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: 4B52DFD6B51FDA26ACBAF4AD87221F25
Владелец: Евсина Татьяна Алексеевна
Действителен: с 01.02.2024 до 26.04.2025

УТВЕРЖДАЮ
Заместитель директора по УР,
совмещающая обязанности по должности
директора филиала КузГТУ в г. Новокузнецке
_____ Т.А. Евсина
«27» июня 2024 г.

Фонд оценочных средств
дисциплины
МДК 02.02 Криптографические средства защиты информации

Специальность
«10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация
«Техник по защите информации»

Форма обучения
очная

Год набора 2022

Срок обучения на базе
среднего общего образования – 2 года 10 месяцев

Новокузнецк 2024 г.

1. Фонд оценочных средств для проведения текущего контроля, промежуточной аттестации обучающихся по дисциплине МДК 02.02 Криптографические средства защиты информации

1.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине.

Дисциплина направлена на формирование следующих компетенций выпускника:

№	Наименование разделов дисциплины	Содержание (темы) раздела	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
1	Введение. Предмет и задачи криптографии. История криптографии. Основные термины.	Предмет и задачи криптографии. История криптографии. Основные термины.	ОК 02.	Знать: источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач; Уметь: использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;	опрос обучающихся по контрольным вопросам, тестирование,
2	Раздел 1. Математические основы защиты информации	Тема 1.1. Математические основы криптографии	ПК 2.4.	Знать: основные понятия криптографии и типовых криптографических методов и средств защиты информации; Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; Иметь практический опыт: применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
3	Раздел 2. Классическая криптография	Тема 2.1. Методы криптографическ ого защиты информации Тема 2.2. Криптоанализ Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	ОК 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ОК 09.	Знать: информационно-коммуникационные технологии профессиональной деятельности; Уметь: использовать информационные технологии в профессиональной деятельности;	

			ПК 2.4.	Знать: основные понятия криптографии и типовых криптографических методов и средств защиты информации; Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; Иметь практический опыт: применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;	
4	Раздел 3. Современная криптография	Тема 3.1. Кодирование информации. Компьютеризация шифрования. Тема 3.2. Симметричные системы шифрования Тема 3.3. Асимметричные системы шифрования Тема 3.4. Аутентификация данных. Электронная подпись Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации Тема 3.6. Криптозащита информации в сетях передачи данных Тема 3.7. Защита информации в электронных платежных системах Тема 3.8. Компьютерная стеганография	ОК 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ПК 2.4.	Знать: основные понятия криптографии и типовых криптографических методов и средств защиты информации; Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; Иметь практический опыт: применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;	

1.2 Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут проводиться как при непосредственном взаимодействии педагогического работника с обучающимися, так и с использованием ресурсов ЭИОС КузГТУ, в том числе синхронного и (или) асинхронного взаимодействия посредством сети «Интернет».

1.2.1 Оценочные средства при текущем контроле

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам и (или) тестировании, и (или) практических работ (при наличии).

При проведении текущего контроля обучающимся письменно, либо устно необходимо ответить на 2 вопроса, выбранных случайным.

ПРИМЕРНОЕ ТЕСТИРОВАНИЕ

Тестирование включает как тесты с выбором ответа, так и задачи с вычисляемым ответом. Последний тип заданий формируется таким образом, чтобы верное решение задания демонстрировало владение материалом курса, но не требовало сложных вычислений. За час обучающийся должен ответить на 10 вопросов теста. Тест формируется таким образом, чтобы охватывать все темы, изучаемые в семестре, а вопрос по каждой теме попадает в тест случайным образом. Каждый верный ответ оценивается в 10 баллов.

Критерии оценивания:

90-100 баллов – при правильном ответе на 90-100%.

80-89 баллов – при правильном ответе на 80-89 %.

60-79 балла – при правильном ответе на 60-79 %.

0-59 баллов – при правильном ответе на менее 59 %.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	2	3	4	5

1.2.2 Оценочные средства при промежуточной аттестации

Формой промежуточной аттестации является **экзамен,** в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Экзамен проводится либо в форме опроса по контрольным вопросам, либо в форме компьютерного тестирования.

Опрос по контрольным вопросам

Во время опроса по контрольным вопросам обучающимся задается два вопроса выбранных случайным образом.

Критерии оценивания

- 85–100 баллов – при правильном и полном ответе на два вопроса;
- 65–84 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 25–64 баллов – 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	65-84	85-100
Школа оценивания	2	3	4	5

ПРИМЕРНОЕ ТЕСТИРОВАНИЕ

Тестирование включает как тесты с выбором ответа, так и задачи с вычисляемым ответом. Последний тип заданий формируется таким образом, чтобы верное решение задания демонстрировало владение материалом курса, но не требовало сложных вычислений. За час обучающийся должен ответить на 10 вопросов теста. Тест формируется таким образом, чтобы охватывать все темы, изучаемые в семестре, а вопрос по каждой теме попадает в тест случайным образом. Каждый верный ответ оценивается в 10 баллов.

Критерии оценивания:

90-100 баллов – при правильном ответе на 90-100%.

80-89 баллов – при правильном ответе на 80-89 %.

60-79 балла – при правильном ответе на 60-79 %.

0-59 баллов – при правильном ответе на менее 59 %.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	2	3	4	5

1.2.3 Методические материалы, определяющие процедуры оценивания знаний, умений, практического опыта деятельности, характеризующие этапы формирования компетенций

Порядок организации проведения текущего контроля и промежуточной аттестации представлен в Положении о проведении текущего контроля и промежуточной аттестации обучающихся, осваивающих образовательные программы среднего профессионального образования в КузГТУ (Ип 06/10)

2. Задания по разделам дисциплины
МДК.02.02 Криптографические средства защиты информации

Раздел 1. Математические основы защиты информации
ПК-2.4

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* Алгоритм, использующий симметричный ключ и алгоритм хэширования: а) HMAC б) 3DES в) ISAKMP-OAKLEY г) RSA	а
Задание 2. *Прочитайте текст, выберите один правильный ответ* Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования а) 3 б) 1 в) 2	б
Задание 3. *Прочитайте текст, выберите один правильный ответ* Использует ли отечественный стандарт симметричного шифрования дополнительный ключ: а) да; б) нет.	а
Задания открытого типа	
Задание 4. *Прочитайте текст и дополните ответ* Способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого называется _____	Шифрование
Задание 5. *Прочитайте текст и дополните ответ* Характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа – это _____	Криптостойкость
Задание 6. *Прочитайте текст и дополните ответ* Преобразование обычного, понятного текста в код называется _____	Кодирование
Задание 7.	

Прочитайте текст и дополните ответ Длина раундового ключа в отечественном стандарте симметричного шифрования составляет_____ бита.	32
Задание 8. *Прочитайте текст и дополните ответ* Метод, который применяют при шифровании с помощью аналитических преобразований, называется _____	Алгебра матриц
Задание 9. *Прочитайте текст и ответьте на вопрос* Сколько существует перестановок в стандарте DES?	3
Задание 10. *Прочитайте текст и ответьте на вопрос* Что требуется для восстановления зашифрованного текста?	Ключ

Раздел 2. Классическая криптография

ОК-01, ОК-09

ПК-2.4

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* **Когда появилось шифрование** а) пять тысяч лет назад б) четыре тысячи лет назад в) две тысячи лет назад	б
Задание 2. *Прочитайте текст, выберите один правильный ответ* **Что такое шифрование?** а) преобразовательный процесс исходного текста в зашифрованный б) упорядоченный набор из элементов алфавита в) нет правильного ответа	а
Задание 3. *Прочитайте текст, выберите один правильный ответ* **Криптографическая система представляет собой.** а) семейство T преобразований открытого текста, члены его семейства индексируются символом k б) систему в) программу	а
Задание 4. *Прочитайте текст, выберите один правильный ответ*	б

Длина раундового ключа в отечественном стандарте симметричного шифрования: а) 8 бит; б) 32 бита; в) 48 бит.	
Задания открытого типа	
Задание 5. *Прочитайте текст и дополните ответ* Обычно криптографические действия выполняет_____	Вычислитель
Задание 6. *Прочитайте текст и ответьте на вопрос* Наиболее известные разновидности полиалфавита?	Многоконтурные
Задание 7. *Прочитайте текст и ответьте на вопрос* Из скольких последовательностей состоит расшифровка текста по таблице Вижинера?	3
Задание 8. *Прочитайте текст и дополните ответ* Один из самых известных методов шифрования носит имя _____	Цезаря
Задание 9. *Прочитайте текст и дополните ответ* Зашифрованный файл, хранящийся на логическом диске, который подключается к системе как еще один логический диск – это_____	Виртуальный контейнер
Задание 10. *Прочитайте текст и дополните ответ* Первым известным применением шифра считается _____	Египетский текст

Раздел 3. Современная криптография

ОК-01

ПК-2.4

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* **Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом – это** а) алгоритм гаммирования б) алгоритм перестановки в) алгоритм подстановки	а

Задание 2. *Прочитайте текст, выберите один правильный ответ* **Сколько существует способов гаммирования?** а) 5 б) 2 в) 3	б
Задание 3. *Прочитайте текст, выберите один правильный ответ* **Чем определяется стойкость шифрования методом гаммирования** а) длина ключа б) свойством гаммы в) нет правильного ответа	б
Задание 4. *Прочитайте текст, выберите один правильный ответ* **Способ осуществления дешифрования текста при аналитических преобразованиях:** а) умножение матрицы на вектор б) деление матрицы на вектор в) перемножение матриц	а
Задания открытого типа	
Задание 5. *Прочитайте текст и ответьте на вопрос* Какая наука разрабатывает методы «вскрытия» шифров?	Криптоанализ
Задание 6. *Прочитайте текст и ответьте на вопрос* Как называется распределенный алгоритм, определяющий последовательность действий каждой из сторон?	Протокол
Задание 7. *Прочитайте текст и ответьте на вопрос* Как называется способ реализации криптографического метода, при котором все процедуры шифрования и расшифрования выполняются специальными электронными схемами по определенным логическим правилам?	Аппаратный
Задание 8. *Прочитайте текст и ответьте на вопрос* Как связаны ключи друг с другом в системе с открытым ключом?	Математически
Задание 9. *Прочитайте текст и ответьте на вопрос*	Шифр

Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты?	
Задание 10. *Прочитайте текст и ответьте на вопрос* Как называется сообщение, полученное после преобразования с использованием любого шифра?	Закрытый текст