Фонд оценочных средств для промежуточной аттестации
по дисциплине
Криптографические протоколы

Направление подготовки (специальность)
10.05.01 Компьютерная безопасность

Направленность (профиль)
специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Присваиваемая квалификация
специалист по защите информации

Форма обучения
очная

Челябинск 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность 10.05.01 Компьютерная безопасность.
Специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем».
Дисциплина: **Криптографические протоколы**.
Семестр (семестры) изучения: 9 семестр.
Форма (формы) промежуточной аттестации: экзамен 9 семестр.
Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Криптографические протоколы» направлено на формирование следующих компетенций:

Коды компетенции согласно ФГОС (ОПОП ВО)	Содержание компетенций согласно ФГОС (ОПОП ВО)	Индикаторы достижения компетенции согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
1	2	3	4
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Знает типовые криптопротоколы, используемые в сетях связи; основные типы криптопротоколов и принципов их построения с использованием шифрсистем. ОПК-10.2 Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. ОПК-10.3 Владеет подходами к разработке и анализу безопасности криптографических протоколов.	Знать: – различия между стеганографией и криптографией; – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты. Уметь: – использовать блочные алгоритмы шифрования для формирования хеш-функции; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать односторонние функции в целях построения криптосистем; – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой

			подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – основными методами симметричного шифрования; алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети Интернет; – методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом; – технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1. Виды оценочных средств

№ п/п	Код компетенции / планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1.	ОПК-10	Раздел 1. Основы криптографических протоколов	Вопросы к коллоквиуму	Вопросы к экзамену
2.	ОПК-10	Раздел 2. Протоколы электронной цифровой подписи	Практическая работа № 3, вопросы к коллоквиуму	Вопросы к экзамену
3.	ОПК-10	Раздел 3. Протоколы аутентификации	Практическая работа № 1-2, вопросы к коллоквиуму	Вопросы к экзамену
4.	ОПК-10	Раздел 4. Протоколы распределения ключей	Практическая работа № 4, вопросы к коллоквиуму	Вопросы к экзамену
5.	ОПК-10	Раздел 5. Прикладные протоколы	Практическая работа № 4, вопросы к коллоквиуму	Вопросы к экзамену
6.	ОПК-10	Раздел 6. Анализ уязвимостей и защита протоколов	Практическая работа № 5, вопросы к коллоквиуму	Вопросы к экзамену

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе дисциплины (модуля). Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.

3.2. Содержание оценочных средств

3.2.1. Список теоретических вопросов к коллоквиуму:

1. Общее понятие хеш-функции.
2. Понятие однашаговой хеш-функции.
3. Области применения хеш-функции.
4. Основное требование к хеш-функции.
5. Почему аутентификация источника данных включает проверку целостности данных?
6. Где может быть использована аутентификация транзакции?
7. Как может быть обеспечена единственность и своевременность?
8. ХФ, задаваемая ключом, области использования.
9. ХФ, не зависимая от ключа, области использования.
10. Зачем в случае однашаговой ХФ использовать фиксированную строку из даты, время, номера, длины сообщения и др.?
11. Какой недостаток построения дополнением ключа в ключевой ХФ на основе бесключевой?
12. Почему CRC32 нельзя использовать в качестве бесключевой ХФ?
13. Почему нельзя использовать ХФ на основе одношаговой сжимающей функции $f_k(x, H) = E_k(x + H)$?
14. Почему нельзя использовать в качестве криптографических хеш-функций линейные отображения?
15. Можно ли использовать в качестве бесключевой хеш-функцию, задаваемую фиксированным общеизвестным ключом?
16. Определение ЦП.
17. Свойства ЦП.
18. Задачи ЦП.
19. Зачем создавать инфраструктуру сертификатов?
20. Понятие центра сертификации.
21. Понятие центра регистрации.
22. Понятие удостоверяющего центра.
23. Равнозначная ли собственноручная подпись на бумажном носителе подписи в электронном документе?
24. Что должно быть указано в договоре между участниками информационного взаимодействия с применением электронных цифровых подписей.
25. Понятие электронной подписи. Отличие от ЦП.
26. Основные подходы к построению схем ЦП.
27. Понятие схемы ЦП с восстановлением текста.
28. Какие недостатки совместного ЦП: ЦП каждого участника?
29. Почему, если при передаче сообщение дополнительно шифруется с помощью асимметричного шифра, то преобразование, используемая в схеме цифровой подписи, должна отличаться от той, которая используется для шифрования сообщений?

30. Почему целесообразнее шифровать подписанные данные, чем, наоборот, - подписывать шифрованные данные?
31. Понятие ЦП с дополнением.
32. Какое достоинство и какой недостаток у ЦП Фиата-Шамира?
33. Какой главный недостаток ПЭП Диффи-Лампорта?
34. Понятие схемы конфиденциальной ЦП (undeniable).
35. Понятие ЦП, подтверждаемая уполномоченным участником.
36. Понятие ЦП вслепую (blind).
37. Понятие схемы групповой ЦП.
38. Встраивание скрытых сообщений в ЦП.
39. Понятие ПА.
40. Классификация ПА.
41. Атаки на ПА на основе фиксированного пароля.
42. Понятие ПА на основе техники доказательства знаний и КП доказательства знаний.
43. Понятие полнота, корректность и нулевое разглашение.
44. Понятие КП с нулевым разглашением, схема.
45. Понятие ДОР, схема.
46. Классификация ДОР, примеры.
47. В каких КП применяют ДОР.
48. Какие типы знаний используются в ДОР.
49. Понятие совместной генерации случайных значений.
50. Суть КП bit committment, применение.
51. Суть КП подбрасывания монеты, применение.
52. С какой целью используется маскировки.
53. Типы КП распределения ключей.
54. Понятие К, СК.
55. Классификация К.
56. Классификация СК.
57. Основные задачи и цели ПА Керберос.
58. Понятие открытого распределения ключей, преимущества.
59. Понятие безопасного аутентифицированного протокола обмена ключами, свойства.
60. Схема предварительного распределения ключей, преимущество и применение.
61. Схема предварительного распределения ключевой информации.
62. Схема распределения секрета, пример.
63. (n,k)-пороговая СРС.
64. Понятие анонимной передачи СК.
65. Понятие генерации ЗК группой участников.
66. Процедуры по управлению ключами.
67. Угрозы инфраструктуры ключей.
68. Политика безопасности управления ключами.
69. Понятие главный ключ, ключ для шифрования ключей, ключ для шифрования данных.
70. Понятие срока действия ключа.

71. Срок хранения ОК и ЗК для ЦП.
72. Архивирование ОК и ЗК для шифрования.
73. Основные центра по управлению ключами.
74. Свойство скрытой (неявной) аутентификации получателя.
75. Свойство защищенности от чтения назад.
76. Свойство инвариантности отправителя.
77. Свойство последовательного представления.
78. Понятие атаки на КП.
79. Факторы стойкости КП.
80. Предположения о КП.
81. Классификация атак на КП.
82. Предположения о противнике.
83. Классификация противников.
84. Типичные атаки.
85. Предположения для анализа КП.

3.2.2. Список практических работ:

№ п/п	Формулировка задания
1	Реализовать один алгоритм аутентификации сообщений с использованием блочного симметричного шифрования из следующего списка: 1. DES 2. Triple-DES 3. IDEA 4. Blowfish 5. Twofish 6. RC2 7. RC5 8. CAST 9. Skipjack 10. ГОСТ 28147-89 11. Solitare 12. SQUARE 13. Serpent 14. S1 15. Safer 16. REDOC 17. 3-Way 18. A5 19. Akellare 20. Bear 21. CRYPTON 22. DEAL 23. DFC

	24. E2 25. FROG 26. HPC 27. Khafre 28. Khufu 29. Lion 30. LOKI 31. NSEA 32. MacGuffin 33. MAGENTA 34. MARS 35. MISTY 36. MMB 37. MPJ
2	Реализовать один алгоритм аутентификации сообщений на основе хеш-функции HMAC из следующего списка: 1. HAVAL 2. Keccak 3. LM-хеш 4. MD2 5. MD4 6. MD5 7. MD6 8. N-Hash 9. RIPEMD-128 10. RIPEMD-160 11. RIPEMD-256 12. RIPEMD-320 13. SHA-1 14. SHA-2 15. SHA-256 16. SHA-384 17. SHA-512 18. Skein 19. Snefru 20. Tiger 21. Whirlpool 22. ГОСТР 34.11-94
3	Реализовать один протокол электронной подписи из следующего списка: 1. ПЭП Фиата-Шамира 2. ПЭП Фейге-Фиата-Шамира 3. ПЭП Гиллу-Кискате 4. ПЭП Эль-Гамаля 5. ПЭП Шнорра

	6. ПЭП DSA 7. ПЭП DSA 1 вариант 8. ПЭП DSA 2 вариант 9. ПЭП RSA 10. ПЭП ГОСТ (старый) 11. ПЭП Esign 12. Одноразовый Лампорта 13. Многоразовый Лампорта 14. Другой протокол undeniable 15. ПЭП Онга-Шнорра-Шамира 16. Общий с (mr', -s, 1) 17. Общий с (mr', ms, 1) 18. Общий с (-r', ms, 1) 19. Общий с (1, ms, -r') 20. Общий с (ms, 1,mr') 21. Общий с (mr', 1, -s)
4	Реализовать один из прикладной протоколов: 1. СРКИ Блума 2. СРКИ KDP 3. КП KEA 4. КП MQV 5. СРС Шамира 6. СРС Блэкли (Blakley) 7. СРС Асмута-Блума 8. СРС Карнина-Грина-Хеллмана 9. Протокол Бурместера-Десменда 10. Д0Р наличие изоморфизма графа 11. Д0Р знания ЗК в RSA 12. Д0Р знания дискретного логарифма 13. Д0Р знания гамильтонового цикла 14. КП бит привязки (bit committment) 15. ППМ Блума 16. Протокол Подписание контракта 17. Протокол Покер по телефону 18. Протокол Электронная почта 19. Протокол Голосование 20. Протокол электронной банкноты 21. Протокол заказное письмо 22. Протокол ограниченной передачи секрета
5	Реализовать один протокол аутентификации из списка. Необходимо описать криптографический протокол и его реализацию. Все сообщения между участниками криптографического протокола должны быть реализованы с помощью сетевого взаимодействия. Каждый участник должен быть реализован в виде отдельного клиента. Должна быть описана схема криптографического протокола в рамках

	общих определении и обозначений, данных на лекции. Должно быть дано подробное описание реализации криптографического протокола и атаки на данный протокол. Должна быть реализована одна атака, в виде некоторой упрощенной модели. Для выбранного протокола необходимо аргументировано описать свойства безопасности, которыми он обладает, в рамках терминов данных на лекции. Должна быть описана схема криптографического протокола в рамках общих определении и обозначений, данных на лекции. Должен быть освящен вопрос об уязвимостях и атаках на данный криптографический протокол с описанием схемы в рамках общих определении и обозначений, данных на лекции. 1. Andrew RPC Handshake 2. ПА BAN Yahalom (Яхолом) 3. ПА Нидхем-Шредер с симметричным шифрованием (исправленный) 4. ПА Нидхем-Шредер с симметричным шифрованием 5. Модифицированный Woo-Lam (Ву-Лам) 6. Woo-Lam (Ву-Лам) 7. ПА Ньюман-Стаблбайн (Neuman-Stubblebine) 8. S-Key 9. STS 10. IKE 11. DHKE 12. ПА Отвея-Рииса ослабленный вариант (Otway-Rees) 13. NSL Needham-Shroeder Long Protocol 14. ISO 15. ISO2 16. ПА Wide-Mouth frog 17. Диффи-Хеллман (со всеми уязвимостями и атаками) 18. Трехпроходный ПА (атака Винера) 19. Бесключевой протокол Шамира (3 атаки) 20. ПА Деннинга-Сакко 21. KEA 22. MTI/A0

3.2.3. Список теоретических вопросов к экзамену:

1. Понятие КП.
2. Классификация участников КП.
3. Задачи КП.
4. Свойства КП.
5. Понятия шага, цикла, прохода, сеанса в КП.
6. Понятие функции-сервиса безопасности, их классификация.
7. Основные функции-сервиса безопасности.
8. Почему нельзя дописать в начало или конец исходного сообщения ключ для ключевой ХФ на основе бесключевой?

9. Доказать, что если функция хеширования h построена на основе одношаговой сжимающей функции, то из устойчивости к коллизиям функции f следует устойчивость к коллизиям функции h.
10. Доказать, что если хеш-функция устойчива к коллизиям, то она устойчива к нахождению второго прообраза.
11. Доказать, что устойчивая к коллизиям хеш-функция не обязательно является однонаправленной.
12. Доказать, что $f(x, H) = E_k(x + H)$, $f(x, H) = E_x(H)$, $f(x, H) = E_{H(x)}$ ХФ являются уязвимыми.
13. Примеры ЦП на основе систем с открытым ключем.
14. Математически объяснить наложения требований в RSA.
15. Найти число возможных вариантов общей ЦП.
16. ПА на основе фиксированного пароля.
17. Защита от перехвата пароля в ПА на основе фиксированного пароля.
18. Усложнение подбора паролей в ПА на основе фиксированного пароля
19. Защита базы данных от компрометации в ПА на основе фиксированного пароля.
20. Защита от повторного использования в ПА на основе фиксированного пароля.
21. ПА на основе одноразовых паролей, примеры.
22. ПА на основе техники <<запрос-ответ>> с СШ, примеры.
23. ПА на основе техники <<запрос-ответ>> с АШ, примеры.
24. ПА на основе техники <<запрос-ответ>> без ЦП, примеры.
25. ПА на основе техники <<запрос-ответ>> с ЦП, примеры.
26. Математически обосновать наложения условия $(p-1)/2$ простое в КП.
27. Математически обосновать наложения условия q делило $p-1$ в КП.
28. Задача КП игры в покер по телефону.
29. Определение коммутативного шифрования, пример, применение.
30. Задача КП подписания контракта.
31. Задача КП электронной почты.
32. Задача КП голосования.
33. Задача КП электронной коммерции.
34. Пример КП ОА и передачи СК.
35. Пример КП ДА и передачи СК.
36. Пример КП передачи СК с доверенным посредником.
37. Пример КП передачи СК без доверенным посредником.
38. Пример КП передачи СК с СШ.
39. Пример КП передачи СК с АШ.
40. Пример КП передачи СК с ЦП.
41. Пример КП обновления СК.
42. Пример безопасного аутентифицированного протокола обмена ключами.
43. Суть схемы Блума.
44. Суть схемы KDP.
45. Суть СРС Шамира, достоинства и недостатки.
46. Суть СРС Блэкли.
47. Суть СРС Асмута-Блума.
48. Суть СРС Карнина-Грина-Хеллмана.

49. Жизненный цикл ключей.
50. Особенности управления ключами в СШ, методы, примеры.
51. Особенности управления ключами в АШ, методы, примеры.
52. Основные свойства, характеризующие безопасность КП.
53. Суть атаки подмены, защита, КП.
54. Суть атаки повторного навязывания, защита, КП.
55. Суть атаки отражения, защита, КП.
56. Суть атаки задержки передачи, защита, КП.
57. Суть атаки комбинированной (чередованием), защита, КП.
58. Суть атаки с параллельными сеансами, защита, КП.
59. Суть атаки со специально подобранными текстами, защита, КП.
60. Суть атаки человек по середине, защита, КП.
61. Суть атаки с известным СК, защита, КП.
62. Суть атаки с неизвестным СК, защита, КП.
63. Суть атаки с неправильным выполнением криптопримитивов, защита, КП.
64. Суть атак специализированных, защита, КП.
65. Структура протокола IPSec.
66. Механизмы AH, ESP.
67. Протокол установления защищенной ассоциации и управления ключами.
68. Дать определение эллиптической кривой.
69. Какие преимущества использования эллиптической кривой в КП в отличии от АШ.
70. Найти вероятность наличия коллизии в парадоксе дней рождений и найти оценку снизу для этой вероятности.
71. Доказать, что для хеш-функции на основе дискретного логарифма выполняется условие сложности подбора коллизий в предположении сложности нахождения дискретного логарифма.
72. Доказать невозможность игры покера по телефону.
73. Базовая схема ПА Керберос.
74. КП Диффи-Хеллмана.
75. Атака на КП Диффи-Хеллмана.
76. Чтение, анализ и модификация любого протокола.
77. Свойства эллиптической кривой, примеры эллиптической кривой.
78. КП Диффи-Хеллмана на основе эллиптической кривой.
79. Суть, цели, задачи IPSec.
80. Понятие защищенной ассоциации.
81. Протокол TLS.
82. Протокол SSL.
83. Протокол электронные выборы.
84. Протокол электронные банкноты.
85. Протокол покер по телефону.
86. Протокол электронная почта.

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

В течение семестра выполняется пять практических работ, каждая из которых оценивается в 10 баллов. Кроме того, в рамках коллоквиума студенту предлагается 2 вопроса, каждый из которых оценивается в 10 баллов. На экзамене студенту предлагается 3 вопроса, каждый из которых оценивается в 10 баллов.

Сводная таблица рейтинга успеваемости (9 семестр)

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Практическая работа №1-5	5x10=50
2	Коллоквиум (теоретический вопрос)	2x10=20
3	Экзамен (теоретический вопрос)	3x10=30
4	Итого	100

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

4.2.1 Критерии оценивания теоретического вопроса (для коллоквиума и экзамена)

Максимальный балл за ответ на теоретический вопрос – 10 баллов.

Отлично/зачтено/9-10 баллов	Хорошо/зачтено/7-8 баллов	Удовлетворительно/ зачтено/5-6 баллов	Неудовлетворительно/не зачтено/0-4 балла
Обучающийся отлично знает материал, понимает терминологию криптографических протоколов. Обучающийся практически не допускает ошибок.	Обучающийся хорошо знает материал, понимает терминологию криптографических протоколов. Обучающийся допускает незначительные ошибки.	Обучающийся знаком с материалом, владеет терминологией криптографических протоколов. Обучающийся допускает фактические ошибки.	Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций

4.2.2. Критерии оценивания практической работы

Практическая работа выполняется на любом доступном студенту языке программирования.

Максимальный балл за практическую работу – 10 баллов.

Оценка	**Отлично/зачтено**	**Хорошо/зачтено**	**Удовлетворительно/зачтено**	**Неудовлетворительно/не зачтено**
Баллы	**9-10 баллов**	**7-8 баллов**	**5-6 баллов**	**0-4 балла**
Критерии	Практическая работа выполнена правильно, в срок, обучающийся отлично знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу.	Выполнено 3/4 практической работы, обучающийся хорошо знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу, но допускает незначительные ошибки.	Выполнено 1/2 практической работы, либо работа сдана значительно позднее, чем предполагалось, при этом обучающийся знает материал, но допускает ошибки.	Работа не выполнена, либо обучающийся не может ответить на контрольные вопросы, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
Уровень освоения проверяемых компетенций	высокий	средний	базовый	недостаточный

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации:

0 – 60 баллов – неудовлетворительно (2);

61 – 74 баллов – удовлетворительно (3);

75 – 90 баллов – хорошо (4);

91 – 100 баллов – отлично (5).

Особенности проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).

Уровни сформированности компетенций определяется следующим образом:

1. Высокий уровень сформированности компетенций соответствует оценке «Отлично»:
   - предполагает формирование компетенций на высоком уровне, готовность к самостоятельной профессиональной деятельности,
   - студент способен аргументировать собственную точку зрения по дискуссионным вопросам дисциплины, решать ситуационные задачи, формулировать собственные выводы.
2. Средний уровень соответствует оценке «Хорошо»:
   - предполагает формирование компетенций на достаточном уровне,
   - студент способен давать развернутые ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Хорошо».
3. Базовый уровень соответствует оценке «Удовлетворительно»:
   - предполагает формирование компетенций на начальном уровне,
   - студент способен давать ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Удовлетворительно»,
   - студент способен отвечать на вопросы в закрытой форме. Количество правильных ответов – не менее 50%.
4. Низкий уровень соответствует оценке «Неудовлетворительно».

Специальность 10.05.01 Компьютерная безопасность
Специализация №6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»
Фонд оценочных средств по дисциплине «Криптографические протоколы»
2025 год набора, очная форма обучения

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:
Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета
математического факультета согласовано Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 8 от 01.02.2025

Заведующий кафедрой согласовано А. Н. Ручай

Автор (составитель) А. Н. Ручай

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1