ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

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

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПО ДИСЦИПЛИНЕ «КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»

НАПРАВЛЕНИЕ ПОДГОТОВКИ 10.03.01
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПРОФИЛЬ
«БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Уровень высшего образования - бакалавриат

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0D8142F19CA901112FC315F43B93C341
Владелец: Бучаев Ахмед Гамидович
Действителен: с 19.05.2022 до 12.08.2023

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.

Оценочные материалы по дисциплине «Криптографические протоколы» разработаны в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г., № 1427, в соответствии с приказом Министерства науки и высшего образования Российской Федерации от 6.04.2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

Оценочные материалы по дисциплине «Криптографические протоколы» размещены на официальном сайте www.dgunh.ru

Гасанова З.А. Оценочные материалы по дисциплине «Криптографические протоколы» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2023 г. – 27 с.

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

Рекомендованы к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

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

СОДЕРЖАНИЕ

Назначение оценочных материалов

Оценочные материалы для текущего контроля успеваемости (оценивания хода освоения дисциплин), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по дисциплине) обучающихся по дисциплине «Криптографические протоколы» на соответствие их учебных достижений поэтапным требованиям образовательной программы высшего образования 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем»

Оценочные материалы по дисциплине «Криптографические протоколы» 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.

Оценочные материалы 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	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-1	Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей

1.2. Перечень компетенций с указанием видов оценочных средств

Формируемые компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций***	***Уровни освоения компетенций***	***Критерии оценивания сформированности компетенций***	***Виды оценочных средств***
ПК-1. Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем	ИПК-1.4. Использует криптографическое методы защиты информации в автоматизированных системах	**Знать:** – прикладные криптографические протоколы, применяемые в автоматизированных системах.	Пороговый уровень	Обучающийся слабо (частично) знает прикладные криптографические протоколы, применяемые в автоматизированных системах.	**Блок А –** задания репродуктивного уровня — тестовые задания; - вопросы для устного опроса
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает прикладные криптографические протоколы, применяемые в автоматизированных системах.	

Формируемые компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций***	***Уровни освоения компетенций***	***Критерии оценивания сформированности компетенций***	***Виды оценочных средств***
управления базами данных и компьютерных сетей			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает прикладные криптографические протоколы, применяемые в автоматизированных системах.	
		<u>Уметь:</u> - осуществлять выбор стандартизированных криптографических протоколов применительно к конкретным требованиям по безопасности информации.	Пороговый уровень	Обучающийся слабо (частично) умеет осуществлять выбор стандартизированных криптографических протоколов применительно к конкретным требованиям по безопасности информации.	**Блок В** – задания реконструктивного уровня – задачи; - тематика рефератов; - тематика презентаций.
			Базовый уровень	Обучающийся с незначительными затруднениями умеет осуществлять выбор стандартизированных криптографических протоколов	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				применительно к конкретным требованиям по безопасности информации.	
			Продвинутый уровень	Обучающийся умеет осуществлять выбор стандартизированных криптографических протоколов применительно к конкретным требованиям по безопасности информации.	
		Владеть: - навыками применения стандартизированных криптографических протоколов в подсистемах безопасности автоматизированных системах.	Пороговый уровень	Обучающийся слабо (частично) владеет навыками применения стандартизированных криптографических протоколов в подсистемах безопасности автоматизированных системах	**Блок С** – задания практико-ориентированного уровня – практические задания.
			Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками применения стандартизирова	

Формируемые компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций***	***Уровни освоения компетенций***	***Критерии оценивания сформированности компетенций***	***Виды оценочных средств***
				нных криптографических протоколов в подсистемах безопасности автоматизированных системах	
			Продвинутый уровень	Обучающийся свободно владеет навыками применения стандартизированных криптографических протоколов в подсистемах безопасности автоматизированных системах	

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

Для проверки сформированности компетенции ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
ИОПК-9.1. Использует типовые криптографические средства защиты информации, в том числе средства электронной подписи
Блок А. Задания репродуктивного уровня («знать»)

А.1 Тестовые задания по дисциплине

1. Протокол, обеспечивающий поддержку функций безопасности с применением криптографических методов защиты информации, называется
- криптографический протокол
- протокол передачи данных
- протокол обеспечения безопасности

2 Для обеспечения свойств защищаемой информации в протоколах
- применяются модели угроз
- политики безопасности
- функции безопасности

3 Методами защиты криптографических протоколов от атак повтора являются
- нумерация сообщений, метки времени, шифрование
- нумерация сообщений, метки времени, нонсы
- нумерация сообщений, метки времени, нонсы, хэш-функции

4 Недостатком метода нумерации сообщений как метода защиты от атак повтора является…
- непредсказуемость их значений
- цикличность их значений
- непредсказуемость их значений
- необходимость синхронизации времени всех пользователей в сети

5 Примитивный криптографический протокол предназначен для …
- использования в виде базового компонента при построении прикладных
- криптографических протоколов
- решения практических задач обеспечения функций безопасности с помощью криптографических систем

- аутентификации и идентификации пользователей криптографической системы

6 Криптографический протокол, предназначенный для решения практических задач обеспечения функций безопасности с помощью криптографических систем, называется

- примитивный
- распределенный
- прикладной

7 Какой криптографический механизм используется для обеспечения целостности передаваемых сообщений

- вычисление кода аутентификации сообщения от зашифрованных полей сообщения
- шифрование передаваемого сообщения на основе симметричной схемы шифрования
- вычисление кода аутентификации сообщения от всех полей сообщения

8 Какой криптографический механизм используется для обеспечения свойства неотказуемости при передаче сообщений

- шифрование симметричным алгоритмом
- электронная подпись
- вычисление кода аутентификации сообщения

9 Если в процессе выполнения протокола нарушено хотя бы одно свойство безопасности, то …

- протокол должен предусматривать возможность выбора участниками дальнейших действий
- протокол должен завершаться с ошибкой протокол должен выполняться дальше

10 Если для обеспечения целостности сообщения применяется хэш-функция, то она должна вычисляться …

- от всего сообщения
- только от полей сообщения, содержащих зашифрованную информацию
- только от нонсов

11 Протоколы, которые позволяют выработать общий секретный ключ, не передавая его по каналу связи, называются

- протоколы явного обмена ключами
- протоколы взаимного обмена ключами
- протоколы неявного обмена ключами

12 Протоколы, в которых ключ в явном виде передается по каналу связи, называются

- протоколы неявного обмена ключами
- протоколы слепой подписи
- протоколы явного обмена ключами

13 Специфическим свойством протоколов электронных платежных систем является

- целостность
- неотслеживаемость
- конфиденциальность

14 Неотслеживаемость обеспечивается с помощью механизма…

- кодов аутентификации сообщений
- слепой подписи шифрования

15 Протоколы аутентификации участника информационного обмена предназначены …

- для подтверждения источника информации в любой момент времени.
- для подтверждения участника протокола на время сеанса связи.
- для подтверждения принимающего информация субъекта системы.

16 Цифровой документ, который связывает открытый ключ с его владельцем, называется

- сертификат открытого ключа
- сертификат ключа формирования электронной подписи
- сертификат безопасности

17. Для обеспечения конфиденциальности в протоколе ESP применяется

- шифрование на основе асимметричных схем шифрования
- шифрование на основе симметричных схем шифрования
- электронная подпись

18. В протоколах аутентификации без знания взаимных секретов…

- проверяющий знает конфиденциальную информацию доказывающего.
- доказывающий убеждает проверяющего в подлинности заявленного им имени без предъявления своих секретов.
- проверяющий не знает конфиденциальную информацию доказывающего перед началом протокола и определяет ее в результате выполнения протокола.

19 Протокол IKE предназначен для…

- аутентификации участников протокола и выработки общего секретного ключа

- передачи информации с обеспечением конфиденциальности
- механизма реализации слепой электронной подписи

10. Протокол OCSP предназначен для…
- взаимной аутентификации клиента и сервера перед установлением связи между ними
- передачи информации с обеспечением конфиденциальности
- проверки статуса сертификата открытого ключа

А2. Вопросы для устного опроса

1. Понятие криптографического протокола. Применение криптографических протоколов для обеспечения информационной безопасности.
2. Классификация криптографических протоколов по цели безопасности.
3. Основные виды уязвимостей и атак на криптографические протоколы, защитные меры.
4. Подходы к оценке безопасности криптографических протоколов. Средства анализа уязвимостей.
5. Правила построения криптографических протоколов. Криптографический протокол передачи сообщений с обеспечением свойства целостности.
6. Криптографические методы обеспечения неотказуемости. Криптографический протокол передачи сообщений с обеспечением свойства неотказуемости.
7. Криптографический протокол передачи сообщений с обеспечением свойства конфиденциальности.
8. Комбинированные криптографические протоколы.
9. Односторонняя и двухсторонняя аутентификация.
10. Протоколы аутентификации на основе паролей, протоколы «рукопожатия» и типа «запрос-ответ».
11. Протоколы аутентификации с использованием систем ассиметричного шифрования.
12. Протоколы аутентификации источника информации.
13. Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем.
14. Двух и трех сторонние протоколы передачи и распределения ключей. Функции доверенной третьей стороны и выполняемые ею роли.
15. Схемы предварительного распределения ключей. Групповые протоколы.
16. Протокол ключевого обмена Диффи-Хеллмана.
17. Протоколы разделения секрета.
18. Автономные схемы электронных платежей. Схемы слепой подписи.
19. Протоколы битовых обязательств.
20. Протокол подбрасывания монеты.
21. Протоколы битовых обязательств на основе однонаправленной функции. Раздел 6 Прикладные криптографические протоколы

22. Особенности построения семейства протоколов IPsec. Туннельный и транспортный режимы. Протокол IKE. Протокол ESP.
23. Базовый протокол Kerberos..
24. Протоколы SKIP, SSL/TLS.
25. Протоколы OCSP и TSP.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Задачи

1. 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?

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

1. Определение и свойства криптографических протоколов. Участники протокола. Общая классификация атак на криптографические протоколы. Компроментация криптографического протокола.
2. Критерии оценки стойкости криптографических алгоритмов и протоколов.
3. Характеристики вычислительно сложных задач теории чисел, возможности их применения в ассиметричной криптографии (задача факторизации и производные от нее задачи, задача дискретного логарифмирования и производные от нее задачи).
4. Парные отображения и их свойства. Вычислительно сложные задачи, основанные на парных отображениях.
5. Основные подходы к конструированию стойких криптографических алгоритмов и протоколов в рамках концепции “доказательной безопасности”.
6. Интерактивные системы доказательства: цель доказательства, общий принцип построения протокола, свойства полноты и корректности.
7. Интерактивные системы доказательства с нулевым разглашением знания: цель доказательства, общий принцип построения протокола, свойство нулевого разглашения знания, теоремы.
8. Классификация протоколов аутентификации. Атаки на протоколы с фиксированными паролями.
9. Протоколы аутентификации с одноразовыми паролями. Схема Лэмпорта.
10. Протоколы аутентификации “запрос-ответ”, основанные на симметричных криптосистемах: классификация, примеры, стандартизация (ISO/IEC 9798).
11. Протоколы аутентификации “запрос-ответ”, основанные на асимметричных криптосистемах: классификация, примеры, стандартизация (ISO/IEC 9798).
12. Протоколы аутентификации, основанные на доказательствах с нулевым разглашением знаний (на примере прооокола Фиата-Шамира).
13. Общая классификация протоколов распределения ключей (ПРК), основные и дополнительные свойства ПРК.
14. Классификация ПРК, основанных на симметричных криптосхемах. Двусторонние протоколы (без центра доверия).
15. ПРК с центром доверия, основанные на симметричных криптосхемах: протокол Needham-Schroeder, протокол Kerberos.
16. ПРК с центром доверия, основанные на симметричных криптосхемах: протокол Otway- Rees, атаки на него.
17. Классификация ПРК, основанных на симметричных криптосхемах. Протокол транспортировки ключей Needham-Schroeder с использованием схем открытого шифрования.
18. Протоколы транспортировки ключей, рекомендованные стандартом

X.509.

19. Протокол транспортировки ключей Beller-Yacobi.
20. Протокол обмена ключами Диффи-Хеллмана, атаки на него.
21. Протокол обмена ключами MTI, атаки на него.
22. Протокол обмена ключами STS.

В3. Тематика презентаций

1. Определение и свойства криптографических протоколов. Участники протокола. Общая классификация атак на криптографические протоколы. Компроментация криптографического протокола.
2. Критерии оценки стойкости криптографических алгоритмов и протоколов.
3. Характеристики вычислительно сложных задач теории чисел, возможности их применения в ассиметричной криптографии (задача факторизации и производные от нее задачи, задача дискретного логарифмирования и производные от нее задачи).
4. Парные отображения и их свойства. Вычислительно сложные задачи, основанные на парных отображениях.
5. Основные подходы к конструированию стойких криптографических алгоритмов и протоколов в рамках концепции “доказательной безопасности”.
6. Интерактивные системы доказательства: цель доказательства, общий принцип построения протокола, свойства полноты и корректности.
7. Интерактивные системы доказательства с нулевым разглашением знания: цель доказательства, общий принцип построения протокола, свойство нулевого разглашения знания, теоремы.
8. Классификация протоколов аутентификации. Атаки на протоколы с фиксированными паролями.
9. Протоколы аутентификации с одноразовыми паролями. Схема Лэмпорта.
10. Протоколы аутентификации “запрос-ответ”, основанные на симметричных криптосистемах: классификация, примеры, стандартизация (ISO/IEC 9798).
11. Протоколы аутентификации “запрос-ответ”, основанные на асимметричных криптосистемах: классификация, примеры, стандартизация (ISO/IEC 9798).
12. Протоколы аутентификации, основанные на доказательствах с нулевым разглашением знаний (на примере прооокола Фиата-Шамира).
13. Общая классификация протоколов распределения ключей (ПРК), основные и дополнительные свойства ПРК.
14. Классификация ПРК, основанных на симметричных криптосхемах. Двусторонние протоколы (без центра доверия).
15. ПРК с центром доверия, основанные на симметричных криптосхемах: протокол Needham-Schroeder, протокол Kerberos.
16. ПРК с центром доверия, основанные на симметричных криптосхемах: протокол Otway- Rees, атаки на него.

17. Классификация ПРК, основанных на симметричных криптосхемах. Протокол транспортировки ключей Needham-Schroeder с использованием схем открытого шифрования.

18. Протоколы транспортировки ключей, рекомендованные стандартом X.509.

19. Протокол транспортировки ключей Beller-Yacobi.

20. Протокол обмена ключами Диффи-Хеллмана, атаки на него.

21. Протокол обмена ключами MTI, атаки на него.

22. Протокол обмена ключами STS.

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

С.1. Практические задания

1. Как преобразовать протокол аутентификации запрос-ответ на базе схемы открытого шифрования в протокол аутентичного распределения ключей? Приведите два примера: для протокола односторонней аутентификации и для протокола взаимной аутентификации.

2. Приведите описание процедуры восстановления секрета из схемы разделения секрета Шамира двумя способами: для случая, когда общее число участников равно 3, максимально допустимое количество утраченных (скомпроментированных) долей секрета равно 2, длина разделяемого секрета равно 128 битам.

3. Какими из основных свойств протоколов распределения ключей (неявная аутентификация ключа, подтверждение ключа, явная аутентификация) обладает протокол Kerberos? Какие практические задачи он позволяет решать?

4. Оцените вычислительную сложность (количество выполненных операций) и коммуникационную сложность (количество пересылок сообщений и объем передаваемых данных) протокола доказательства знания дискретного логарифма для каждого участника. Приведите пример такого задания параметров протокола, при котором вероятность обмана доказывающим проверяющего не превысит 2-30.

5. Сравните по стойкости к различным видам атак два метода аутентификации по одноразовым паролям: метод Лэмпорта и последовательно обновляемые одноразовые пароли. Какие выводы о предпочтительности того или иного метода можно сделать?

6. Модифицируйте протокол обеспечения свойства конфиденциальности и целостности передачи сообщений для предварительного обмена сессионным ключом симметричной схемы шифрования.

7. Модифицируйте протокол обеспечения свойства неотказуемости и целостности передачи сообщений для предварительной аутентификации участников информационного обмена.

8. Модифицируйте протокол обеспечения конфиденциальности и

неотказуемости сообщений для предварительного обмена сессионным ключом симметричной схемы шифрования.

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1. Перечень контрольных вопросов

1 Понятие криптографического протокола.
2 Классификация криптографических протоколов.
3 Основные виды уязвимостей и атак на криптографические протоколы
4 Основные защитные меры в криптографических протоколах
5 Криптографический протокол передачи сообщений с обеспечением свойства целостности.
6 Криптографический протокол передачи сообщений с обеспечением свойства конфиденциальности.
7 Криптографический протокол передачи сообщений с обеспечением свойства неотказуемости.
8 Комбинированные криптографические протоколы.
9 Односторонняя и двухсторонняя аутентификация.
10 Протоколы аутентификации на основе паролей
11 Протоколы аутентификации на основе рукопожатия
12 Протоколы аутентификации типа запрос-ответ.
13 Протоколы генерации и передачи ключей на основе симметричных и асимметричных схем шифрования
14 Двух и трех сторонние протоколы передачи и распределения ключей.
15 Функции доверенной третьей стороны и выполняемые ею роли.
16 Схемы предварительного распределения ключей.
17 Групповые протоколы.
18 Протокол ключевого обмена Диффи-Хеллмана.
19 Свойства неотслеживаемости и несвязывемости криптографических протоколов электронных платежных систем.
20 Протоколы битовых обязательств.
21 Автономные схемы электронных платежей.
22 Базовый протокол Kerberos.
23 Протоколы IPsec.
24 Протоколы SKIP, SSL/TLS.
25 Протоколы OCSP и TSP

Д1. Практические задания

1 Приведите формальное описание примитивного протокола для обеспечения свойства неотказуемости и целостности передачи сообщений.

2 Приведите формальное описание примитивного протокола для обеспечения свойства конфиденциальности и целостности передачи сообщений.

3 Приведите формальное описание примитивного протокола для обеспечения свойства конфиденциальности и неотказуемости сообщений.

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 – 20 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
Бинарная	Зачтено			Не зачтено

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 практического задания	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***
Зачет	0-20	«не зачтено» «зачтено»

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-9	«не зачтено»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы
10-14	«зачтено»	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.
15-17	«зачтено»	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
18-20	«зачтено»	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	«неудовле твори-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; 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; 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	«неудовле		Задача не нешена, обнаруживается существенное непонимание проблемы

	твори-тельно»		

Практические задания. 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 работы, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания выполнения *практических работ*

Баллы	***Оценка***	***Показатели***	***Критерии***
13-15	«отлично»	4. Полнота выполнения задания; 5. Своевременность выполнения задания; 6. 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
9-12	«хорошо»		Основные требования к выполнению задания 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 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 работы не выполнены, обнаруживается существенное непонимание проблемы.

Лист актуализации оценочных материалов по дисциплине «Криптографические протоколы»

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 _____