ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

Утвержден решением
Ученого совета ДГУНХ,
протокол № 11
от 30 мая 2024 г

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО МЕЖДИСЦИПЛИНАРНОМУ КУРСУ

«КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

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

Форма обучения – очная

Махачкала – 2024

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 междисциплинарному курсу «Криптографические средства защиты информации» размещены на официальном сайте www.dgunh.ru

Гасанова З.А. Фонд оценочных средств по междисциплинарному курсу «Криптографические средства защиты информации» по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. – Махачкала: ДГУНХ, 2024 г. – 47 с.

Рекомендован к утверждению Учебно-методическим советом ДГУНХ 28 мая 2024 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» 23 мая 2024 г., протокол № 10.

.

СОДЕРЖАНИЕ

Назначение оценочных материалов……..4

РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины …..……..5

1.1 Перечень формируемых компетенций……5

1.2 Перечень компетенций с указанием видов оценочных средств …….5

РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине……..12

РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания…….....37

РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций……41

Лист актуализации оценочных материалов по дисциплине…….47

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:** – основные задачи и понятия криптографии; – 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 — тестовые задания; - 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;	
	<u>Уметь:</u> - 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 – задачи; - тематика рефератов; - 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	
	<u>Владеть:</u>	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 – 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.	**Знать:** – принципы построения криптографических алгоритмов. – принципы построения ЭЦП	Пороговый уровень	Обучающийся слабо (частично) знает принципы построения криптографических алгоритмов и построения ЭЦП	**Блок А –** задания репродуктивного уровня — тестовые задания; - 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	
	Уметь: – использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки; – 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 – задачи; - тематика рефератов; - 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	
	Владеть: – криптографической терминологией – 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 – 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:** – 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 — тестовые задания; - 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: – применять средства ЭЦП	Пороговый уровень	Обучающийся слабо (частично) умеет применять средства ЭЦП	**Блок В** – задания реконструктивного уровня – задачи; - тематика рефератов; - 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: – навыками программирования криптографических алгоритмов.	Пороговый уровень	Обучающийся слабо (частично) владеет навыками программирования криптографических алгоритмов.	**Блок С** – задания практико-ориентированного уровня – 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. Прочтите текст задания и выберите один верный ответ

Что необходимо сделать перед установкой программного средства криптозащиты на рабочую станцию?

Варианты ответов:

а. Удалить все антивирусные программы
б. Подключить устройство к интернету без брандмауэра
в. Проверить совместимость с операционной системой
г. Отключить экран монитора

2. Прочтите текст задания и выберите один верный ответ

Какой стандарт используется для форматирования сертификатов электронной подписи в России?

Варианты ответов:

а. X.509
б. ГОСТ Р 34.10-2012
в. RSA-2048
г. SHA-1

3. Прочтите текст задания и выберите один верный ответ

Какой тип устройства относится к программно-аппаратным средствам защиты информации?

Варианты ответов:

а. Антивирусная программа
б. USB-токен
в. Блокнот для записей
г. Принтер

4. Прочтите текст задания и выберите один верный ответ

Какова основная цель использования драйверов при установке СКЗИ?

Варианты ответов:

а. Увеличение скорости интернета

б. Обеспечение взаимодействия между аппаратным криптосредством и ОС
в. Шифрование всех папок пользователя
г. Автоматическое обновление офисных приложений

5. Прочтите текст задания и выберите один верный ответ
Что такое "регистрация носителя" при работе со СКЗИ?
Варианты ответов:
а. Запись названия флешки в реестре
б. Процесс инициализации и привязки криптографического носителя к пользователю и системе
в. Создание резервной копии данных на внешний диск
г. Настройка ярлыков на рабочем столе

6. Прочтите текст задания и выберите один верный ответ
Какой из следующих действий повышает безопасность при использовании USB-токена?
Варианты ответов:
а. Оставлять токен подключённым постоянно
б. Использовать простой PIN-код
в. Настроить блокировку токена после нескольких неудачных попыток ввода PIN
г. Делиться PIN-кодом с коллегами

7. Прочтите текст задания и выберите один верный ответ
Какой документ требуется для легального использования СКЗИ в организации?
Варианты ответов:
а. Паспорт сотрудника
б. Лицензионное соглашение или сертификат ФСБ
в. Договор аренды сервера
г. Чек из магазина

8. Прочтите текст задания и выберите один верный ответ
8 Что означает термин "инициализация токена"?
Варианты ответов:
а. Форматирование токена как обычного накопителя
б. Настройка начальных параметров: PIN, административный ключ, установка провайдера
в. Подключение токена к интернету
г. Установка драйверов видеокарты

9. Прочтите текст задания и выберите один верный ответ

Какой из ниже перечисленных этапов следует выполнить первым при настройке СКЗИ?

Варианты ответов:

а. Генерация ключей электронной подписи
б. Установка драйверов и криптопровайдера
в. Шифрование всей файловой системы
г. Настройка облачного хранилища

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. Тестовые задания

Прочтите текст задания и установите соответствие

Установите соответствие между протоколами и их основным назначением:

1. SSL/TLS	а. Защита электронной почты и файлов
2. IPsec	б. Аутентификация в распределенных системах
3. PGP	в. Защита данных на сетевом уровне
4. Kerberos	г. Защита данных на транспортном уровне

Прочтите текст задания и установите соответствие

Установите соответствие между элементами инфраструктуры открытых ключей (PKI) и их функциями:

1. CA (Certification Authority)	а. Проверка статуса сертификата в режиме реального времени
2. RA (Registration Authority)	б. Выпуск и подписание цифровых сертификатов
3. CRL (Certificate Revocation List)	в. Список отозванных сертификатов
4. OCSP (Online Certificate Status Protocol)	г. Проверка идентификационных данных пользователей

Прочтите текст задания и установите соответствие

Установите соответствие между криптографическими протоколами и их уровнем модели OSI/TCP-IP:

1. TLS (Transport Layer Security)	а. Прикладной уровень (End-to-end encryption сообщений)
2. IPsec (Internet Protocol Security)	б. Сетевой уровень (Защита IP-пакетов)
3. PGP (Pretty Good Privacy)	в. Транспортный уровень (Защита TCP/UDP)
4. SSH (Secure Shell)	г. Прикладной уровень (Удаленное управление и туннелирование)

Прочтите текст задания и установите соответствие

Установите соответствие между режимами работы блочных шифров и их функциональными свойствами:

1. ECB (Electronic Codebook)	а. Режим обратной связи по шифртексту, позволяет использовать блочный шифр как самосинхронизирующийся поточный шифр
2. CBC (Cipher Block Chaining)	б. Режим сцепления блоков шифртекста, требующий вектора инициализации и обеспечивающий распространение ошибок
3. CTR (Counter)	в. Простейший режим, при котором одинаковые блоки открытого текста дают одинаковые блоки шифртекста
4. CFB (Cipher Feedback)	г. Режим гаммирования на основе счетчика, преобразующий блочный шифр в поточный, допускающий параллельное шифрование

B2. 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.
2. Вычислить, используя быстрые алгоритмы возведения в степень, 2^8 mod 10, 3^7 mod 10, 7^{19} mod 100, 7^{57} mod 100.
3. Разложить на простые множители числа 108, 77, 65, 30, 159.
4. Определить, какие из пар чисел (25,12), (25,15), (13,39), (40,27) взаимно просты.
5. Найти значения функции Эйлера φ(14), φ (20).
6. Используя свойства функции Эйлера, вычислить φ *(53)*, φ (21), φ(159).
7. Используя теорему Ферма, вычислить 3^{13} mod 13, 5^{22} mod 11, 3^{17}mod5.
8. Используя теорему Эйлера, вычислить 3^9 mod 20, 2^{14} mod 21, 2^{107} mod 159.
9. С помощью алгоритма Евклида найти gcd(21,12), gcd(30,12), gcd(24,40), gcd(33,16).

10. 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 $(1,2,3) \rightarrow (3,2,1)$, 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. $C_A = 9$, $C_B = 7$, Алиса перемешивает карты по правилу $(1,2,3) \rightarrow (3,2,1)$, Боб выбирает третье число и использует перестановку $(1,2) \rightarrow (1,2)$. Алиса выбирает второе из полученных чисел.
    д. $C_A = 15$, $C_B = 5$, Алиса перемешивает карты по правилу $(1,2,3) \rightarrow (1,2,3)$, Боб выбирает первое число и использует перестановку $(1,2) \rightarrow (2,1)$- 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 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

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

20. Найти все допустимые варианты выбора параметра g в системе Диффи-Хеллмана при p = 11.
21. Вычислить секретные ключи Y_A Y_B и общий ключ Z_{AB} для системы Диффи-Хеллмана с параметрами:
    a. p = 23, 0 = 5, X_A = 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, $X_A = 4$, $X_в = 8$.

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.

В3. Тематика рефератов

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

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

В4. 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»)

С1. Тестовые задания

Прочтите текст и вставьте пропущенное слово.
Криптографическое преобразование информации, позволяющее одновременно удостоверить целостность и авторство документа, называется _____ подписью.

Прочтите текст и вставьте пропущенное слово.
Совокупность аппаратных, программных и организационных средств для управления жизненным циклом сертификатов открытых ключей называется инфраструктурой _____ ключей (PKI).

Прочтите текст и вставьте пропущенное слово.
Для безопасного хранения криптографических ключей и выполнения криптографических операций в защищенной среде используется аппаратный _____ безопасности (HSM).

С.2. 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. Тестовые задания

1. Прочтите текст задания и выберите один верный ответ

Какова основная цель криптографии?

Варианты ответов:

а. Замедление работы компьютерных систем.
б. Увеличение скорости передачи данных.
в. Защита информации от несанкционированного доступа, изменения или раскрытия.
г. Создание резервных копий данных.

2. Прочтите текст задания и выберите один верный ответ

Какой из следующих принципов безопасности обеспечивает хэш-функция?

Варианты ответов:

а. Конфиденциальность.
б. Доступность.
в. Целостность.
г. Неотказуемость.

3. Прочтите текст задания и выберите один верный ответ

Какой алгоритм является примером симметричного шифрования?

Варианты ответов:

а. RSA.
б. Диффи-Хеллман.
в. AES.
г. ECC.

4. Прочтите текст задания и выберите один верный ответ

В чем заключается ключевое отличие асимметричной криптографии от симметричной?

Варианты ответов:

а. Асимметричная криптография использует один и тот же ключ для шифрования и дешифрования.
б. Асимметричная криптография использует два разных, математически связанных ключа (открытый и закрытый).
в. Асимметричная криптография всегда быстрее симметричной.
г. Асимметричная криптография не может быть использована для цифровых подписей.

5. Прочтите текст задания и выберите один верный ответ

Что в криптографии называется "ключом"?

Варианты ответов:

а. Имя алгоритма шифрования.
б. Программа, используемая для выполнения криптографических операций.
в. Параметр, используемый криптографическим алгоритмом для преобразования данных.
г. Идентификатор пользователя в системе.

6. Прочтите текст задания и выберите один верный ответ

Для чего в основном используется алгоритм Диффи-Хеллмана?

Варианты ответов:

а. Для создания цифровых подписей.
б. Для обмена секретными ключами по незащищенному каналу.
в. Для шифрования больших объемов данных.

г. Для проверки целостности файлов.

7. Прочтите текст задания и выберите один верный ответ

Какой из видов атак заключается в систематическом переборе всех возможных значений ключа до тех пор, пока не будет найден правильный?

Варианты ответов:

а. Атака по словарю.
б. Атака "человек посередине" (Man-in-the-Middle).
в. Атака грубой силы (Brute-force).
г. Атака по известному открытому тексту.

8. Прочтите текст задания и выберите один верный ответ

Что такое Цифровая Подпись?

Варианты ответов:

а. Электронный аналог рукописной подписи, используемый для идентификации автора сообщения.
б. Криптографический механизм, обеспечивающий целостность сообщения и неотказуемость отправителя от факта его отправки.
в. Тип шифрования, предназначенный для коротких сообщений.
г. Метод сжатия данных перед их передачей.

9. Прочтите текст задания и выберите один верный ответ

Какая из перечисленных характеристик относится к блочным шифрам?

Варианты ответов:

а. Обрабатывают данные по одному биту за раз.
б. Делят сообщение на блоки фиксированного размера и шифруют каждый блок.
в. В основном используются для генерации случайных чисел.
г. Имеют более низкую скорость работы по сравнению с потоковыми шифрами.

А2. Вопросы для устного опроса

1. Функции, используемые в криптографических алгоритмах
2. Элементы теории чисел
3. Формальное математическое определение криптосистемы

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тестовые задания

Прочтите текст задания и установите соответствие

Установите соответствие между криптографическими алгоритмами и их длиной ключа:

1. AES-256	а. 168 бит
2. RSA (минимальная рекомендуемая длина)	б. 256 бит
3. 3DES	в. 2048 бит
4. Blowfish (максимальная)	г. 448 бит

Прочтите текст задания и установите соответствие

Установите соответствие между блочными шифрами и размером их блока в битах:

а. AES (Advanced Encryption Standard)	128 бит
б. DES (Data Encryption Standard)	64 бита
в. RC5 (базовый вариант)	32 бита
г. Blowfish	Переменная (до 2048 бит)

Прочтите текст задания и установите соответствие

Установите соответствие между российскими стандартами криптографии и их полным назначением:

ГОСТ Р 34.10-2012	Функция хеширования (Стрибог)
ГОСТ Р 34.11-2012	Блочный шифр (Магма и Кузнечик)
ГОСТ 28147-89	Процесс формирования и проверки электронной цифровой подписи
ГОСТ Р 34.12-2015	Системы обработки информации. Защита криптографическая. (Блочный шифр)

Прочтите текст задания и установите соответствие

Установите соответствие между криптографическими стандартами и странами/организациями их разработки:

1. ГОСТ 28147-89	а. Япония
2. DES	б. СССР/Россия
3. Camellia	в. Европейский союз
4. PRESENT	г. США

В2. 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.

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

С1. Тестовые задания

Прочтите текст задания и выберите один верный ответ

Сообщение зашифровано шифром Цезаря. Известно, что в английском языке буква 'E' является наиболее частотной (встречается примерно в 12.7% случаев). При анализе шифртекста длиной 500 символов обнаружено, что наиболее частотной является буква 'K', которая встречается 61 раз. Каков наиболее вероятный ключ сдвига, использованный при шифровании?

Варианты ответов:

а. 3
б. 6
в. 9
г. 11

Прочтите текст задания и выберите один верный ответ

Открытый текст "CRYPTO" шифруется шифром Виженера с ключом "KEY". Используется стандартный английский алфавит из 26 букв, где A=0, B=1, ..., Z=25. Шифрование выполняется по формуле: C = (P + K) mod 26.

Какой будет шифртекст?

Варианты ответов:

а. MBSDFG
б. MXSZDY
в. CTAVZE
г. MAIZFE

Прочтите текст и вставьте пропущенное слово.

В _____ криптографии для шифрования и расшифрования данных используется один и тот же секретный ключ.

Действующим в России стандартом алгоритма блочного шифрования является ГОСТ Р 34.12-2015, также известный как «_____».

С.2. 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-2.4.**:** Осуществлять обработку, хранение и передачу информации ограниченного доступа

Блок А. Задания репродуктивного уровня («знать»)

А.1 Тестовые задания по дисциплине

1. Прочтите текст задания и выберите один верный ответ

Какой алгоритм симметричного шифрования установлен в качестве основного в актуальных российских нормативных документах ФСБ России для защиты информации ограниченного доступа (не содержащей гостайну)?
Варианты ответов:

а. AES-256
б. Кузнечик
в. Магма
г. Camellia

2. Прочтите текст задания и выберите один верный ответ
Какой алгоритм хеш-функции установлен в национальном стандарте РФ для использования в системах электронной подписи и защиты информации ограниченного доступа?
Варианты ответов:

а. SHA-256
б. Стрибог
в. Whirlpool
г. BLAKE2

3. Прочтите текст задания и выберите один верный ответ
Какой протокол рекомендуется ФСТЭК России для криптографической защиты каналов передачи информации ограниченного доступа в автоматизированных системах класса 1Г–4?
Варианты ответов:

а. SSL 3.0
б. TLS 1.3 с российскими криптографическими алгоритмами (по RFC 9150, RFC 9189)
в. IPsec в режиме ESP с AES-GCM
г. OpenVPN с RSA

4. Прочтите текст задания и выберите один верный ответ
Какой класс средств криптографической защиты информации (СКЗИ) требуется для защиты информации ограниченного доступа, обрабатываемой в государственных информационных системах 1 уровня значимости?
Варианты ответов:

а. КС1
б. КС2
в. КС3
г. КЦ1

5. Прочтите текст задания и выберите один верный ответ
Какой способ хранения ключевой информации является обязательным при использовании сертифицированных ФСБ СКЗИ для обработки информации ограниченного доступа?

Варианты ответов:

а. Хранение в реестре Windows
б. Хранение в файле на рабочем столе
в. Хранение в неизвлекаемой форме на носителе, сертифицированном по требованиям безопасности информации
г. Хранение в облачном сервисе

6. Прочтите текст задания и выберите один верный ответ

Какое требование предъявляется к обработке информации ограниченного доступа в соответствии с приказом ФСТЭК № 17 при использовании средств шифрования?

Варианты ответов:

а. Допускается временное расшифрование в оперативной памяти без контроля
б. Запрещается расшифрование информации в общесистемных временных файлах и на незащищённых носителях
в. Разрешено сохранять расшифрованные данные в профиле пользователя
г. Допустимо использование подкачки (swap) для расшифрованных данных

7. Прочтите текст задания и выберите один верный ответ

Какое действие обязательно при уничтожении носителя, содержащего информацию ограниченного доступа, зашифрованную сертифицированным СКЗИ?

Варианты ответов:

а. Простое форматирование
б. Удаление файлов и очистка корзины
в. Надёжное уничтожение ключевой информации (носителя ключей) с составлением акта
г. Перезапись нулями один раз

8. Прочтите текст задания и выберите один верный ответ

Для чего в первую очередь предназначена Инфраструктура Открытых Ключей (PKI)?

Варианты ответов:

а. Для шифрования всего сетевого трафика в организации.
б. Для управления цифровыми сертификатами и ключами, обеспечивая доверие в асимметричных криптосистемах.
в. Для создания распределенных баз данных.
г. Для физической защиты серверов.

9. Прочтите текст задания и выберите один верный ответ

Какой из принципов криптографической защиты гарантирует, что отправитель не сможет впоследствии отказаться от факта отправки сообщения?

Варианты ответов:

а. Конфиденциальность.
б. Целостность.

в. Доступность.
г. Неотказуемость

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»)

В.1 Тестовые задания

Прочтите текст задания и установите соответствие

Установите соответствие между типами атак на криптосистемы и их описанием:

1. Атака на основе подобранного открытого текста	а. Использование физических характеристик реализации (время, энергопотребление)
2. Атака на основе подобранного шифртекста	б. Атакующий может выбирать шифртексты для расшифрования
3. Атака по сторонним каналам	в. Применяется против каскадных шифров с использованием двух направлений
4. Атака «встреча посередине»	г. Атакующий может выбирать открытые тексты для шифрования

Прочтите текст задания и установите соответствие

Установите соответствие между криптографическими хеш-функциями и размером их выходного значения:

1. MD5	а. 160 бит
2. SHA-1	б. 512 бит
3. SHA-256	в. 128 бит
4. SHA-512	г. 256 бит

Прочтите текст задания и установите соответствие

Установите соответствие между алгоритмами асимметричной криптографии и математическими задачами, лежащими в их основе:

1. RSA	а. Задача дискретного логарифмирования в конечном поле
2. Эль-Гамаль (ElGamal)	б. Задача факторизации больших целых чисел
3. Эллиптическая криптография (ECC/ECDH)	в. Задача укладки рюкзака (задача о сумме подмножеств)
4. Рюкзачная криптосистема (Меркла-Хеллмана)	г. Задача дискретного логарифмирования в группе точек эллиптической кривой

Прочтите текст задания и установите соответствие

Установите соответствие между криптографическими примитивами и их классификацией:

1. RC4	а. Протокол согласования ключей
2. Diffie-Hellman	б. Асимметричный алгоритм шифрования
3. HMAC	в. Код аутентификации сообщения
4. RSA	г. Поточный шифр

В2. 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:
   a. $C_A = 13$, $C_B = 5$, 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. $C_{А}$ = 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. $C_{А}$ = 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. $C_{А}$ = 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 , a 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.

В3. Тематика рефератов

27. Исторические методы стеганографии.
28. История отечественной криптографии.
29. Первый блочный шифр – Lucifer.
30. Электронные водяные знаки.
31. Шифрование и аутентификация в современных беспроводных сетях связи.
32. Парольные схемы аутентификации.
33. Одноразовые пароли.
34. Протоколы с нулевым разглашением.
35. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ
36. Композиции шифров. Enigma. Шифр Хейглина

37. Атаки, которые могут быть использованы при нападении на протоколы идентификации
38. Достоинства и недостатки систем поточного шифрования по сравнению с блочными шифрами
39. Сокрытие информации средствами стеганографии, на примере графических и видео файлов
40. Ранцевые криптоситемы
41. Случайные последовательности в криптографии
42. Генераторы ПСЧ чисел и ПСП
43. Удостоверяющие центры и производители ЭЦП
44. Модели атак на алгоритмы ЭЦП

В4. 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 Тестовые задания

Прочтите текст и вставьте пропущенное слово.
Для проверки целостности данных без возможности их восстановления из результата используется функция _____.

Прочтите текст и вставьте пропущенное слово.
В асимметричных криптосистемах для шифрования используется открытый ключ, а для расшифрования — соответствующий ему _____ ключ.

Прочтите текст и вставьте пропущенное слово.
Цифровой документ, который связывает открытый ключ с определённым субъектом и подписан удостоверяющим центром, называется _____ открытого ключа.

Прочтите текст и вставьте пропущенное слово.
Свойство системы, не позволяющее пользователю отказаться от факта совершения определённых действий (например, отправки сообщения), называется _____.

Прочтите текст и вставьте пропущенное слово.
Основным свойством безопасности информации, обеспечиваемым процедурой шифрования, является её _____.

С.2. 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

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» «удовлетворительно» «хорошо» «отлично»
Подготовка реферата	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Подготовка презентации	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Решение задач	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Тестирование	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение лабораторной работы	0-15	«неудовлетворительно» «удовлетворительно» «хорошо» «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» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся

Баллы	*Оценка*	*Уровень*	*Критерии оценивания*

		освоения компетенций	
0-9	«неудовлетвори тельно»	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	«удовлетворите льно»	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; 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: 1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 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; 2. Своевременность выполнения; 3. Правильность ответов на вопросы.	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»		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; 2. Своевременность выполнения; 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; 5. Своевременность выполнения;	Выполнены все требования к подготовке презентации: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на

		6. Четкость изложения идеи презентации во время защиты.	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; 2. Своевременность выполнения задачи; 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	«неудовлетвори-тельно»		Задача не нешена, обнаруживается 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; 5. Своевременность выполнения задания лабораторной работы; 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	«неудовле твори-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 _____