяются обычно в современных блочных алгоритмах симмет-ричного шифрования?

сложение по модулю
нахождение остатка от деления на большое простое число
замена бит по таблице замен
перестановка бит
возведение в степень

4. Асимметричные криптосистемы

1. Какие шифры (механизмы обмена ключами) относятся к асимметричным (выбрать все верные):

Диффи–Хелмана (D-H)
Ривест–Шамир–Адлеман (RSA)
Криптография эллиптической кривой (ECC)

2. Какая связь существует между двумя ключами в асимметричной криптографии?

логическая
физическая
математическая
никакая

3. Верны ли утверждения? (выбрать все верные)

В асимметричных криптосистемах не решена проблема распределения ключей.
Асимметричные криптосистемы существенно медленнее симметричных.

5. Криптографические средства контроля целостности

1. Основу криптографического контроля целостности составляют понятия: выбрать все верные

электронная подпись +
хэш-функция +
алгоритм RSA
симметричное шифрование
асимметричное шифрование
блокчейн

2. Выберите верное утверждение:

благодаря криптографическим методам можно надежно контролировать целостность отдельных порций данных и их наборов
благодаря криптографическим методам можно надежно контролировать целостность всего непрерывного блока данных
благодаря криптографическим методам можно надежно контролировать целостность каждого символа в информационном блоке
нет верного ответа

3. К кодам аутентификации, используемым при контроле целостности информации предъявляются требования: выбрать все верные

невозможность вычисления значения проверочной комбинации для заданного сообщения без знания ключа;
невозможность подбора для заданного сообщения с известным значением проверочной комбинации другого сообщения, с известным значением, без знания ключа.
длина кода должна быть не менее 128 бит

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1.Тема работы.

2. Задачи работы.

3. Краткое описание хода выполнения работы.

4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

5. Выводы

Критерии оценивания:

- 75 – 100 баллов – при раскрытии всех разделов в полном объеме

- 0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формами промежуточной аттестации являютя экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

ответы на вопросы во время опроса по разделам дисциплины или пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На экзамене обучающийся отвечает на 2 вопроса, либо отвечает на 20 тестовых заданий

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-99	100
Шкала оценивания	Неуд		Хорошо	Отлично	
	не зачтено		зачтено		

Критерии оценивания при тестировании:

- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85…94 баллов – при правильном ответе на 16-18 вопросов;
- 75…84 баллов – при правильном ответе на 13-15 вопросов;
- 65…74 баллов – правильном ответе на 10-12 вопросов
- 25…64 – при правильном ответе только на 1-9 вопрос(ов);
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд		Хорошо	Хорошо	Отлично
	не зачтено		зачтено		

Примерный перечень вопросов на экзамен:

1. История криптографии. Классические алгоритмы шифрования. Стойкость классических шифров.
2. Симметричное и ассиметричное шифрование.
3. Модель угрозы Долева-Яо.
4. Протокол Нидхема-Шредера. Возможные атаки. Понятия аутентификации сущности и аутентификации сообщений.
5. Ассиметричная версия протокола Нидхема-Шредера.
6. Обобщенный алгоритм Евклида.
7. Понятие группы. Фактор-группа. Теорема Лагранжа. Порядок группы.
8. Циклические группы.
9. Предмет криптографии. Определения. Задачи. Исторические примеры.
10. Виды атак на криптографические алгоритмы. Понятие стойкости.
11. Классификация алгоритмов шифрования. Примеры простейших шифров.
12. Шифры замены. Математическая модель. Примеры.
13. Шифры перестановки. Математическая модель. Примеры.
14. Шифры гаммирования. Математическая модель. Примеры.
15. Принципы построения блочных шифров. Схема Фейстеля.
16. Алгоритм симметричного шифрования DES.
17. Алгоритм симметричного шифрования ГОСТ 28147-99.
18. Алгоритм симметричного шифрования Rijndael.
19. Алгоритмы симметричного шифрования IDEA и Blowfish.
20. Режимы выполнения алгоритмов симметричного шифрования.
21. Поточные криптосистемы. Принципы построения. Классификация. Проблема синхронизации.
22. Линейные конгруэнтные генераторы. Линейные регистры сдвига.
23. Поточные шифры. Отличия от блочных. Стойкость. Методы анализа.
24. Примеры поточных шифров на основе LFSR.
25. Примеры поточных шифров, использующих аддитивные генераторы.
26. Примеры поточных шифров на основе FCSR.
27. Математические методы криптоанализа: метод опробывания, методы на основе теории статистических решений.
28. Линейный криптоанализ.
29. Разностный криптоанализ.
30. Основные принципы построения асимметричных криптосистем. Стойкость.
31. Шифросистема RSA. Стойкость.
32. Шифросистема Эль-Гамаля. Стойкость.
33. Шифросистема на основе принципа «рюкзака».
34. Шифросистема Рабина. Стойкость.
35. Алгоритм обмена ключами Диффи-Хеллмана.
36. Хэш-функции. Требования. Типы функций хэширования.
37. Атаки на функции хэширования.
38. Функция хеширования MD5.
39. Функция хеширования SHA-1.

40. Функция хеширования ГОСТ 3411-94.
41. Функция хеширования СТБ 1176.1-99.
42. Общие положения электронной цифровой подписи. Задачи. Требования.
43. Прямая и арбитражная цифровая подписи. Примеры.
44. Стандарт электронной цифровой подписи DSS.
45. Цифровая подпись на основе алгоритмов с открытыми ключами. Схема Фиата-Шамира.
46. Цифровая подпись Эль-Гамаля. Схема RSA.
47. Стандарт электронной цифровой подписи DSS.
48. Стандарт электронной цифровой подписи ГОСТ-Р 34.10-94.
49. Стандарт электронной цифровой подписи СТБ 1176.2-99.
50. Применение эллиптических кривых в криптографии. Алгоритм шифрования на основе эллиптических кривых.
51. Алгоритмы обмена ключами и электронной цифровой подписи на основе эллиптических кривых.
52. Стеганографические методы защиты информации. Основные понятия и определения. Области применения.
53. Общая модель стеганосистемы. Проблема устойчивости. Стегоанализ.
54. Методы сокрытия информации в неподвижных изображениях.
55. Методы сокрытия информации в текстовых данных.
56. Протоколы аутентификации. Двусторонняя аутентификация.
57. Протоколы аутентификации. Односторонняя аутентификация.
58. Принципы работы механизмов проверки целостности данных

Примерный перечень тестовых заданий:

1. Выберите правильный вариант ответа: Криптосистема обладает следующими чертами: предусматривает использование одного и того же закрытого ключа для шифрования и дешифрования данных, характеризуется высокой скоростью работы, но сложностью безопасной передачи самого этого закрытого ключа. Назовите тип криптосистемы.

а Асимметричная криптосистема
б Симметричная криптосистема
в Криптосистема, использующая инфраструктуру открытых ключей (PKI)
г Избыточная криптосистема

1. Выберите правильный вариант ответа: Что из указанного не является предметом изучения криптографии?

а Шифрование с открытым ключом
б Создание алгоритмов надежной электронной подписи
в Метод циклического кода CRC
г Защита передаваемых данных от несанкционированного изменения

1. Выберите все правильные варианты ответов: Укажите все верные утверждения о шифровании данных.

а Любой известный алгоритм шифрования (исключая абсолютно стойкий шифр) можно взломать, перебрав все возможные варианты ключей шифрования

б При сопоставимой криптостойкости длина криптостойкого ключа для симметричного алгоритма шифрования меньше, чем для асимметричного алгоритма

в Современные алгоритмы шифрования ГОСТ 28147-89 (Россия) и AES (США) являются асимметричными

г Асимметричных алгоритмы шифрования работают медленнее по сравнению с симметричными алгоритмами

д Для асимметричных алгоритмов шифрования не известно доказательство нижней оценки их стойкости

1. Выберите правильный вариант ответа: RC4 - это …

а Алгоритм потокового шифрования (stream cipher)
б Алгоритм блочного шифрования (block cipher)
в Алгоритм асимметричного шифрования (public-key encryption)

г Алгоритм хэширования (hash algorithm)
д Алгоритм создания цифровой подписи (digital signature)

1. Выберите правильный вариант ответа: Для какого алгоритма шифрования типичной является длина ключа 1024 бит?

а RC4
б AES
в 3DES
г RSA
д ГОСТ 28147-89

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

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответам на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом : [учебное пособие] / Ю. А. Котов ; Ю. А. Котов ; Новосибирский государственный технический университет, Факультет автоматики и вычислительной техники. – Новосибирск : Изд-во НГТУ, 2017. – 1 файл (1,5 Мб). – URL: http://library.kuzstu.ru/meto.php?n=236930.pdf&type=nstu:common (дата обращения: 23.03.2026). – Текст : электронный.

2. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140740 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Котов, Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов. — Новосибирск : НГТУ, 2016. — 59 с. — ISBN 978-5-7782-2959-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118209 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

6.2 Дополнительная литература

1. Кожомбердиева, Г. И. Криптографическая защита информации и управление доступом на платформе Java : учебно-методическое пособие / Г. И. Кожомбердиева, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2016. — 87 с. — ISBN 978-5-7641-0856-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/91082 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие / М. А. Иванов, И. В. Чугунков. — Москва : НИЯУ МИФИ, 2012. — 400 с. — ISBN 978-5-7262-1676-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/75810 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Лапонина, О. Р. Криптографические основы безопасности : учебное пособие : [16+] / О. Р. Лапонина. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 244 с. : ил. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429092 (дата обращения: 16.04.2026). – Библиогр. в кн. – ISBN 5-9556-00020-5. – Текст : электронный.

4. Ищукова, Е. А. Криптографические протоколы и стандарты : учебное пособие : [16+] / Е. А. Ищукова, Е. А. Лобова ; Южный федеральный университет, Южный федеральный университет, Инженерно-технологическая академия. – Таганрог : Южный федеральный университет, 2016. – 80 с. :

ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=493059 (дата обращения: 17.04.2026). – Библиогр. в кн. – ISBN 978-5-9275-2066-4. – Текст : электронный.

5. Косолапов, Ю. В. Криптографические протоколы на основе линейных кодов : учебное пособие : [16+] / Ю. В. Косолапов ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 100 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598671 (дата обращения: 10.04.2026). – Библиогр. в кн. – ISBN 978-5-9275-3316-9. – Текст : электронный.

6. Фороузан, Б. А. Математика криптографии и теория шифрования : учебное пособие : [16+] / Б. А. Фороузан. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 511 с. : ил., схем. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428998 (дата обращения: 16.04.2026). – Библиогр. в кн. – ISBN 978-5-9963-0242-0. – Текст : электронный.

7. Игнатьев, Е. Б. Основы криптографии : учебное пособие / Е. Б. Игнатьев. — Иваново : ИГЭУ, 2020. — 88 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154559 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

8. Майстренко, Н. В. Основы теории информации и криптографии : учебное электронное издание : учебное пособие / Н. В. Майстренко, А. В. Майстренко. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 81 с. : табл., граф., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=570354 (дата обращения: 09.04.2026). – Библиогр. в кн. – ISBN 978-5-8265-1950-9. – Текст : электронный.

9. Аграновский, А. В. Практическая криптография : алгоритмы и их программирование : учебное пособие : [16+] / А. В. Аграновский, Р. А. Хади. – Москва : СОЛОН-ПРЕСС, 2009. – 256 с. – (Аспекты защиты). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=117663 (дата обращения: 14.04.2026). – ISBN 5-98003-002-6. – Текст : электронный.

6.3 Методическая литература

1. Криптографические методы защиты информации : методические материалы для обучающихся специальности 10.05.03 "Информационная безопасность автоматизированных систем" очной формы обучения / ФГБОУ ВО "Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева", Каф. информ. безопасности ; сост.: Е. В. Прокопенко, И. В. Чичерин. – Кемерово : КузГТУ, 2018. – 21 с. – URL: http://library.kuzstu.ru/meto.php?n=9123 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
2. Электронная библиотечная система «Лань» http://e.lanbook.com
3. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
4. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
5. Образовательная платформа «Юрайт» https://urait.ru/
6. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/projects/subscription/rus_titles_open.asp?
7. Национальная электронная библиотека https://rusneb.ru/

6.5 Периодические издания

1. Информационные системы и технологии : научно-технический журнал https://eivis.ru/browse/publication/542286
2. Информационные технологии и вычислительные системы : журнал https://elibrary.ru/contents.asp?titleid=8746
3. Информация и безопасность : научный журнал
4. Программные продукты и системы : международный научно-практический журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Методы и средства криптографической защиты информации"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Методы и средства криптографической защиты информации", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Libre Office
2. Mozilla Firefox
3. Google Chrome
4. 7-zip
5. Microsoft Windows
6. ESET NOD32 Smart Security Business Edition
7. Kaspersky Endpoint Security
8. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Методы и средства криптографической защиты информации"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.