УТВЕРЖДАЮ
Проректор по научной работе
_____А.И. Бирюков
«_31_» _____03_____ 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)*

2.1.2.2. «Криптографические протоколы»

Научная специальность – 2.3.6. Методы и системы защиты информации, информационная безопасность

Направленность (профиль) – Методы и системы защиты информации, информационная безопасность

Высшее образование – подготовка кадров высшей квалификации

Форма обучения
очная

Челябинск, 2025

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

© ФГБОУ ВО «ЧелГУ»

Программа по дисциплине «Криптографические протоколы» составлена в соответствии с паспортом научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность и федеральными государственными требованиями (уровень образования: высшее образование – подготовка кадров высшей квалификации), утвержденными приказом Министерства науки и высшего образования Российской Федерации от 20 октября 2021 года № 951.

Разработчик программы:

Зав. кафедрой компьютерной безопасности
и прикладной алгебры,
кандидат физико-математических наук, доцент А.Н. Ручай

Программа одобрена на заседании кафедры компьютерной безопасности и прикладной алгебры от «04» марта 2025 г., протокол № 10.

Зав. кафедрой компьютерной безопасности
и прикладной алгебры А.Н. Ручай

Программа принята на заседании Ученого совета математического факультета от «27» 03 2025 г., протокол № 8.

Согласовано:

Декан математического факультета Е.А. Сбродова

Зав. отделом аспирантуры
и докторантуры Н.В. Бочкарева

© ФГБОУ ВО «ЧелГУ»

Аннотация программы: Изучение принципов построения и алгоритмов протоколов, обеспечивающих конфиденциальность, целостность и аутентичность информации. В результате изучения курса аспирант должен иметь представления о криптографических примитивах, основных направлениях современной криптографии, основных типах криптосистем, а также протоколах, которые имеют дело с этими криптосистемами. Аспирант должен иметь представление об области применения криптографических протоколов. Аспирант должен знать и уметь реализовывать на практике основные примитивные и прикладные протоколы, иметь представление об анализе стойкости протоколов.

1. Цели и задачи освоения дисциплины

Цели дисциплины:

– изучение принципов построения и алгоритмов протоколов, обеспечивающих конфиденциальность, целостность и аутентичность информации.

Задачи дисциплины:

– формирование у обучающихся представления об основных направлениях современной криптографии, основных типах криптосистем, а также протоколах, которые имеют дело с этими криптосистемами;

– формирование у обучающихся представления об области применения криптографических протоколов;

– формирование у обучающихся навыков, необходимых для применения соответствующего математического аппарата для формализации, анализа и решения проблем, возникающих в ходе профессиональной деятельности;

– формирование у обучающихся навыков, необходимых для разработки методов построения и расчета оценок качества криптографических протоколов, основанных на сложных математических проблемах

2. Место дисциплины в структуре образовательной программы

Дисциплина «Криптографические протоколы» (дисциплина по выбору) является обязательной. Преподавание дисциплины осуществляется на первом курсе (во 2 семестре).

Общая трудоемкость дисциплины, в том числе и промежуточная аттестация, составляет 2 зачетных единиц/72 часов, из них:

контактная работа с преподавателем составляет – 0,67 зачетных единиц/ 24 часов (лекционные занятия – 12 часов, практические занятия – 12 часов),

© ФГБОУ ВО «ЧелГУ»

самостоятельная работа – 1,28 зачетных единиц/46 часов,

контроль – 0,05 зачетных единиц/2 часов.

Освоение дисциплины опирается на знания алгебры, теории конечных групп, колец и полей, моделей безопасности компьютерных систем, теоретико-числовых методов в криптографии, методов и средств криптографической защиты информации.

Для освоения дисциплины обучаемый должен обладать навыками аналитической работы, а также владеть основными навыками владения современными вычислительными средствами.

Дисциплина «Криптографические протоколы» призвана помочь аспирантам овладеть навыками и знаниями, необходимыми для подготовки к кандидатскому экзамену, выполнения научно-исследовательской работы, включая выполнение кандидатской диссертации.

Требования к «входным» знаниям, умениям и опыту деятельности обучающегося, необходимые при изучении дисциплины

Знать	Уметь	Владеть
– основные алгебраические понятия и алгебраические методы решения прикладных задач	– использовать знания, полученные в курсе, для решения прикладных задач, в программировании	– алгебраическими методами при построении модели прикладной задачи
– основные формальные модели политик безопасности, модели дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков; – виды и состав угроз информационной безопасности; – принципы и общие методы обеспечения информационной безопасности; – основы разработки систем защиты информации предприятия (организации) и подсистемы информационной	– самостоятельно разрабатывать новые и дорабатывать типовые модели политик безопасности; – определять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию; – определять возможные каналы и методы несанкционированного доступа; – организовывать системное обеспечение защиты информации; – самостоятельно разрабатывать системы защиты информации предприятия (организации) и подсистемы	– методами разработки моделей политик безопасности, управления доступом и информационными потоками; – навыками определения угроз информации в зависимости от среды эксплуатации продуктов информационных технологий; – навыками разработки основных политик безопасности; – методами разработки системы защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы.

© ФГБОУ ВО «ЧелГУ»

безопасности компьютерной системы; – методы выявления уязвимостей.	информационной безопасности компьютерной системы.	
– основные теоретико-числовые свойства делимости, непрерывных дробей, систем и классов вычетов.	– применять методы теории чисел для решения задач.	– решения теоретико-числовых задач.
– основные понятия и классификацию средств криптографической защиты информации; шифрования	– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем	– навыками обеспечения безопасной работы в сети Интернет

3. Требования к результатам освоения содержания дисциплины

Результаты обучения по дисциплине	
знать	– основные понятия и классификацию средств криптографической защиты информации; – основные методы симметричного шифрования; – классификацию методов симметричного шифрования; – понятие хеш-функции; – основные понятия, основные алгоритмы электронной цифровой подписи; – основные стандарты на алгоритмы цифровой подписи; – 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 компьютерных 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	– навыками применения симметричного шифрования; формирования хеш-функций; – навыками применения асимметричных криптосистем; управления ключами в системах с открытым ключом; – навыками обеспечения безопасной работы в сети Интернет.

© ФГБОУ ВО «ЧелГУ»

4. Структура и содержание дисциплины

4.1. Структура дисциплины

Вид работы	Семестр				Всего
	1	2	3	4	
Общая трудоёмкость, акад. часов		72			72
Контактная работа:		24			24
Лекции, акад. часов		12			12
Практические (семинары), акад. часов		12			12
Лабораторные работы, акад. часов					
Самостоятельная работа, акад. часов		46			46
Контроль		2			2
Вид контроля (зачёт, экзамен)		дифференц. зачет			

4.2. Содержание разделов дисциплины

№ раздела	Наименование раздела	Количество часов						Форма текущего контроля
		Всего	Контактная работа				Самостоятельная работа	
			Лекции	Практические, семинары	Лаб. работы	Контроль		
1.	Основы криптографических протоколов	9	1				8	Устный опрос на практических занятиях
2.	Протоколы электронной цифровой подписи	12	2	2			8	
3	Протоколы аутентификации	13	3	2			8	
4	Протоколы распределения ключей	13	3	2			8	
5	Прикладные протоколы	11	1	2			8	
6	Анализ уязвимостей и защита протоколов	12	2	4			6	
	Контроль	2				2		
	Итого:	**72**	**12**	**12**		**2**	**46**	

© ФГБОУ ВО «ЧелГУ»

№ раздела	Наименование раздела	Содержание раздела
1.	Основы криптографических протоколов	**Лекционные занятия:** Понятие криптографического протокола. Классификация протоколов и их примеры **Самостоятельная работа:** Основы криптографических протоколов
2.	Протоколы электронной цифровой подписи	**Лекционные занятия:** Криптографическая хеш-функция. Протоколы электронной цифровой подписи Стандарты электронной цифровой подписи **Практические занятия:** Протоколы электронной цифровой подписи. Основы построения и особенности реализации Протоколы электронной цифровой подписи. Разработка и реализация протоколов **Самостоятельная работа:** Протоколы электронной цифровой подписи /
3	Протоколы аутентификации	**Лекционные занятия:** Обзор протоколов аутентификации Протоколы с нулевым разглашением Стандарты протоколов аутентификации **Практические занятия:** Протоколы аутентификации. Основы построения и особенности реализации Протоколы аутентификации. Разработка и реализация протокола **Самостоятельная работа:** Протоколы аутентификации
4	Протоколы распределения ключей	**Лекционные занятия:** Протоколы открытого распределения ключей Протоколы с аутентифицированной передачей ключей Протоколы предварительного распределения ключей **Практические занятия:** Протоколы распределения ключей. Основы построения и особенности реализации Протоколы распределения ключей. Разработка и реализация протокола **Самостоятельная работа:** Протоколы распределения ключей
5	Прикладные протоколы	**Лекционные занятия:** Прикладные протоколы. Основы построения и особенности реализации

© ФГБОУ ВО «ЧелГУ»

		Практические занятия: Прикладные протоколы. Протокол электронной коммерции и почты Прикладные протоколы. Протокол электронные выборы и игровые протоколы **Самостоятельная работа:** Прикладные протоколы. TLS, SSL Прикладные протоколы. IPSec
6	Анализ уязвимостей и защита протоколов	**Лекционные занятия:** Управление ключами. Уязвимости и защита протоколов **Практические занятия:** Анализ уязвимостей и защита протоколов. Основы построения и особенности реализации Анализ уязвимостей и защита протоколов. Разработка и реализация протокола **Самостоятельная работа:** Анализ уязвимостей и защита протоколов

© ФГБОУ ВО «ЧелГУ»

5. Образовательные технологии

- информационно-коммуникационные технологии;
- исследовательские методы в обучении;
- интерактивные технологии;
- применение новых методов обучения, связанных с использованием возможностей виртуальной информационной среды (мультимедийные технологии).

В соответствии с утвержденной основной образовательной программой по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (направленность (профиль) - Методы и системы защиты информации, информационная безопасность) программа дисциплины «Криптографические протоколы» предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков у обучающихся. Эффективность применения интерактивных форм обучения обеспечивается реализацией следующих условий:

- создание диалогического пространства в организации учебного процесса;
- использование принципов социально-психологического обучения в учебной и научной деятельности;
- формирование психологической готовности преподавателей к использованию интерактивных форм обучения, направленных на развитие внутренней активности аспиранта и достижения ряда важнейших образовательных целей: стимулирование мотивации и интереса в области изучения криптографических протоколов; повышение уровня активности и самостоятельности научно-исследовательской работы; развитие навыков анализа, критичности мышления, научной коммуникации.

© ФГБОУ ВО «ЧелГУ»

6. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

6.1. Паспорт фонда оценочных средств по дисциплине «Криптографические протоколы»

№	Контролируемые разделы дисциплины	Результаты обучения	Наименование оценочного средства
1.	Основы криптографических протоколов	**знать:** – основные определения, понятия и свойства криптографических протоколов	Устный опрос на практических занятиях
2.	Протоколы электронной цифровой подписи	**знать:** – основные понятия, основные алгоритмы электронной цифровой подписи; – понятие хеш-функции; – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты; **уметь:** – использовать блочные алгоритмы шифрования для формирования хеш-функции; – проектировать и использовать системы электронной цифровой подписи; **владеть:** – основными методами симметричного шифрования; алгоритмами формирования хеш-функций	Устный опрос на практических занятиях
3	Протоколы аутентификации	**знать:** – методы построения криптопротоколов, связанных с аутентификацией (сообщений, источника сообщений); – основные методы симметричного и несимметричного шифрования; – стандарты протоколов аутентификации; **уметь:** – использовать симметричные и несимметричные криптосистемы; **владеть:** – навыками использования протоколов аутентификации для обеспечения безопасной работы в сети Интернет	Устный опрос на практических занятиях
4	Протоколы распределения ключей	**знать:** – методы построения криптопротоколов, связанных с выработкой и передачей ключевой информации;	Устный опрос на практических занятиях

© ФГБОУ ВО «ЧелГУ»

		– методы построения систем открытого распределения ключей; **уметь:** – использовать алгоритмы генерации, хранения и распределения ключей; – применять на практике алгоритмы управления открытыми ключами; **владеть:** – методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом	
5	Прикладные протоколы	**знать:** – основы построения и особенности реализации изученных прикладных протоколов; **уметь:** – выбирать параметры криптопротоколов, обеспечивающих требуемые свойства; **владеть:** – навыками использования прикладных протоколов для обеспечения безопасной работы в сети Интернет	Устный опрос на практических занятиях
6	Анализ уязвимостей и защита протоколов	**знать:** – методы оценки качества криптопротоколов; **уметь**: – выбирать параметры криптопротоколов, обеспечивающих требуемые свойства; **владеть:** – навыками выбора необходимых параметров криптопротоколов, при которых обеспечиваются их заданные качества	Устный опрос на практических занятиях

© ФГБОУ ВО «ЧелГУ»

6.2. Оценочные средства

6.2.1. Текущий контроль (Вопросы для устного опроса)

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 $fk(x, H) = Ek(x + H)$?
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.

© ФГБОУ ВО «ЧелГУ»

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.

© ФГБОУ ВО «ЧелГУ»

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.

6.2.2. Примерные темы практических работ

Практическая работа №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

© ФГБОУ ВО «ЧелГУ»

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

Практическая работа №2

Реализовать один алгоритм аутентификации сообщений на основе хеш-функции HMAC из следующего списка:

1. HAVAL
2. Keccak
3. LM-хеш
4. MD2

© ФГБОУ ВО «ЧелГУ»

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

Практическая работа №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)

© ФГБОУ ВО «ЧелГУ»

19. Общий с (1, ms, -r’)
20. Общий с (ms, 1,mr’)
21. Общий с (mr’, 1, -s)

Практическая работа №4

Реализовать один из прикладных 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

Практическая работа №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

© ФГБОУ ВО «ЧелГУ»

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

© ФГБОУ ВО «ЧелГУ»

6.2.3. Промежуточная аттестация

Вопросы к дифференцированному зачету

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 \oplus 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 технике запрос-ответ с СШ, примеры.
23. ПА на основе технике запрос-ответ с АШ, примеры.
24. ПА на основе технике запрос-ответ без ЦП, примеры.
25. ПА на основе технике 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.

© ФГБОУ ВО «ЧелГУ»

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.

© ФГБОУ ВО «ЧелГУ»

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 $\log_{\alpha} \beta$.
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

© ФГБОУ ВО «ЧелГУ»

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене/зачете.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа,
– в форме аудиофайла,
– в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа,
– в форме аудиофайла.

© ФГБОУ ВО «ЧелГУ»

6.3. Критерии оценивания результатов обучения

Оценивание результатов обучения проводится по пятибалльной шкале:
Оценка **«Отлично» (5 баллов)** ставится при соблюдении следующих условий:

- Аспирантом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, в котором он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса.

Оценка **«Хорошо»** (4 балла) ставится при соблюдении следующих условий:

- Аспирантом дан развернутый ответ на поставленный вопрос, в котором студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, логичность и последовательно выстраивает ответ. Однако, допускает неточность в ответе.

Оценка «**Удовлетворительно» (3 балла)** ставится, если:

- Аспирантом дан ответ, свидетельствующий, в основном, о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточной логичностью и последовательностью ответа.

Оценка **«Неудовлетворительно» (1-2 балла)** ставится, если:

- Аспирантом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, отсутствием логичности и последовательности. Выводы поверхностны. Обучающийся не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине

© ФГБОУ ВО «ЧелГУ»

(модулю) обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме на языке Брайля, устно с использованием услуг сурдопереводчика);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно на языке Брайля, с использованием услуг ассистента, устно).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине (модулю) может проводиться в несколько этапов.

7. Учебно-методическое обеспечение дисциплины

Самостоятельная работа аспирантов проводится в форме изучения отдельных теоретических вопросов по предлагаемой литературе и самостоятельного решения задач с дальнейшим их разбором или обсуждением на аудиторных занятиях. Во время самостоятельной подготовки обучающиеся обеспечены доступом к базам данных и библиотечным фондам и доступом к сети Интернет.

Самостоятельная работа способствует:

– углублению и расширению знаний;

– формированию интереса к самостоятельной научно-исследовательской деятельности;

– овладению приемами процесса познания и развитию познавательных способностей.

Самостоятельная работа аспирантов имеет основную цель – обеспечить качество подготовки выпускаемых специалистов.

Самостоятельная работа аспиранта является показателем научного потенциала, умения работы с литературными источниками и нормативными актами, материалами практики, способности аспиранта к самостоятельному анализу проблемных вопросов. Она состоит в изучении учебной и научной литературы, в выполнении заданий для самостоятельной работы.

© ФГБОУ ВО «ЧелГУ»

Аспиранты очной формы обучения изучают и нарабатывают теоретический и практический материал по большей части самостоятельно. На кафедре компьютерной безопасности и прикладной алгебры в списке рекомендованной литературы предложен объем учебной и научной литературы, следовательно, аспиранту необходимо как можно чаще обращаться к фондам научных библиотек, а также и к периодической литературе, следить за новыми изданиями в области защиты информации и информационной безопасности. При изучении научной, учебной литературы необходимо сопоставить содержание имеющейся в наличии литературы с программой кандидатского экзамена по специальности. В случае отсутствия того или иного источника литературы, необходимо обратиться к фондам Российской государственной библиотеки (г. Москва). Аспирант должен провести тщательную подготовительную работу с научной литературой по своей специальности, освоить различные методы поиска информации.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа,
– в форме аудиофайла,
– в печатной форме на языке Брайля.
Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа,
– в форме аудиофайла.

© ФГБОУ ВО «ЧелГУ»

Рекомендованная литература

Основная литература				
	Авторы, составители	Заглавие	Издательство, год	Ресурс
1	Фороузан Б. А.	Математика криптографии и теория шифрования: учебное пособие (https://biblioclub.ru/index.php?page=book&id=428998)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
2	Лапонина О. Р.	Криптографические основы безопасности: учебное пособие (https://biblioclub.ru/index.php?page=book&id=429092)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
3	Ищукова Е. А., Лобова Е. А.	Криптографические протоколы и стандарты: учебное пособие (https://biblioclub.ru/index.php?page=book&id=493059)	Таганрог : Южный федеральный университет, 2016	ЭБС
Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Ресурс
1	Шубович В. Г., Капитанчук В. В., Знаенко Н. С., Титаренко Ю. И.	Разработка моделей криптографической защиты информации: монография (https://biblioclub.ru/index.php?page=book&id=278070)	Ульяновск : Ульяновский государственный педагогический университет (УлГПУ), 2013	ЭБС
2	Зубов А. Ю.	Криптографические методы защиты информации. Совершенные шифры: учебное пособие	Москва : Гелиос АРВ, 2005	
3	Смарт Н., Кулешова С. А., Ландо С. К,	Криптография	М.: Техносфера, 2006	
4	Аграновский А. В., Хади Р. А.	Практическая криптография: алгоритмы и их программирование: учебное пособие (https://biblioclub.ru/index.php?page=book&id=117663)	Москва : СОЛОН-ПРЕСС, 2009	ЭБС

© ФГБОУ ВО «ЧелГУ»

Электронные фонды и ресурсы

Профессиональные базы данных и информационно-справочные системы
1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.
2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.
3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp.
4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php.
5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.
6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/

Лицензионное программное обеспечение по дисциплине (модулю)

Adobe Reader
Octave
VirtualBox
Visual Studio
Notepad++

8. Материально-техническое обеспечение

Для реализации дисциплины «Криптографические протоколы» используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

Практические занятия проходят в учебных лабораториях технических средств защиты информации и «Сетевой полигон» (ауд. 421, 423, учебный корпус № 1). Материально-техническое обеспечение приведено в паспортах лабораторий.

Для проведения занятий по дисциплинам, предусмотренным учебным планом подготовки аспирантов, имеется необходимая материально-

© ФГБОУ ВО «ЧелГУ»

техническая база, соответствующая действующим санитарным и противопожарным правилам и нормам, обеспечивающей проведение всех видов теоретической и практической подготовки, а также эффективное выполнение выпускной квалификационной работы (диссертации):

– лекционные аудитории, оснащенные мультимедийными комплексами на основе антивандальной трибуны;

– специализированные компьютерные классы с подключенным к ним периферийным устройством и оборудованием;

– методические материалы для проведения самостоятельной работы по дисциплине.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Университет располагает компьютерными классами, объединенными в локальную сеть, выходом в Интернет, оснащенными современными высокопроизводительными компьютерами. Поддерживается собственный сайт: http://csu.ru.

Для получения высшего образования по программам аспирантуры инвалидами и лицами с ограниченными возможностями здоровья в университете имеются аудитории, оснащенные следующим оборудованием:

Название кабинета	Оборудование
Тифлотехническая аудитория, кабинет А-28 первого учебного корпуса	Тифлотехнические средства: брайлевский компьютер с дисплеем и принтером, тифлокомплекс «Читающая машина», телевизионное увеличивающее устройство, тифломагнитолы кассетные (3 шт.) и цифровые диктофоны (6 шт.). Специальное программное обеспечение: программа речевой навигации JAWS, речевые синтезаторы («говорящая мышь»), экранные лупы.
Сурдотехническая аудитория, кабинет А-27 первого учебного корпуса	Радиокласс «Сонет-Р» (на 6 человек), программируемые слуховые аппараты (6 шт.) индивидуального пользования с устройством задания режима работы на компьютере, аудиотехника.
Аудитория адаптивных информационных технологий, кабинет А-27 первого учебного корпуса	Компьютерный класс на 2 мест, интерактивная доска ActiveBoard с системой голосования, акустический усилитель и колонки, мультимедийный проектор, телевизор, видеомагнитофон, устройство видеоконференцсвязи VCON HD3000.

Все указанные в настоящей рабочей программе дисциплины методическое и техническое обеспечение учебного процесса для инвалидов и лиц с ограниченными возможностями здоровья предоставляется Региональным учебно-научным центром инклюзивного образования ЧелГУ.

© ФГБОУ ВО «ЧелГУ»

9. Методические указания для обучающихся по освоению дисциплины (модуля)

При изучении данной дисциплины используются лекционные, практические занятия и самостоятельная работа аспиранта. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала аспиранту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.

На практических занятиях изучаются криптографические протоколы. Рекомендуется перед каждым практическим занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Аспиранту желательно проявлять активное участие в практических и лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, форумы, электронная почта и др.).

Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Обучающиеся имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.

Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего

© ФГБОУ ВО «ЧелГУ»

образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

© ФГБОУ ВО «ЧелГУ»