**ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»**

***Утвержден решением***
***Ученого совета ДГУНХ,***
***протокол № 11***
***от 06 июня 2023 г***

**КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ «КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

## Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем
## Квалификация – техник по защите информации

## Форма обучения – очная



Махачкала – 2023

**УДК 681.518(075.8)**

**ББК 32.81.73**

**Составитель –** Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внутренний рецензент –** Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внешний рецензент –** Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры прикладной математики Дагестанского государственного университета.

**Представитель работодателя** - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

Фонд оценочных средств *разработаны в соответствии с требованиями федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённого приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г., № 1553, в соответствии с приказом Министерства образования и науки РФ от 14 июня 2013г., № 464 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования».*

Фонд оценочных средств по дисциплине «Криптографические средства защиты информации» размещены на официальном сайте www.dgunh.ru

Гасанова З.А. Фонд оценочных средств по дисциплине «Криптографические средства защиты информации» по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. – Махачкала: ДГУНХ, 2023 г. – 52 с.

Рекомендован к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 г.

Рекомендован к утверждению руководителем образовательной программы СПО – программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, к.пед.н., Гасановой З.А.

Одобрен на заседании кафедры «Информационные технологии и информационная безопасность» 31 мая 2023 г., протокол № 10.

**СОДЕРЖАНИЕ**

## Назначение оценочных материалов

Фонд оценочных средств для текущего контроля успеваемости (оценивания хода освоения дисциплин), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по дисциплине) обучающихся по дисциплине «Криптографические средства защиты информации» на соответствие их учебных достижений поэтапным требованиям соответствующей образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Фонд оценочных средств по дисциплине «Криптографические средства защиты информации» включают в себя: перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения ОПОП; методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Фонд оценочных средств сформированы на основе ключевых принципов оценивания:

- валидности: объекты оценки должны соответствовать поставленным целям обучения;
- надежности: использование единообразных стандартов и критериев для оценивания достижений;
- объективности: разные обучающиеся должны иметь равные возможности для достижения успеха.

Основными параметрами и свойствами оценочных материалов являются:

- предметная направленность (соответствие предмету изучения конкретной дисциплины);
- содержание (состав и взаимосвязь структурных единиц, образующих содержание теоретической и практической составляющих дисциплины);
- объем (количественный состав оценочных материалов);
- качество оценочных материалов в целом, обеспечивающее получение объективных и достоверных результатов при проведении контроля с различными целями.

## РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины

### 1.1 Перечень формируемых компетенций

| код компетенции | формулировка компетенции |
|---|---|
| ПК-2.1. | Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. |
| ПК-2.2. | Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. |
| ПК-2.4. | Осуществлять обработку, хранение и передачу информации ограниченного доступа. |

### 1.2. Перечень компетенций с указанием видов оценочных средств

| ***Формируемые компетенции*** | ***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*** | ***Уровни освоения компетенций*** | ***Критерии оценивания сформированности компетенций*** | ***Виды оценочных средств*** |
|---|---|---|---|---|
| **ПК-2.1.** Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. | **Знать:**<br>– основные задачи и понятия криптографии;<br>– требования к шифрам и основные характеристики шифров; | Пороговый уровень | Обучающийся слабо (частично) знает основные задачи, понятия криптографии и требования к шифрам и основные характеристики шифров; | **Блок А** – задания репродуктивного уровня<br>— тестовые задания;<br>- вопросы для устного опроса |
| | | Базовый уровень | Обучающийся с незначительными ошибками и отдельными пробелами знает основные задачи, понятия криптографии и требования к шифрам и основные | |

| *Формируемые компетенции* | *Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций* | *Уровни освоения компетенций* | *Критерии оценивания сформированности компетенций* | *Виды оценочных средств* |
|---|---|---|---|---|
| | | | характеристики шифров; | |
| | | Продвинутый уровень | Обучающийся с требуемой степенью полноты и точности знает основные задачи, понятия криптографии и требования к шифрам и основные характеристики шифров; | |
| | **Уметь:**<br>- использовать базовые знания теории чисел для реализации арифметических алгоритмов в криптографических системах | Пороговый уровень | Обучающийся слабо (частично) умеет использовать базовые знания теории чисел для реализации арифметических алгоритмов в криптографических системах | **Блок В** – задания реконструктивного уровня<br>– задачи;<br>- тематика рефератов;<br>- тематика презентаций. |
| | | Базовый уровень | Обучающийся с незначительными затруднениями умеет использовать базовые знания теории чисел для реализации арифметических алгоритмов в криптографических системах | |
| | | Продвинутый уровень | Обучающийся умеет использовать базовые знания теории чисел для реализации арифметических алгоритмов в криптографических системах | |
| | **Владеть:** | Пороговый | Обучающийся слабо | **Блок С** – задания |

| *Формируемые компетенции* | *Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций* | *Уровни освоения компетенций* | *Критерии оценивания сформированности компетенций* | *Виды оценочных средств* |
|---|---|---|---|---|
| | – навыками математического моделирования в криптографии. | уровень | (частично) владеет навыками математического моделирования в криптографии. | практико-ориентированного уровня<br>– лабораторные работы. |
| | | Базовый уровень | Обучающийся с небольшими затруднениями владеет навыками математического моделирования в криптографии. | |
| | | Продвинутый уровень | Обучающийся свободно владеет навыками математического моделирования в криптографии. | |
| **ПК-2.2.** Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. | **<u>Знать:</u>**<br>– принципы построения криптографических алгоритмов.<br>– принципы построения ЭЦП | Пороговый уровень | Обучающийся слабо (частично) знает принципы построения криптографических алгоритмов и построения ЭЦП | **Блок А** – задания репродуктивного уровня<br>— тестовые задания;<br>- вопросы для устного опроса |
| | | Базовый уровень | Обучающийся с незначительными ошибками и отдельными пробелами знает принципы построения криптографических алгоритмов и построения ЭЦП | |
| | | Продвинутый уровень | Обучающийся с требуемой степенью полноты и точности знает принципы | |

| *Формируемые компетенции* | *Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций* | *Уровни освоения компетенций* | *Критерии оценивания сформированности компетенций* | *Виды оценочных средств* |
|---|---|---|---|---|
| | | | построения криптографических алгоритмов и построения ЭЦП | |
| | **<u>Уметь:</u>**<br>– использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;<br>– применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности | Пороговый уровень | Обучающийся слабо (частично) умеет использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки и применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности | **Блок В** – задания реконструктивного уровня<br>– задачи;<br>- тематика рефератов;<br>- тематика презентаций. |
| | | Базовый уровень | Обучающийся с незначительными затруднениями умеет использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки и применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности | |
| | | Продвинутый уровень | Обучающийся умеет использовать частотные | |

| *Формируемые компетенции* | *Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций* | *Уровни освоения компетенций* | *Критерии оценивания сформированности компетенций* | *Виды оценочных средств* |
|---|---|---|---|---|
| | | | характеристики открытых текстов для анализа простейших шифров замены и перестановки и применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности | |
| | **<u>Владеть:</u>**<br>– криптографической терминологией<br>– навыками использования ПЭВМ в анализе простейших шифров; | Пороговый уровень | Обучающийся слабо (частично) владеет криптографической терминологией и навыками использования ПЭВМ в анализе простейших шифров; | **Блок С** – задания практико-ориентированного уровня<br>– лабораторные работы. |
| | | Базовый уровень | Обучающийся с небольшими затруднениями владеет навыками криптографической терминологией и навыками использования ПЭВМ в анализе простейших шифров; | |
| | | Продвинутый уровень | Обучающийся свободно владеет навыками криптографической терминологией и навыками использования ПЭВМ в анализе простейших | |

| *Формируемые компетенции* | *Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций* | *Уровни освоения компетенций* | *Критерии оценивания сформированности компетенций* | *Виды оценочных средств* |
|---|---|---|---|---|
| | | | шифров; | |
| **ПК-2.4.** Осуществлять обработку, хранение и передачу информации и ограниченного доступа. | **Знать:**<br>– криптографические стандарты и их использование в информа-ционных системах. | Пороговый уровень | Обучающийся слабо (частично) знает криптографические стандарты и их использование в информационных системах. | **Блок А** – задания репродуктивного уровня<br>— тестовые задания;<br>- вопросы для устного опроса |
| | | Базовый уровень | Обучающийся с незначительными ошибками и отдельными пробелами знает криптографические стандарты и их использование в информационных системах. | |
| | | Продвинутый уровень | Обучающийся с требуемой степенью полноты и точности знает криптографические стандарты и их использование в информационных системах. | |
| | **Уметь:**<br>– применять средства ЭЦП | Пороговый уровень | Обучающийся слабо (частично) умеет применять средства ЭЦП | **Блок В** – задания реконструктивного уровня<br>– задачи;<br>- тематика рефератов;<br>- тематика презентаций. |
| | | Базовый уровень | Обучающийся с незначительными затруднениями умеет применять средства ЭЦП | |

| *Формируемые компетенции* | *Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций* | *Уровни освоения компетенций* | *Критерии оценивания сформированности компетенций* | *Виды оценочных средств* |
|---|---|---|---|---|
| | | Продвинутый уровень | Обучающийся умеет применять средства ЭЦП | |
| | **Владеть:**<br>– навыками программирования криптографических алгоритмов. | Пороговый уровень | Обучающийся слабо (частично) владеет навыками программирования криптографических алгоритмов. | **Блок С** – задания практико-ориентированного уровня<br>– лабораторные работы. |
| | | Базовый уровень | Обучающийся с небольшими затруднениями владеет навыками программирования криптографических алгоритмов. | |
| | | Продвинутый уровень | Обучающийся свободно владеет навыками программирования криптографических алгоритмов. | |

## РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине

**Для проверки сформированности компетенции ПК-2.1.** Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

**А.1 Тестовые задания по дисциплине**

1. Шифры замены бывают:
   a) простые одноалфавитные
   b) одноконтурные полиалфавитные.
   c) многоконтурные полиалфавитные.
   d) монофонические полиалфавитные.
   e) усложненные по маршрутам

2. Криптосистемы с секретным ключом называют:
   a) Симметричными криптосистемами.
   b) Асимметричными криптосистемами.
   c) Одноключевыми криптосистемами.
   d) Двуключевыми криптосистемами.

3. Хэш-функция должна обладать следующими функциями:
   a) Устойчивость к коллизиям.
   b) Симметричность.
   c) Однонаправленность.
   d) Линейность

4. Устройство «Сцитало» является примером шифрования:
   a) Методом подстановки
   b) Методом перестановки
   c) Методом гаммирования

5. Шифры делятся на
   a) Блоковые и последовательные
   b) Блочные и поточные
   c) Потоковые и дискретные

6. К достоинствам блочных шифров относят
   a) высокую скорость шифрования
   b) дешевизну реализации
   c) похожесть процедур шифрования и расшифрования

7. Устройство «Сцитало» является примером шифрования:

a) Методом подстановки
b) Методом перестановки
c) Методом гаммирования

8. Шифры делятся на
a) Блоковые и последовательные
b) Блочные и поточные
c) Потоковые и дискретные

9. К достоинствам блочных шифров относят
a) высокую скорость шифрования
b) дешевизну реализации
c) похожесть процедур шифрования и расшифрования

10. Преобразование открытого текста сообщения в закрытый называется:
a) процедура шифрования;
b) алгоритм шифрования;
c) обеспечение аутентификации;
d) цифровая запись.

11. Входные параметры процесса шифрования {несколько верных ответов):
a) зашифрованный текст;
b) ключ;
c) открытый текст;
d) алгоритм.

12. В чем состоит задача криптографа?
a) взломать систему защиты
b) обеспечить конфиденциальность и аутентификацию передаваемых сообщений

13. Наука о скрытой передаче информации путем сохранения в тайне самого факта
a) передачи называется
b) криптография
c) стеганография

14. Что такое криптология?
a) защищенная информация
b) область доступной информации
c) тайная область связи

15. Какой режим применяется для шифрования небольших объемов информации, размером не более одного блока или для шифрования ключей

a) Обратная связь по шифротексту
b) Электронная кодовая книга
c) Сцепление блоков шифротекста

16. Какие из сервисов реализуются при использовании криптографических преобразований {несколько верных ответов):
a) контроль целостности;
b) аутентификация;
c) шифрование;
d) алгоритм.

17 Знание ключа позволяет:
a) использовать криптографические сервисы безопасности;
b) обеспечить аутентификацию;
c) предотвратить утечку информации;
d) выполнить обратное преобразование.

18. Что в криптографии понимается под термином «элементарное опробование»:
a) операция над двумя «-разрядными двоичными числами;
b) проверка ключа на целостность;
c) сопоставление двух паролей;
d) передача ключа по какому-либо каналу связи.

19. Чем определяется уровень надежности применяемых криптографических преобразований:
a) значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях;
b) сложностью комбинации символов, выбранных случайным образом;
c) использованием большого числа ключей для шифрования;
d) отношением количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию.

20. Ниже перечислены механизмы защиты информационных систем от несанкционированного доступа. Что здесь лишнее:
a) идентификация и аутентификация пользователей и субъектов доступа;
b) управление доступом;
c) обеспечение постоянного числа пользователей сети;
d) обеспечения целостности;
e) регистрация и учет.

21. Что называется имитовставкой:

a) это блок данных, переменной длины, который вырабатывают по определенному правилу из открытых данных с использованием ключа и затем добавляют к зашифрованным данным для обеспечения их имитозащиты;
b) это блок данных фиксированной длины, который вырабатывают по определенному правилу из открытых данных с использованием ключа и затем добавляют к зашифрованным данным для обеспечения их имитозащиты.

22. Какой алгоритм не используется при симметричном шифровании:
a) поточное шифрование;
b) побитовое шифрование;
c) блочное шифрование;
d) алгоритм Эль-Гамаля.

23. Алгоритм RSA основан на использовании
a) односторонней функции
b) односторонней функции с лазейкой
c) надежного простого числа
d) составного числа, образованного двумя простыми числами

24. К симметричным криптосистемам относятся алгоритмы
a) DES
b) 3DES
c) AES RSA
d) TWOFISH

25. Какой из режимов алгоритма DES используется для построения шифров гаммирования?
a) электронная кодовая книга;
b) сцепление блоков шифра;
c) обратная связь по шифротексту;
d) обратная связь по выходу.

26. Какова длина блока алгоритма шифрования DES:
a) 16 бит;
b) 56 бит;
c) 64 бита;
d) 5 байт.

27. Сколько всего циклов выполняется операция зашифровывания в алгоритме DES:
a) 10;

b) 14;
c) 16;
d) 20.

28. Что является преимуществом симметричного шифрования:
a) скорость выполнения криптографических преобразований;
b) легкость внесения изменений в алгоритм шифрования;
c) секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
d) применение в системах аутентификации (электронная подпись).

29. Какой размер ключа в отечественном стандарте симметричного шифрования:
a) 56 бит;
b) 124 бит;
c) 256 бит.

30. Какие из режимов шифрования данных не включает в себя отечественный стандарт симметричного шифрования:
a) режим гаммировани;
b) режим простой замены;
c) режим обратной связи по шифротексту;
d) режим гаммирования с обратной связью.

31. Режим выработка имитовставки в стандарте шифрования ГОСТ 28147-89 гарантирует:
a) конфиденциальность сообщения
b) целостность сообщения
c) аутентификацию сообщения

32. Использует ли отечественный стандарт симметричного шифрования дополнительный ключ:
a) да;
b) нет.

33. Какое из этих утверждений является верным:
a) у S-блоков ГОСТ 4-битовые входы и выходы;
b) у S-блоков ГОСТ 4-битовые входы и 8-битовые выходы;
c) у S-блоков ГОСТ 8-битовые входы и 4-битовые выходы.

34. Используется ли в отечественном стандарте симметричного шифрования процедура генерации подключей из ключей, как в DES:
a) да, но эта процедура сравнительно проста;
b) не используется;

c) используется аналогичная по сложности процедура.

35. В отечественном стандарте симметричного шифрования применяется подстановка, основанная на применении S-блоков. Сколько таких блоков используется в ГОСТ:
    a) 8;
    b) 12;
    c) 16;
    d) 24.

36. Длина раундового ключа в отечественном стандарте симметричного шифрования:
    a) 8 бит;
    b) 32 бита;
    c) 48 бит.

37. Выберите правильное утверждение:
    a) в отечественном стандарте симметричного шифрования есть начальная, но нет конечной битовых перестановок шифруемого блока;
    b) в отечественном стандарте симметричного шифрования нет начальной и конечной битовых перестановок шифруемого блока, так как они не влияют на стойкость шифра;
    c) в DES нет начальной и конечной битовых перестановок шифруемого блока.

38. Что означает «многократное шифрование» применительно к блочным шифрам:
    a) повторное применение алгоритма шифрования к шифротексту с теми же ключами;
    b) шифрование одного и того же блока открытого текста несколько раз с несколькими ключами;
    c) повторное применение алгоритма шифрования к шифротексту с другими ключами;
    d) увеличение числа этапов шифрования открытого текста.

**А2. Вопросы для устного опроса**

1. История криптографии.
2. Основные задачи криптографии.
3. Базовые определения и принципы
4. Виды криптосистем
5. Обзор исторических шифров
6. Классификация поточных шифров
7. Регистр сдвига с линейной обратной связью

8. Нелинейные регистры сдвига с обратной связью
9. Классификация блочных шифров
10. Регистр сдвига с линейной обратной связью
11. Нелинейные регистры сдвига с обратной связью
12. Основные определения и функционал
13. Требования к протоколам
14. Функции, используемые в криптографических алгоритмах
15. Элементы теории чисел
16. Формальное математическое определение криптосистемы
17. Основные характеристики и структура алгоритма DES.
18. Процедура расширения ключа.
19. Криптостойкость алгоритма DES.
20. Основные характеристики и структура алгоритма AES.
21. Основные схемы работы алгоритма ГОСТ 28147-89
22. Режимы работы алгоритма ГОСТ 28147-89
23. Криптостойкость алгоритма.
24. Модификации алгоритма и их анализ
25. Новый стандарт российского блочного шифра
26. Описание алгоритма Диффи-Хеллман
27. Протокол Диффи-Хеллмана
28. Математическая модель ассиметричных шифров
29. Приложения ассиметричной криптографии
30. Распределенные системы, построенные на ассиметричной криптографии
31. Основные свойства ассиметричного шифрования
32. Описание алгоритма RSA
33. Приложения RSA
34. Возможные атаки на RSA

## Блок В. Задания реконструктивного уровня («уметь»)

### В1. Задачи

1. Привести результат выражений 5, 16, 27, -4, -13, 3 + 8, 3 — 8, 3-8, 3-8-5:
    а. по модулю 10,
    б. по модулю 11.
1. Вычислить, используя быстрые алгоритмы возведения в степень, $2^8$ mod 10, $3^7$ mod 10, $7^{19}$ mod 100, $7^{57}$ mod 100.
2. Разложить на простые множители числа 108, 77, 65, 30, 159.
3. Определить, какие из пар чисел (25,12), (25,15), (13,39), (40,27) взаимно просты.
4. Найти значения функции Эйлера φ(14), φ (20).

5. Используя свойства функции Эйлера, вычислить φ *(53)*, φ (21), φ(159).
6. Используя теорему Ферма, вычислить $3^{13} \bmod 13$, $5^{22} \bmod 11$, $3^{17} \bmod 5$.
7. Используя теорему Эйлера, вычислить $3^{9} \bmod 20$, $2^{14} \bmod 21$, $2^{107} \bmod 159$.
8. С помощью алгоритма Евклида найти gcd(21,12), gcd(30,12), gcd(24,40), gcd(33,16).
9. С помощью обобщенного алгоритма Евклида найти значения $x$ и $y$ в уравнениях
   а. 21x + 12y = gcd(21,12),
   б. 30x + 12y = gcd(30,12),
   в. 24x + 40y = gcd(24,40),
   г. 33x + 16y= gcd(33,16).
13. Вычислить $3^{-1} \bmod 7$, $5^{-1} \bmod 8$, $3^{-1} \bmod 53$, $10^{-1} \bmod 53$.
14. Выписать все простые числа, меньшие 100. Какие из них соответствуют виду $p = 2q + 1$, где $q$ также простое?
15. Для реализации протокола "ментальный покер" выбраны сследующие общие параметры: p = 23, α= 5, β = 7, γ = 14. Кроме того, имеются следующие варианты для Алисы и Боба:
   а. $C_A = 13$, $C_B = 5$, Алиса перемешивает карты по правилу (1,2,3) → (3,2,1), Боб выбирает первое число и использует перестановку (1,2) → (2,1). Алиса выбирает второе из полученных чисел.
   б. $C_A = 7$, $C_B = 15$, Алиса перемешивает карты по правилу (1,2,3) → (1,3,2), Боб выбирает второе число использует перестановку (1,2) → (1,2). Алиса выбирает первое из полученных чисел.
   в. $C_A = 19$, $C_B = 3$, Алиса перемешивает карты по правилу (1,2,3) → (2,1,3), Боб выбирает второе число и использует перестановку (1,2) → (2,1). Алиса выбирает второе из полученных чисел.
   г. $C_A = 9$, $C_B = 7$, Алиса перемешивает карты по правилу (1,2,3) → (3,2,1), Боб выбирает третье число и использует перестановку (1,2) → (1,2). Алиса выбирает второе из полученных чисел.
   д. $C_A = 15$, $C_B = 5$, Алиса перемешивает карты по правилу (1,2,3) → (1,2,3), Боб выбирает первое число и использует перестановку (1,2) → (2,1)- Алиса выбирает первое из полученных чисел.

   Определить, какие карты достанутся Алисе и Бобу. Какие передаваемые числа будет наблюдать Ева?

16. В системе электронных денег выбраны секретные параметры банка P = 17, Q = 7, c = 7 7 , а соответствующие им открытые параметры $N = 119$, $d = 5$. Сформировать электронные банкноты со следующими номерами:

   а. $n$ = 11 при r = 5,
   б $n$ = 99 при r = 6,

в. $n$ = 55 при $r$ = 10,

г. $n$ = 44 при $r$ = 15,

Д $n$ = 77 при $r$ = 30.

17. Зашифровать с помощью алгоритма S-DES сообщение X = 123 на ключе K = 568. Полученное шифр-сообщение дешифровать.

| P10 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 5 | 2 | 7 | 4 | 10 | 1 | 9 | 8 | 6 |

| P8 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | 3 | 7 | 4 | 8 | 5 | 10 | 9 |

| IP | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2 | 6 | 3 | 1 | 4 | 8 | 5 | 7 |

| $IP^{-1}$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | 1 | 3 | 5 | 7 | 2 | 8 | 6 |

| E/P | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 3 | 2 | 3 | 4 | 1 |

| P4 | | | |
|---|---|---|---|
| 2 | 4 | 3 | 1 |

| S1 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 0 | 3 | 2 |
| 1 | 3 | 2 | 1 | 0 |
| 2 | 0 | 2 | 1 | 3 |
| 3 | 3 | 1 | 3 | 1 |

| S2 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 1 | 2 | 3 |
| 1 | 2 | 0 | 1 | 3 |
| 2 | 3 | 0 | 1 | 0 |
| 3 | 2 | 1 | 0 | 3 |

2. Зашифровать с помощью алгоритма S-AES сообщение X = (7 5 4 5) на ключе К = (8 6 1 е). Полученное шифр-сообщение дешифровать.

$\varphi(x) = x^4 \oplus x \oplus 1$

преобразование **Sub Half-Bytes*()**

| **x** | **Y** | | | |
|---|---|---|---|---|
| | **00** | **01** | **10** | **11** |
| **00** | 9 | e | 5 | 1 |
| **01** | 8 | b | d | a |
| **10** | 6 | 7 | f | 3 |
| **11** | c | 4 | 0 | 2 |

преобразование **ISub Half-Bytes*()**

| **x** | **Y** | | | |
|---|---|---|---|---|
| | **00** | **01** | **10** | **11** |
| **00** | e | 3 | f | B |
| **01** | d | 2 | 8 | 9 |
| **10** | 4 | 0 | 7 | 5 |
| **11** | c | 6 | 1 | a |

**Mix Columns*()**

$$\begin{bmatrix} S_{0c}' \\ S_{1c}' \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} S_{0c} \\ S_{1c} \end{bmatrix}, 0 \le c \le 1,$$

где с – номер столбца массива данных. В результате такого умножения полубайты столбца $S_{0c}$ и $S_{1c}$ заменяются соответственно на полубайты:

$$S_{0c}' = (\{3\} \bullet S_{0c}) \oplus (\{2\} \bullet S_{1c}),$$
$$S_{1c}' = (\{2\} \bullet S_{0c}) \oplus (\{3\} \bullet S_{1c}).$$

**Алгоритм выработки подключей**

$K_{00}^{r} = \text{Sub Half-Bytes*}(K_{11}^{r-1}) \oplus K_{00}^{r-1}$;
$K_{10}^{r} = \text{Sub Half-Bytes*}(K_{01}^{r-1}) \oplus K_{10}^{r-1} \oplus 2^{r-2}$;
$K_{01}^{r} = K_{00}^{r} \oplus K_{01}^{r-1}$;
$K_{11}^{r} = K_{10}^{r} \oplus K_{11}^{r-1}$,

20. Найти все допустимые варианты выбора параметра g в системе Диффи-Хеллмана при p = 11.
21. Вычислить секретные ключи $У_А$ $У_В$ и общий ключ $Z_{АВ}$ для системы Диффи-Хеллмана с параметрами:
    а. p = 23, 0 = 5, $X_А$ = Ь, $X_в$ = 7,
    б. p=19, 0 = 2, $X_А$ = 5, $X_в$ = 7,

в. p = 23, 0 = 7, $X_A$ = 3, $X_в$=4,
г. p = 17, 0 = 3, $X_A$ = 10, $X_в$ = 5,
д. p = 19, 0 = 10, $X_A$ = 4, $X_в$ = 8.

22. Пусть для схемы Диффи-Хеллмана известны открытые параметры p = 59 и g = 13. Чему будет равен секретный ключ К, если Алисе известен закрытый ключ a = 1201 и Боб передал ей свой открытый ключ B = 37?
23. Пусть для схемы Диффи-Хеллмана известны открытые параметры p = 59 и g = 13. Чему будет равен секретный ключ К, если Бобу известен закрытый ключ b = 433 и Алиса передала ему свой открытый ключ A = 52?
24. Пусть для схемы Диффи-Хеллмана известны открытые параметры p = 61 и g = 17. Чему будет равен секретный ключ К, если Алисе известен закрытый ключ a = 421 и Боб передал ей свой открытый ключ B = 26?
25. В системе RSA с заданными параметрами $P_A$, $Q_A$, $d_A$ найти недостающие параметры и описать процесс передачи сообщения га пользователю *A:*

а. $P_A$ = 5, $Q_A$ = 11, $d_A$ = 3, m = 12,
б. $P_A$ = 5, $Q_A$ = 13, $d_A$ = 5, m = 20,
в. $P_A$ = 7, $Q_A$ = 11, $d_A$ = 7, m = 17,
г. $P_A$ = 7, $Q_A$ = 13, $d_A$ = 5, m = 30,
д. $P_A$ = 3, $Q_A$ = 11, $d_A$ = 3, m = 15.

26. Пользователю системы RSA с параметрами TV = 187, d = 3 передано зашифрованное сообщение *e* = 100. Расшифровать это сообщение, взломав систему RSA пользователя.
27. Сгенерируйте пару ключей с помощью чисел n = 23 и q = 47. Зашифруйте сообщение M = 21 с помощью алгоритма RSA. Дешифруйте результат шифрования.
28. Сгенерируйте пару ключей с помощью чисел n = 13 и q = 31. Подпишите сообщение M = 14 с помощью алгоритма RSA. Проверьте правильность подписи.
29. Сгенерируйте пару ключей с помощью чисел n = 17 и q = 61. Зашифруйте сообщение M = 18 с помощью алгоритма RSA. Дешифруйте результат шифрования.

## **В2. Тематика рефератов**

1. Исторические методы стеганографии.
2. История отечественной криптографии.
3. Первый блочный шифр – Lucifer.
4. Электронные водяные знаки.
5. Шифрование и аутентификация в современных беспроводных сетях связи.
6. Парольные схемы аутентификации.

7. Одноразовые пароли.
8. Протоколы с нулевым разглашением.
9. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ
10. Композиции шифров. Enigma. Шифр Хейглина
11. Атаки, которые могут быть использованы при нападении на протоколы идентификации
12. Достоинства и недостатки систем поточного шифрования по сравнению с блочными шифрами
13. Сокрытие информации средствами стеганографии, на примере графических и видео файлов
14. Ранцевые криптоситемы
15. Случайные последовательности в криптографии
16. Генераторы ПСЧ чисел и ПСП
17. Удостоверяющие центры и производители ЭЦП
18. Модели атак на алгоритмы ЭЦП
19. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94
20. Возможные атаки на алгоритм DES
21. Модификации DES
22. Назначение и структура сертификата открытого ключа
23. Роторная машина Энигма
24. Шифратор Джефферсона

**В3. Тематика презентаций**

1. Исторические методы стеганографии.
2. История отечественной криптографии.
3. Первый блочный шифр – Lucifer.
4. Электронные водяные знаки.
5. Шифрование и аутентификация в современных беспроводных сетях связи.
6. Парольные схемы аутентификации.
7. Одноразовые пароли.
8. Протоколы с нулевым разглашением.
9. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ
10. Композиции шифров. Enigma. Шифр Хейглина
11. Атаки, которые могут быть использованы при нападении на протоколы идентификации
12. Достоинства и недостатки систем поточного шифрования по сравнению с блочными шифрами
13. Сокрытие информации средствами стеганографии, на примере графических и видео файлов

14. Ранцевые криптоситемы
15. Случайные последовательности в криптографии
16. Генераторы ПСЧ чисел и ПСП
17. Удостоверяющие центры и производители ЭЦП
18. Модели атак на алгоритмы ЭЦП
19. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94
20. Возможные атаки на алгоритм DES
21. Модификации DES
22. Назначение и структура сертификата открытого ключа
23. Роторная машина Энигма
24. Шифратор Джефферсона

## Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

### С.1. Лабораторная работа

#### Лабораторные работы

1. Написать и отладить набор подпрограмму, реализующую возведение в степень по модулю ($a^x \bmod m$).
2. Написать и отладить набор подпрограмму, реализующую вычисление наибольшего общего делителя (gcd(a,b)).
3. Написать и отладить набор подпрограмму, реализующую вычисление инверсии ($x^{-1} \bmod m$).
4. Выполнить компьютерную реализацию алгоритма гаммирования.
5. Выполнить компьютерную реализацию шифра замены
6. Выполнить компьютерную реализацию шифра перестановки
7. Выполнить компьютерную реализацию протокола "Ментальный покер", самостоятельно выбрав все необходимые параметры.
8. Выполнить компьютерную реализацию протокола доказательства с нулевым знанием на основе задачи о раскраске графа, все необходимые параметры выбрать самостоятельно.
9. Выполнить компьютерную реализацию протокола доказательства с нулевым знанием на основе задачи о гамильтоновом цикле в графе, все необходимые параметры выбрать самостоятельно.
10. Выполнить компьютерную реализацию протокола "Электронные деньги", все необходимые параметры выбрать самостоятельно.
11. Выполнить компьютерную реализацию протокола Нидхама-Шредера, конкретный вид шифра с открытым ключом и все необходимые параметры выбрать самостоятельно.
12. Выполнить компьютерную реализацию алгоритма DES
13. Выполнить компьютерную реализацию алгоритма ГОСТ28147-89

14. Написать программу, реализующую систему Диффи-Хеллмана. Рекомендуемые значения параметров $p$ = 30803, $д$ = 2. Секретные ключи генерировать случайным образом.
15. Написать программу, реализующую шифр Шамира. В качестве простого модуля можно взять число $p$ = 30803. Остальные параметры генерировать случайным образом.
16. Написать программу, реализующую шифр Эль-Гамаля. Рекомендуемые значения параметров $p$ — 30803, $д$ = 2. Секретные ключи и другие параметры генерировать случайным образом.
17. Написать программу, реализующую шифр RSA для передачи секретных сообщений в адрес абонентов *A* или *B*.

## Блок Д. Задания для использования в рамках промежуточной аттестации

### Д1. Перечень контрольных вопросов

1. Стойкость криптоалгоритмов
2. Определения криптографии. Задачи и методы криптографии.
3. Классификация криптосистем.
4. Синхронные, асинхронные и самосинхронизирующиеся поточные шифры
5. Регистр сдвига с линейной обратной связью
6. Нелинейные регистры сдвига с обратной связью
7. Алгоритмы работы блочных шифров
8. Криптографические протоколы: основные принципы работы
9. Примеры реализации прикладных протоколов
10. Классификация атак на основные криптографические протоколы
11. Построение и анализ генераторов случайных чисел
12. Гаммирование и роторные машины
13. Обмен ключами с помощью симметричного шифрования
14. Обмен ключами с помощью ассиметричного шифрования
15. Формальное математическое определение криптосистемы
16. Функции, используемые в криптографических алгоритмах
17. Элементы теории чисел
18. Формальное математическое определение криптосистемы
19. Алгоритм открытого распределения ключей Диффи — Хеллмана
20. Алгоритм распределения ключей Хьюза
21. Основная схема работы алгоритма DES
22. Основная схема работы алгоритма ГОСТ 28147-89
23. Схема работы новых стандартов российских блочных шифров ("Кузнечик", "Магма")
24. Основные атаки на блочные шифры
25. Ассиметричный протокол Диффи-Хеллмана

26.Математическая модель ассиметричных шифров
27.Основная схема алгоритма RSA
28. Возможные атаки на алгоритм RSA
29. Схема Эль-Гамаля цифровой электронной подписи
30.Алгоритм электронной цифровой подписи ГОСТ Р 34.10-2012
31.Схема идентификации FFS
32.Основные направления криптоанализа
33.Классификация методов криптоанализа
34.Факторизация целых чисел (Поллард)
35.Дискретное логарифмирование

**Для проверки сформированности компетенции ПК-2.2.** Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

**Блок А. Задания репродуктивного уровня («знать»)**

**А1. Вопросы для устного опроса**

35.Функции, используемые в криптографических алгоритмах
36.Элементы теории чисел
37.Формальное математическое определение криптосистемы

**Блок В. Задания реконструктивного уровня («уметь»)**

**В1. Задачи**

1. Привести результат выражений 5, 16, 27, -4, -13, 3 + 8, 3 — 8, 3-8, 3-8-5:
   а. по модулю 10,
   б. по модулю 11.
10. Вычислить, используя быстрые алгоритмы возведения в степень, $2^8$ mod 10, $3^7$ mod 10, $7^{19}$ mod 100, $7^{57}$ mod 100.
11. Разложить на простые множители числа 108, 77, 65, 30, 159.
12. Определить, какие из пар чисел (25,12), (25,15), (13,39), (40,27) взаимно просты.
13. Найти значения функции Эйлера φ(14), φ (20).
14. Используя свойства функции Эйлера, вычислить φ *(53)*, φ (21), φ(159).
15. Используя теорему Ферма, вычислить $3^{13}$ mod 13, $5^{22}$ mod 11, $3^{17}$mod5.
16. Используя теорему Эйлера, вычислить $3^9$ mod 20, $2^{14}$ mod 21, $2^{107}$ mod 159.
17. С помощью алгоритма Евклида найти gcd(21,12), gcd(30,12), gcd(24,40), gcd(33,16).
18. С помощью обобщенного алгоритма Евклида найти значения

*x* и *y* в уравнениях

а. 21x + 12y = gcd(21,12),

б. 30x + 12y = gcd(30,12),

в. 24x + 40y = gcd(24,40),

г. 33x + 16y= gcd(33,16).

13. Вычислить $3^{-1} \bmod 7$, $5^{-1} \bmod 8$, $3^{-1} \bmod 53$, $10^{-1} \bmod 53$.
14. Выписать все простые числа, меньшие 100. Какие из них соответствуют виду $p = 2q + 1$, где $q$ также простое?

**Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)**

**С.1. Лабораторная работа**

**Лабораторные работы**

*18.* Написать и отладить набор подпрограмму, реализующую возведение в степень по модулю ($a^x \bmod m$).
*19.* Написать и отладить набор подпрограмму, реализующую вычисление наибольшего общего делителя (gcd(a,b)).
*20.* Написать и отладить набор подпрограмму, реализующую вычисление инверсии ($x^{-1} \bmod m$).

**Блок Д. Задания для использования в рамках промежуточной аттестации**

**Д1.Перечень контрольных вопросов**

36.Формальное математическое определение криптосистемы
37.Функции, используемые в криптографических алгоритмах
38.Элементы теории чисел
39.Формальное математическое определение криптосистемы

**Для проверки сформированности компетенции ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.**

**Блок А. Задания репродуктивного уровня («знать»)**

**А.1 Тестовые задания по дисциплине**

1. Шифры замены бывают:
   f) простые одноалфавитные
   g) одноконтурные полиалфавитные.
   h) многоконтурные полиалфавитные.
   i) монофонические полиалфавитные.
   j) усложненные по маршрутам

2. Криптосистемы с секретным ключом называют:
   e) Симметричными криптосистемами.
   f) Асимметричными криптосистемами.
   g) Одноключевыми криптосистемами.
   h) Двуключевыми криптосистемами.

3. Хэш-функция должна обладать следующими функциями:
   e) Устойчивость к коллизиям.
   f) Симметричность.
   g) Однонаправленность.
   h) Линейность

4. Устройство «Сцитало» является примером шифрования:
   d) Методом подстановки
   e) Методом перестановки
   f) Методом гаммирования

5. Шифры делятся на
   d) Блоковые и последовательные
   e) Блочные и поточные
   f) Потоковые и дискретные

6. К достоинствам блочных шифров относят
   d) высокую скорость шифрования
   e) дешевизну реализации
   f) похожесть процедур шифрования и расшифрования

7. Устройство «Сцитало» является примером шифрования:
   d) Методом подстановки
   e) Методом перестановки
   f) Методом гаммирования

8. Шифры делятся на
   d) Блоковые и последовательные
   e) Блочные и поточные
   f) Потоковые и дискретные

9. К достоинствам блочных шифров относят
   d) высокую скорость шифрования
   e) дешевизну реализации
   f) похожесть процедур шифрования и расшифрования

10. Преобразование открытого текста сообщения в закрытый называется:
   e) процедура шифрования;
   f) алгоритм шифрования;
   g) обеспечение аутентификации;
   h) цифровая запись.

11. Входные параметры процесса шифрования {несколько верных ответов):
   e) зашифрованный текст;
   f) ключ;
   g) открытый текст;
   h) алгоритм.

12. В чем состоит задача криптографа?
   c) взломать систему защиты
   d) обеспечить конфиденциальность и аутентификацию передаваемых сообщений

13. Наука о скрытой передаче информации путем сохранения в тайне самого факта
   d) передачи называется
   e) криптография
   f) стеганография

14. Что такое криптология?
   d) защищенная информация
   e) область доступной информации
   f) тайная область связи

15. Какой режим применяется для шифрования небольших объемов информации, размером не более одного блока или для шифрования ключей
   d) Обратная связь по шифротексту
   e) Электронная кодовая книга
   f) Сцепление блоков шифротекста

16. Какие из сервисов реализуются при использовании криптографических преобразований {несколько верных ответов):
   e) контроль целостности;
   f) аутентификация;

g) шифрование;
h) алгоритм.

17 Знание ключа позволяет:
e) использовать криптографические сервисы безопасности;
f) обеспечить аутентификацию;
g) предотвратить утечку информации;
h) выполнить обратное преобразование.

18. Что в криптографии понимается под термином «элементарное опробование»:
e) операция над двумя «-разрядными двоичными числами;
f) проверка ключа на целостность;
g) сопоставление двух паролей;
h) передача ключа по какому-либо каналу связи.

19. Чем определяется уровень надежности применяемых криптографических преобразований:
e) значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях;
f) сложностью комбинации символов, выбранных случайным образом;
g) использованием большого числа ключей для шифрования;
h) отношением количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию.

20. Ниже перечислены механизмы защиты информационных систем от несанкционированного доступа. Что здесь лишнее:
f) идентификация и аутентификация пользователей и субъектов доступа;
g) управление доступом;
h) обеспечение постоянного числа пользователей сети;
i) обеспечения целостности;
j) регистрация и учет.

21. Что называется имитовставкой:
c) это блок данных, переменной длины, который вырабатывают по определенному правилу из открытых данных с использованием ключа и затем добавляют к зашифрованным данным для обеспечения их имитозащиты;
d) это блок данных фиксированной длины, который вырабатывают по определенному правилу из открытых данных с использованием ключа и затем добавляют к зашифрованным данным для обеспечения их имитозащиты.

22. Какой алгоритм не используется при симметричном шифровании:
   e) поточное шифрование;
   f) побитовое шифрование;
   g) блочное шифрование;
   h) алгоритм Эль-Гамаля.

**А2. Вопросы для устного опроса**

1. История криптографии.
2. Основные задачи криптографии.
3. Базовые определения и принципы
4. Виды криптосистем
5. Обзор исторических шифров
6. Классификация поточных шифров
7. Регистр сдвига с линейной обратной связью
8. Нелинейные регистры сдвига с обратной связью
9. Классификация блочных шифров
10. Регистр сдвига с линейной обратной связью
11. Нелинейные регистры сдвига с обратной связью
12. Основные определения и функционал
13. Требования к протоколам
14. Параметры протоколов
15. Функции – виды протоколов
16. Регулирование протоколов
17. Классификация основных атак
18. Некоторые прикладные протоколы

## Блок В. Задания реконструктивного уровня («уметь»)

**В1. Задачи**

1. Для реализации протокола "ментальный покер" выбраны сследующие общие параметры: $p = 23$, $\alpha = 5$, $\beta = 7$, $\gamma = 14$. Кроме того, имеются следующие варианты для Алисы и Боба:
   а. $C_A = 13$, $C_B = 5$, Алиса перемешивает карты по правилу $(1,2,3) \rightarrow (3,2,1)$, Боб выбирает первое число и использует перестановку $(1,2) \rightarrow (2,1)$. Алиса выбирает второе из полученных чисел.
   б. $C_A = 7$, $C_B = 15$, Алиса перемешивает карты по правилу $(1,2,3) \rightarrow (1,3,2)$, Боб выбирает второе число использует перестановку $(1,2) \rightarrow (1,2)$. Алиса выбирает первое из полученных чисел.
   в. $C_A = 19$, $C_B = 3$, Алиса перемешивает карты по правилу $(1,2,3) \rightarrow (2,1,3)$, Боб выбирает второе число и использует перестановку $(1,2) \rightarrow (2,1)$. Алиса выбирает второе из полученных чисел.

г. $C_{А}$ = 9, $C_B$ = 7, Алиса перемешивает карты по правилу (1,2,3) → (3,2,1), Боб выбирает третье число и использует перестановку (1,2) → (1,2). Алиса выбирает второе из полученных чисел.

д. $C_{А}$ = 15, $C_B$ = 5, Алиса перемешивает карты по правилу (1,2,3) → (1,2,3), Боб выбирает первое число и использует перестановку (1,2) → (2,1)- Алиса выбирает первое из полученных чисел.

Определить, какие карты достанутся Алисе и Бобу. Какие передаваемые числа будет наблюдать Ева?

2. В системе электронных денег выбраны секретные параметры банка P = 17, Q = 7, c = 7 7 , а соответствующие им открытые параметры $N$ = 119, $d$ = 5. Сформировать электронные банкноты со следующими номерами:

а. $n$ = 11 при r = 5,

б $n$ = 99 при r = 6,

в. $n$ = 55 при $r$ = 10,

г. $n$ = 44 при $r$ = 15,

Д $n$ = 77 при $r$ = 30.

## **В2. Тематика рефератов**

25. Исторические методы стеганографии.
26. История отечественной криптографии.
27. Первый блочный шифр – Lucifer.
28. Электронные водяные знаки.
29. Шифрование и аутентификация в современных беспроводных сетях связи.
30. Парольные схемы аутентификации.
31. Одноразовые пароли.
32. Протоколы с нулевым разглашением.
33. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ
34. Композиции шифров. Enigma. Шифр Хейглина
35. Атаки, которые могут быть использованы при нападении на протоколы идентификации
36. Достоинства и недостатки систем поточного шифрования по сравнению с блочными шифрами
37. Сокрытие информации средствами стеганографии, на примере графических и видео файлов
38. Ранцевые криптоситемы

39. Случайные последовательности в криптографии
40. Генераторы ПСЧ чисел и ПСП
41. Удостоверяющие центры и производители ЭЦП
42. Модели атак на алгоритмы ЭЦП

**В3. Тематика презентаций**

25. Исторические методы стеганографии.
26. История отечественной криптографии.
27. Первый блочный шифр – Lucifer.
28. Электронные водяные знаки.
29. Шифрование и аутентификация в современных беспроводных сетях связи.
30. Парольные схемы аутентификации.
31. Одноразовые пароли.
32. Протоколы с нулевым разглашением.
33. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ
34. Композиции шифров. Enigma. Шифр Хейглина
35. Атаки, которые могут быть использованы при нападении на протоколы идентификации
36. Достоинства и недостатки систем поточного шифрования по сравнению с блочными шифрами
37. Сокрытие информации средствами стеганографии, на примере графических и видео файлов
38. Ранцевые криптоситемы
39. Случайные последовательности в криптографии
40. Генераторы ПСЧ чисел и ПСП
41. Удостоверяющие центры и производители ЭЦП
42. Модели атак на алгоритмы ЭЦП

## Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

### С.1. Лабораторная работа

**Лабораторные работы:**

1. Выполнить компьютерную реализацию алгоритма гаммирования.
2. Выполнить компьютерную реализацию шифра замены
3. Выполнить компьютерную реализацию шифра перестановки
4. Выполнить компьютерную реализацию протокола "Ментальный покер", самостоятельно выбрав все необходимые параметры.
5. Выполнить компьютерную реализацию протокола доказательства с

нулевым знанием на основе задачи о раскраске графа, все необходимые параметры выбрать самостоятельно.

6. Выполнить компьютерную реализацию протокола доказательства с нулевым знанием на основе задачи о гамильтоновом цикле в графе, все необходимые параметры выбрать самостоятельно.
7. Выполнить компьютерную реализацию протокола "Электронные деньги", все необходимые параметры выбрать самостоятельно.
8. Выполнить компьютерную реализацию протокола Нидхама-Шредера, конкретный вид шифра с открытым ключом и все необходимые параметры выбрать самостоятельно.

**Блок Д. Задания для использования в рамках промежуточной аттестации**

**Д1.Перечень контрольных вопросов**

1. Стойкость криптоалгоритмов
2. Определения криптографии. Задачи и методы криптографии.
3. Классификация криптосистем.
4. Синхронные, асинхронные и самосинхронизирующиеся поточные шифры
5. Регистр сдвига с линейной обратной связью
6. Нелинейные регистры сдвига с обратной связью
7. Алгоритмы работы блочных шифров
8. Криптографические протоколы: основные принципы работы
9. Примеры реализации прикладных протоколов
10. Классификация атак на основные криптографические протоколы
11. Построение и анализ генераторов случайных чисел
12. Гаммирование и роторные машины
13. Обмен ключами с помощью симметричного шифрования
14. Обмен ключами с помощью ассиметричного шифрования

**Для проверки сформированности компетенции ПК-2.4.** Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

**Блок А. Задания репродуктивного уровня («знать»)**

**А.1 Тестовые задания по дисциплине**

1. Алгоритм RSA основан на использовании
   e) односторонней функции
   f) односторонней функции с лазейкой
   g) надежного простого числа

h) составного числа, образованного двумя простыми числами

2. К симметричным криптосистемам относятся алгоритмы
   e) DES
   f) 3DES
   g) AES RSA
   h) TWOFISH

3. Какой из режимов алгоритма DES используется для построения шифров гаммирования?
   e) электронная кодовая книга;
   f) сцепление блоков шифра;
   g) обратная связь по шифротексту;
   h) обратная связь по выходу.

4. Какова длина блока алгоритма шифрования DES:
   e) 16 бит;
   f) 56 бит;
   g) 64 бита;
   h) 5 байт.

5. Сколько всего циклов выполняется операция зашифровывания в алгоритме DES:
   e) 10;
   f) 14;
   g) 16;
   h) 20.

6. Что является преимуществом симметричного шифрования:
   e) скорость выполнения криптографических преобразований;
   f) легкость внесения изменений в алгоритм шифрования;
   g) секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
   h) применение в системах аутентификации (электронная подпись).

7. Какой размер ключа в отечественном стандарте симметричного шифрования:
   d) 56 бит;
   e) 124 бит;
   f) 256 бит.

8. Какие из режимов шифрования данных не включает в себя отечественный стандарт симметричного шифрования:
   e) режим гаммировани;

f) режим простой замены;
g) режим обратной связи по шифротексту;
h) режим гаммирования с обратной связью.

9. Режим выработка имитовставки в стандарте шифрования ГОСТ 28147-89 гарантирует:
   d) конфиденциальность сообщения
   e) целостность сообщения
   f) аутентификацию сообщения

10. Использует ли отечественный стандарт симметричного шифрования дополнительный ключ:
   c) да;
   d) нет.

11. Какое из этих утверждений является верным:
   d) у S-блоков ГОСТ 4-битовые входы и выходы;
   e) у S-блоков ГОСТ 4-битовые входы и 8-битовые выходы;
   f) у S-блоков ГОСТ 8-битовые входы и 4-битовые выходы.

12. Используется ли в отечественном стандарте симметричного шифрования процедура генерации подключей из ключей, как в DES:
   d) да, но эта процедура сравнительно проста;
   e) не используется;
   f) используется аналогичная по сложности процедура.

13. В отечественном стандарте симметричного шифрования применяется подстановка, основанная на применении S-блоков. Сколько таких блоков используется в ГОСТ:
   e) 8;
   f) 12;
   g) 16;
   h) 24.

14. Длина раундового ключа в отечественном стандарте симметричного шифрования:
   d) 8 бит;
   e) 32 бита;
   f) 48 бит.

15. Выберите правильное утверждение:
   d) в отечественном стандарте симметричного шифрования есть начальная, но нет конечной битовых перестановок шифруемого блока;

e) в отечественном стандарте симметричного шифрования нет начальной и конечной битовых перестановок шифруемого блока, так как они не влияют на стойкость шифра;
f) в DES нет начальной и конечной битовых перестановок шифруемого блока.

16. Что означает «многократное шифрование» применительно к блочным шифрам:
e) повторное применение алгоритма шифрования к шифротексту с теми же ключами;
f) шифрование одного и того же блока открытого текста несколько раз с несколькими ключами;
g) повторное применение алгоритма шифрования к шифротексту с другими ключами;
h) увеличение числа этапов шифрования открытого текста.

**А2. Вопросы для устного опроса**

1. Основные характеристики и структура алгоритма DES.
2. Процедура расширения ключа.
3. Криптостойкость алгоритма DES.
4. Основные характеристики и структура алгоритма AES.
5. Основные схемы работы алгоритма ГОСТ 28147-89
6. Режимы работы алгоритма ГОСТ 28147-89
7. Криптостойкость алгоритма.
8. Модификации алгоритма и их анализ
9. Новый стандарт российского блочного шифра
10. Описание алгоритма Диффи-Хеллман
11. Протокол Диффи-Хеллмана
12. Математическая модель ассиметричных шифров
13. Приложения ассиметричной криптографии
14. Распределенные системы, построенные на ассиметричной криптографии
15. Основные свойства ассиметричного шифрования
16. Описание алгоритма RSA
17. Приложения RSA
18. Возможные атаки на RSA

**Блок В. Задания реконструктивного уровня («уметь»)**

**В1. Задачи**

**Задачи.**

1. Зашифровать с помощью алгоритма S-DES сообщение X = 123 на ключе K = 568. Полученное шифр-сообщение дешифровать.

| P10 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 5 | 2 | 7 | 4 | 10 | 1 | 9 | 8 | 6 |

| P8 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | 3 | 7 | 4 | 8 | 5 | 10 | 9 |

| IP | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2 | 6 | 3 | 1 | 4 | 8 | 5 | 7 |

| $IP^{-1}$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | 1 | 3 | 5 | 7 | 2 | 8 | 6 |

| E/P | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 3 | 2 | 3 | 4 | 1 |

| P4 | | | |
|---|---|---|---|
| 2 | 4 | 3 | 1 |

| S1 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 0 | 3 | 2 |
| 1 | 3 | 2 | 1 | 0 |
| 2 | 0 | 2 | 1 | 3 |
| 3 | 3 | 1 | 3 | 1 |

| S2 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 1 | 2 | 3 |
| 1 | 2 | 0 | 1 | 3 |
| 2 | 3 | 0 | 1 | 0 |
| 3 | 2 | 1 | 0 | 3 |

2. Зашифровать с помощью алгоритма S-AES сообщение X = (7 5 4 5) на ключе K = (8 6 1 e). Полученное шифр-сообщение дешифровать.

$\varphi(x) = x^4 \oplus x \oplus 1$

преобразование **Sub Half-Bytes*()**

| **x** | **Y** | | | |
|---|---|---|---|---|
| | **00** | **01** | **10** | **11** |
| **00** | 9 | e | 5 | 1 |
| **01** | 8 | b | d | a |
| **10** | 6 | 7 | f | 3 |
| **11** | c | 4 | 0 | 2 |

преобразование **ISub Half-Bytes*()**

| **x** | **Y** | | | |
|---|---|---|---|---|
| | **00** | **01** | **10** | **11** |
| **00** | e | 3 | f | B |
| **01** | d | 2 | 8 | 9 |
| **10** | 4 | 0 | 7 | 5 |
| **11** | c | 6 | 1 | a |

**Mix Columns*()**

$$\begin{bmatrix} S_{0c}' \\ S_{1c}' \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} S_{0c} \\ S_{1c} \end{bmatrix}, 0 \le c \le 1,$$

где c – номер столбца массива данных. В результате такого умножения полубайты столбца $S_{0c}$ и $S_{1c}$ заменяются соответственно на полубайты:

$$S_{0c}' = (\{3\} \bullet S_{0c}) \oplus (\{2\} \bullet S_{1c}),$$
$$S_{1c}' = (\{2\} \bullet S_{0c}) \oplus (\{3\} \bullet S_{1c}).$$

**Алгоритм выработки подключей**

$K_{00}^{r} = \text{Sub Half-Bytes*}(K_{11}^{r-1}) \oplus K_{00}^{r-1}$;
$K_{10}^{r} = \text{Sub Half-Bytes*}(K_{01}^{r-1}) \oplus K_{10}^{r-1} \oplus 2^{r-2}$;
$K_{01}^{r} = K_{00}^{r} \oplus K_{01}^{r-1}$;
$K_{11}^{r} = K_{10}^{r} \oplus K_{11}^{r-1}$,

3. Найти все допустимые варианты выбора параметра g в системе Диффи-Хеллмана при p = 11.
4. Вычислить секретные ключи $У_А$ $У_В$ и общий ключ $Z_{АВ}$ для системы Диффи-Хеллмана с параметрами:
   a. p = 23, 0 = 5, $X_А$ = Ь, $X_в$ = 7,

б. p=19, 0 = 2, $X_A$ = 5, $X_в$ = 7,
в. p = 23, 0 = 7, $X_A$ = 3, $X_в$=4,
г. p = 17, 0 = 3, $X_A$ = 10, $X_в$ = 5,
д. p = 19, 0 = 10, $X_A$ = 4, $X_в$ = 8.

5. Пусть для схемы Диффи-Хеллмана известны открытые параметры p = 59 и g = 13. Чему будет равен секретный ключ К, если Алисе известен закрытый ключ a = 1201 и Боб передал ей свой открытый ключ B = 37?
6. Пусть для схемы Диффи-Хеллмана известны открытые параметры p = 59 и g = 13. Чему будет равен секретный ключ К, если Бобу известен закрытый ключ b = 433 и Алиса передала ему свой открытый ключ A = 52?
7. Пусть для схемы Диффи-Хеллмана известны открытые параметры p = 61 и g = 17. Чему будет равен секретный ключ К, если Алисе известен закрытый ключ a = 421 и Боб передал ей свой открытый ключ B = 26?

*8.* В системе RSA с заданными параметрами $P_A$, $Q_A$, $d_A$ найти недостающие параметры и описать процесс передачи сообщения га пользователю *A:*

а. $P_A$ = 5, $Q_A$ = 11, $d_A$ = 3, m = 12,
б. $P_A$ = 5, $Q_A$ = 13, $d_A$ = 5, m = 20,
в. $P_A$ = 7, $Q_A$ = 11, $d_A$ = 7, m = 17,
г. $P_A$ = 7, $Q_A$ = 13, $d_A$ = 5, m = 30,
д. $P_A$ = 3, $Q_A$ = 11, $d_A$ = 3, m = 15.

9. Пользователю системы RSA с параметрами TV = 187, d = 3 передано зашифрованное сообщение *e* = 100. Расшифровать это сообщение, взломав систему RSA пользователя.
10. Сгенерируйте пару ключей с помощью чисел n = 23 и q = 47. Зашифруйте сообщение M = 21 с помощью алгоритма RSA. Дешифруйте результат шифрования.
11. Сгенерируйте пару ключей с помощью чисел n = 13 и q = 31. Подпишите сообщение M = 14 с помощью алгоритма RSA. Проверьте правильность подписи.
12. Сгенерируйте пару ключей с помощью чисел n = 17 и q = 61. Зашифруйте сообщение M = 18 с помощью алгоритма RSA. Дешифруйте результат шифрования.

**<u>В2. Тематика рефератов</u>**.

1. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94
2. Возможные атаки на алгоритм DES
3. Модификации DES
4. Назначение и структура сертификата открытого ключа
5. Роторная машина Энигма
6. Шифратор Джефферсона

**<u>В3. Тематика презентаций</u>**

1. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94
2. Возможные атаки на алгоритм DES
3. Модификации DES
4. Назначение и структура сертификата открытого ключа
5. Роторная машина Энигма
6. Шифратор Джефферсона

## Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

### С.1. Лабораторная работа

**1.** Выполнить компьютерную реализацию алгоритма DES
**2.** Выполнить компьютерную реализацию алгоритма ГОСТ28147-89
**3.** Написать программу, реализующую систему Диффи-Хеллмана. Рекомендуемые значения параметров $p$ = 30803, $д$ = 2. Секретные ключи генерировать случайным образом.
**4.** Написать программу, реализующую шифр Шамира. В качестве простого модуля можно взять число $p$ = 30803. Остальные параметры генерировать случайным образом.
**5.** Написать программу, реализующую шифр Эль-Гамаля. Рекомендуемые значения параметров $p$ — 30803, $д$ = 2. Секретные ключи и другие параметры генерировать случайным образом.

***6.*** Написать программу, реализующую шифр RSA для передачи секретных сообщений в адрес абонентов *A* или *B*.

## Блок Д. Задания для использования в рамках промежуточной аттестации

### Д1.Перечень контрольных вопросов

1. Алгоритм открытого распределения ключей Диффи — Хеллмана
2. Алгоритм распределения ключей Хьюза
3. Основная схема работы алгоритма DES
4. Основная схема работы алгоритма ГОСТ 28147-89
5. Схема работы новых стандартов российских блочных шифров ("Кузнечик", "Магма")
6. Основные атаки на блочные шифры
7. Ассиметричный протокол Диффи-Хеллмана
8. Математическая модель ассиметричных шифров
9. Основная схема алгоритма RSA
10. Возможные атаки на алгоритм RSA

11.Схема Эль-Гамаля цифровой электронной подписи
12.Алгоритм электронной цифровой подписи ГОСТ Р 34.10-2012
13.Схема идентификации FFS
14.Основные направления криптоанализа
15.Классификация методов криптоанализа
16.Факторизация целых чисел (Полларда)
17.Дискретное логарифмирование

## РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Балльно-рейтинговая система является базовой системой оценивания сформированности компетенций обучающихся очной формы обучения.

Итоговая оценка сформированности компетенции(й) обучающихся в рамках балльно-рейтинговой системы осуществляется в ходе текущего контроля успеваемости, промежуточной аттестации и определяется как сумма баллов, полученных обучающимися в результате прохождения всех форм контроля.

Оценка сформированности компетенции(й) по дисциплине складывается из двух составляющих:

✓ первая составляющая – оценка преподавателем сформированности компетенции(й) в течение семестра в ходе текущего контроля успеваемости (максимум 100 баллов). Структура первой составляющей определяется технологической картой дисциплины, которая в начале семестра доводится до сведения обучающихся;

✓ вторая составляющая – оценка сформированности компетенции(й) обучающихся на экзамене (максимум – 30 баллов).

Для студентов очно-заочной формы обучения применятся 4-балльная и бинарная шкалы оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся.

| **уровни освоения компетенций** | продвинутый уровень | базовый уровень | пороговый уровень | допороговый уровень |
|---|---|---|---|---|
| **100 – балльная шкала** | 85 и ≥ | 70 – 84 | 51 – 69 | 0 – 50 |
| **4 – балльная шкала** | «отлично» | «хорошо» | «удовлетворительно» | «неудовлетворительно» |

**Шкала оценок при текущем контроле успеваемости по различным показателям**

| ***Показатели оценивания сформированности компетенций*** | ***Баллы*** | ***Оценка*** |
|---|---|---|
| Устный опрос | 0-5 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |
| Подготовка реферата | 0-5 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |
| Подготовка презентации | 0-5 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |
| Решение задач | 0-10 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |
| Тестирование | 0-30 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |
| Выполнение лабораторной работы | 0-15 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |

**Соответствие критериев оценивания уровню освоения компетенций по текущему контролю успеваемости**

| ***Баллы*** | ***Оценка*** | ***Уровень освоения компетенций*** | ***Критерии оценивания*** |
|---|---|---|---|
| 0-50 | «неудовлетворительно» | Допороговый уровень | Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины |
| 51-69 | «удовлетворительно» | Пороговый уровень | Не менее 50% заданий, подлежащих текущему контролю успеваемости, выполнены без существенных ошибок |
| 70-84 | «хорошо» | Базовый уровень | Обучающимся выполнено не менее 75% заданий, подлежащих текущему контролю успеваемости, или при |

| | | | |
|---|---|---|---|
| | | | выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала и применения его при решении практических заданий; задания выполнены без ошибок |
| 85-100 | «отлично» | Продвинутый уровень | 100% заданий, подлежащих текущему контролю успеваемости, выполнены самостоятельно и в требуемом объеме; обучающийся проявляет умение обобщать, систематизировать материал и применять его при решении практических заданий; задания выполнены с подробными пояснениями и аргументированными выводами |

**Шкала оценок по промежуточной аттестации**

| ***Наименование формы промежуточной аттестации*** | ***Баллы*** | ***Оценка*** |
|---|---|---|
| Экзамен | 0-30 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |

**Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся**

| ***Баллы*** | ***Оценка*** | ***Уровень освоения компетенций*** | ***Критерии оценивания*** |
|---|---|---|---|
| 0-9 | «неудовлетворительно» | Допороговый уровень | Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы |
| 10-16 | «удовлетворительно» | Пороговый уровень | Обучающийся дал неполные ответы на вопросы, с недостаточной аргументацией, практические задания выполнены не полностью, компетенции, осваиваемые в процессе |

| | | | |
|---|---|---|---|
| | | | изучения дисциплины сформированы не в полном объеме. |
| 17-23 | «хорошо» | Базовый уровень | Обучающийся в целом приобрел знания и умения в рамках осваиваемых в процессе обучения по дисциплине компетенций; обучающийся ответил на все вопросы, точно дал определения и понятия, но затрудняется подтвердить теоретические положения практическими примерами; обучающийся показал хорошие знания по предмету, владение навыками систематизации материала и полностью выполнил практические задания |
| 25-30 | «отлично» | Продвинутый уровень | Обучающийся приобрел знания, умения и навыки в полном объеме, закрепленном рабочей программой дисциплины; терминологический аппарат использован правильно; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать, систематизировать материал и выполняет практические задания с подробными пояснениями и аргументированными выводами |

## РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций

Устный опрос проводится в первые 15 минут занятий семинарского типа в формате обсуждения с названными преподавателем студентами. Остальные обучающиеся вправе дополнить или уточнить ответ по своему желанию (соблюдаю очередность ответа). Основной темой для опроса являются вопросы для обсуждения, соответствующие теме предыдущей лекции, но преподаватель может уточнять задаваемый вопрос, задавать наводящие вопросы или сужать вопрос до отдельного аспекта обсуждаемой темы.

**Методика оценивания ответов на устные вопросы**

| ***Баллы*** | ***Оценка*** | ***Показатели*** | ***Критерии*** |
|---|---|---|---|
| 5 | «отлично» | 1. Полнота данных ответов;<br>2. Правильность ответов на вопросы. | Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, привести необходимые примеры. Изложение материала последовательно и правильно. |
| 3-4 | «хорошо» | | Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет. |
| 1-2 | «удовлетворительно» | | Студент обнаруживает знание и понимание основных положений данного задания, но:<br>1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил;<br>2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры;<br>3) излагает материал непоследовательно и допускает ошибки. |
| 0 | «неудовлетвори-тельно» | | Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. |

Тестирование проводится с помощью системы дистанционного обучения «Прометей», входящей в состав электронной информационно-образовательной среды Дагестанского государственного университета народного хозяйства.

На тестирование отводится 45 минут. Каждый вариант тестовых заданий включает 30 вопросов.

**Методика оценивания выполнения тестов**

| **Баллы** | **Оценка** | **Показатели** | **Критерии** |
|---|---|---|---|
| 25-30 | «отлично» | 1. Полнота выполнения тестовых заданий;<br>2. Своевременность выполнения;<br>3. Правильность | Выполнено более 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос |
| 19-24 | «хорошо» | | Выполнено более 70 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на |

| | | | |
|---|---|---|---|
| | | | поставленный вопрос; однако были допущены неточности в определении понятий, терминов и др. |
| 15-18 | «удовлетворительно» | ответов на вопросы. | Выполнено более 54 % заданий предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со стилистическими и орфографическими ошибками. |
| 0-14 | «неудовлетвори-тельно» | | Выполнено не более 53 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях). |

Тема реферата выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На написание реферата отводится одна неделя. Реферат оформляется согласно действующим в Дагестанском государственном университете народного хозяйства требованиям к оформлению письменных работ. Объем представленного реферата должен быть не менее 10 страниц машинописного текста без учета титульного листа.

Публичная защита реферата проводится в присутствии остальных студентов, защищающих рефераты. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель реферата, а также цельно сформулировать базовую идею, отраженную в реферате.

**Методика оценивания выполнения рефератов**

| ***Баллы*** | ***Оценка*** | ***Показатели*** | ***Критерии*** |
|---|---|---|---|
| 5 | «отлично» | 1. Полнота выполнения рефератов;<br>2. Своевременность выполнения;<br>3. Четкость изложения идеи реферата во время защиты. | Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, четкое и последовательное выступление во время защиты. |
| 3-4 | «хорошо» | | Основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в |

| | | | |
|---|---|---|---|
| | | | изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; выступление во время защиты требует дополнительных вопросов. |
| 1-2 | «удовлетворительно» | | Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы во время выступления. |
| 0 | «неудовлетвори-тельно» | | Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы, не проведена защита реферата. |

Тема презентации выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На подготовку презентации отводится одна неделя.

Публичная презентация проводится в присутствии остальных студентов. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель презентации, а также цельно сформулировать базовую идею.

**Методика оценивания выполнения презентаций**

| ***Баллы*** | ***Оценка*** | ***Показатели*** | ***Критерии*** |
|---|---|---|---|
| 5 | «отлично» | 4. Полнота выполнения;<br>5. Своевременность выполнения;<br>6. Четкость изложения идеи презентации во время защиты. | Выполнены все требования к подготовке презентации: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, четкое и последовательное выступление во время демонстрации. |
| 3-4 | «хорошо» | | Основные требования к подготовке презентации выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем презентации; имеются упущения в оформлении; выступление во время демонстрации требует |

| | | | |
|---|---|---|---|
| | | | дополнительных вопросов. |
| 1-2 | «удовлетворительно» | | Имеются существенные отступления от требований к презентации. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании презентации или при ответе на дополнительные вопросы во время выступления. |
| 0 | «неудовлетвори-тельно» | | Тема презентации не раскрыта, обнаруживается существенное непонимание проблемы, не проведена демонстрация презентации. |

Задачи выполняются непосредственно во время занятий семинарского типа (одно задание на одну пару согласно текущей тематике занятия). Студенты должны выполнять задачи самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности представленного решения. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения задания, то это негативно отражается на оценке выполняющего задание студента.

**Методика оценивания выполнения задач**

| ***Баллы*** | ***Оценка*** | ***Показатели*** | ***Критерии*** |
|---|---|---|---|
| 9-10 | «отлично» | 1. Полнота выполнения задачи;<br>2. Своевременность выполнения задачи;<br>3. Самостоятельность решения. | Основные требования к выполнению задания выполнены. Продемонстрировано умение анализировать ситуацию и находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для достижения поставленной цели |
| 6-8 | «хорошо» | | Основные требования к выполнению задания реализованы, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений |
| 3-5 | «удовлетворительно» | | Имеются существенные отступления от выполнения работы. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат |
| 1-2 | «неудовле | | Задача не нешена, обнаруживается |

| | | | |
|---|---|---|---|
| | твори-тельно» | | существенное непонимание проблемы |

Лабораторные работы выполняются в специализированной аудитории во время лабораторных занятий. Предусмотрено выполнение одной лабораторной работы в течение одного занятия согласно текущей тематике. Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности полученного результата. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения шагов лабораторной работы, то это негативно отражается на оценке выполняющего задание студента.

**Методика оценивания выполнения *лабораторных работ***

| ***Баллы*** | ***Оценка*** | ***Показатели*** | ***Критерии*** |
|---|---|---|---|
| 13-15 | «отлично» | 4. Полнота выполнения задания лабораторной работы;<br>5. Своевременность выполнения задания лабораторной работы;<br>6. Самостоятельность решения. | Основные требования к выполнению задания лабораторной работы выполнены. Продемонстрировано умение анализировать ситуацию и находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для достижения поставленной цели |
| 9-12 | «хорошо» | | Основные требования к выполнению задания лабораторной работы реализованы, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений |
| 5-8 | «удовлетворительно» | | Имеются существенные отступления от выполнения лабораторной работы. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат |
| 0-4 | «неудовлетвори-тельно» | | Шаги выполнения лабораторной работы не выполнены, обнаруживается существенное непонимание проблемы. |

Время подготовки ответа при сдаче экзамена в устной форме должно составлять не менее 40 минут (по желанию обучающегося ответ может быть досрочным). Время ответа – не более 15 минут.

При подготовке к устному экзамену экзаменуемый, как правило, ведет записи в листе устного ответа, который затем (по окончании экзамена) сдается экзаменатору.

Экзаменатору предоставляется право задавать обучающимся дополнительные вопросы в рамках программы дисциплины текущего семестра, а также, помимо теоретических вопросов, давать задачи, которые изучались на практических занятиях.

Оценка результатов устного аттестационного испытания объявляется обучающимся в день его проведения.

**Лист актуализации оценочных материалов по дисциплине**

«Криптографические средства защиты информации»

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____20___г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____20___г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____20___г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____20___г. №_____

Зав. кафедрой _____