**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: 65A182AF55E85519218FE36C1C7FB48A
Владелец: Евсина Татьяна Алексеевна
Действителен: с 16.11.2022 до 09.02.2024

**УТВЕРЖДАЮ**
Директор филиала КузГТУ
_____ Т.А. Евсина
«29» мая 2023 г.

# Фонд оценочных средств дисциплины
# 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
основное общего образования – 3 года 10 месяцев

Новокузнецк 2023 г.

**1. Фонд оценочных средств для проведения текущего контроля, промежуточной аттестации обучающихся по дисциплине**

**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 криптографического защиты информации Тема | ОК 01. | Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; | опрос обучающихся по контрольным вопросам, защита |

| | | | | | |
|---|---|---|---|---|---|
| | | 2.2. Криптоанализ<br>Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел | | Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам; | отчетов по практическим заданиям, тестирование |
| | | | ОК 09. | Знать: информационно-коммуникационные технологии профессиональной деятельности;<br>Уметь: использовать информационные технологии в профессиональной деятельности; | |
| | | | ПК 2.4. | Знать: основные понятия криптографии и типовых криптографических методов и средств защиты информации;<br>Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись;<br>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.<br>Тема 3.2. Симметричные системы шифрования<br>Тема 3.3. Асимметричные системы шифрования<br>Тема 3.4. Аутентификация данных. Электронная подпись<br>Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации<br>Тема | ОК 01. | Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам;<br>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;<br>Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в | |

| | | | | | |
|---|---|---|---|---|---|
| | | 3.6. Криптозащита информации в сетях передачи данных<br>Тема 3.7. Защита информации в электронных платежных системах<br>Тема<br>3.8. Компьютерная стеганография | | том числе электронную подпись;<br>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.

**ПРИМЕРНЫЕ ВОПРОСЫ:**

Критерии оценивания при текущем контроле:

- 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 |

**Например вопросы:**

| Вопрос | Ответ |
|---|---|
| Преобразование открытого текста сообщения в закрытый называется:<br>1)процедура шифрования;<br>2) алгоритм шифрования;<br>3) обеспечение аутентификации;<br>4) цифровая запись. | **1** |
| Входные параметры процесса шифрования (несколько верных ответов):<br>1) зашифрованный текст;<br>2) ключ;<br>3) открытый текст;<br>4) алгоритм. | **2,3** |
| Какие из сервисов реализуются при использовании криптографических преобразований (несколько верных ответов):<br>1) контроль целостности;<br>2) аутентификация;<br>3) шифрование;<br>4) алгоритм. | **1,2** |
| Какова длина блока алгоритма шифрования DES:<br>1) 16 бит;<br>2) 56 бит;<br>3) 64 бита;<br>4) 5 байт. | **3** |

**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 |
|---|---|---|---|---|

**Пример тестирования:**

| Вопрос | Ответ |
|---|---|
| Сколько всего циклов выполняется операция зашифровывания в алгоритме DES:<br>1) Ю;<br>2) 14;<br>3) 16;<br>4) 20. | **3** |
| Использует ли отечественный стандарт симметричного шифрования дополнительный ключ:<br>1) да;<br>2) нет. | **1** |
| Какое из этих утверждений является верным:<br>1) у S-блоков ГОСТ 4-битовые входы и выходы;<br>2) у S-блоков ГОСТ 4-битовые входы и 8-битовые выходы;<br>3) у S-блоков ГОСТ 8-битовые входы и 4-битовые выходы. | **1** |
| Длинараундового ключа в отечественном стандарте симметричного шифрования:<br>1) 8 бит;<br>2) 32 бита;<br>3) 48 бит. | **2** |

**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 |

**Например вопросы:**

| Вопрос | Ответ |
|---|---|
| Что такое шифрование?<br>а) преобразовательный процесс исходного текста в зашифрованный<br>б) упорядоченный набор из элементов алфавита<br>в) нет правильного ответа | **А** |
| Метод, который применяют при шифровании с помощью аналитических преобразований:<br>А) Факториал<br>Б) алгебры матриц<br>В) матрица | **Б** |
| Алгоритм, использующий симметричный ключ и алгоритм хэширования:<br>а) HMAC<br>б) 3DES<br>в) ISAKMP-OAKLEY<br>г) RSA | **А** |
| Способ осуществления дешифрования текста при аналитических преобразованиях:<br>а) умножение матрицы на вектор | **А** |

| | |
|---|---|
| б) деление матрицы на вектор<br>в) перемножение матриц | |

**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 |

| Вопрос | Ответ |
|---|---|
| То, что применяют в качестве ключа при шифровании с помощью аналитических преобразований: | матрица А+ |
| Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст: | Кластеризация ключей |
| Алгоритм, основанный на сложности разложения больших чисел на два исходных простых сомножителя: | RSA |
| Что такое криптостойкость? | характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа |

**Оценочные средства для формирования компетенции**

**ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам**

**Задания закрытого типа**

| Вопрос | Ответ |
|---|---|
| Шифрование - это.<br>А) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств<br>Б) удобная среда для вычисления конечного пользователя<br>В) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого | **В** |
| Кодирование - это.<br>А) написание программы<br>Б) преобразование обычного, понятного текста в код<br>В) преобразование | **Б** |
| Что требуется для восстановления зашифрованного текста<br>А) матрица<br>Б) вектор<br>В) ключ | **В** |
| Когда появилось шифрование<br>А) пять тысяч лет назад<br>Б) четыре тысячи лет назад<br>В) две тысячи лет назад | **Б** |
| Первым известным применением шифра считается<br>А) египетский текст<br>Б) нет правильного ответа<br>В) русский | **А** |

**Задания открытого типа**

| Вопрос | Ответ |
|---|---|
| Какой ключ используется в шифре ГОСТ | **256-битовый** |
| Сколько существует перестановок в стандарте DES | **3** |
| Один из самых известных методов шифрования носит имя. | **Цезеря** |
| Зашифрованный файл, хранящийся на логическом диске, который подключается к системе как еще один логический диск - это. | **Виртуальный контейнер** |

| | |
|---|---|
| Устройство, дающее статически случайный шум - это. | **Генератор случайных числе** |

**Оценочные средства для формирования компетенции**

**ОК 02.** Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

| Вопрос | Ответ |
|---|---|
| **Криптографическая система представляет собой.**<br>А) семейство T преобразований открытого текста, члены его семейства индексируются символом k<br>Б) систему<br>В) программу | **А** |
| Пространство ключей k - это.<br>А) длина ключа<br>Б) набор возможных значений ключа<br>В) нет правильного ответа | **Б** |
| Криптосистемы разделяются на:<br>А) симметричные<br>Б) ассиметричные<br>В) с открытым ключом | **А,Б,В** |
| Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования<br>А) 3<br>Б) 1<br>В) 2 | **Б** |
| Когда был введен в действие ГОСТ 28147-89<br>А) 1990<br>Б) 1995<br>В) 1890 | **А** |

**Задания открытого типа**

| Вопрос | Ответ |
|---|---|
| Какие перестановки существуют в стандарте DES | **Расширенные, сокращенные** |
| Какие дополнительные порты ввода-вывода содержит УКЗД: | **COM,**<br>**USB** |
| Устройство, дающее статически случайный шум - это. | **Генератор случайных чисел** |
| Криптографические действия выполняет. | **Вычислитель** |
| Наиболее известные разновидности полиалфавита: | **Многоконтурные** |

**Оценочные средства для формирования компетенции**

**ОК 09. Использовать информационные технологии в профессиональной деятельности.**

**Задания закрытого типа**

| Вопрос | Ответ |
|---|---|
| Сколько ключей используется в системах с открытым ключом<br>А) 1<br>Б) 3<br>В) 2 | **В** |
| Какие ключи используются в системах с открытым ключом<br>А) Закрытый<br>Б) открытый<br>В) нет правильного ответа | **А** |
| Как связаны ключи друг с другом в системе с открытым ключом<br>А) логически<br>Б) алгоритмически<br>В) математически | **В** |
| Электронной подписью называется.<br>А) присоединяемое к тексту его криптографическое преобразование<br>Б) зашифрованный текст<br>В) текст | **А** |
| Криптостойкость - это.<br>А) свойство гаммы<br>Б) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа<br>В) все ответы верны | **Б** |

**Задания открытого типа**

| Вопрос | Ответ |
|---|---|
| Какие бывают состояния процессоров: | **Готовый** |
| Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты? | **Шифр** |
| Как называется сообщение, полученное после преобразования с использованием любого шифра? | **Закрытый текст** |
| Что в криптографии называют открытым текстом? | **Исходное сообщение** |
| Гарантирование невозможности несанкционированного изменения информации - это: | **Обеспечение целостности** |

**Оценочные средства для формирования компетенции**
**ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.**
**Задания закрытого типа**

| Вопрос | Ответ |
|---|---|
| Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом - это.<br>А) алгоритм гаммирования<br>Б) алгоритм перестановки<br>В) алгоритм подстановки | **А** |
| Самой простой разновидность подстановки является<br>А) простая перестановка<br>Б) простая замена<br>В) перестановка | **А** |
| Из скольких последовательностей состоит расшифровка текста по таблице Вижинера<br>А) 5<br>Б) 3<br>В) 4 | **Б** |
| Сколько существует способов гаммирования<br>А) 5<br>Б) 2<br>В) 3 | **Б** |
| Чем определяется стойкость шифрования методом гаммирования<br>А) длина ключа<br>Б) свойством гаммы<br>В) нет правильного ответа | **Б** |

**Задания открытого типа**

| Вопрос | Ответ |
|---|---|
| Какая наука разрабатывает методы «вскрытия» шифров? | **Криптоанализ** |
| Как называется распределенный алгоритм, определяющий последовательность действий каждой из сторон? | **Протокол** |
| Как называется способ реализации криптографического метода, при котором все процедуры шифрования и расшифрования выполняются специальными электронными схемами по определенным логическим правилам? | **Аппаратный** |
| Выберите то, как связаны ключи друг с другом в системе с открытым ключом: | **Математически** |
| Ключи, используемые в системах с открытым ключом: | **Открытый, закрытый** |

**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)