УТВЕРЖДАЮ
Проректор по учебной работе
/ В.Е. Федоров
«06» 08 2020 г.

Рабочая программа дисциплины (модуля)*
Криптографические протоколы

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация № 1 "Анализ безопасности компьютерных систем"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год(ы) набора 2018, 2019, 2020

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

Челябинск 2020 г.

Рабочая программа дисциплины (модуля) принята:
Ученым советом математического факультета

Протокол заседания № 11 от «27» 08 2020 г.

Председатель Ученого совета
математического факультета _____ Е.А. Сбродова

Секретарь Ученого совета
математического факультета _____ С.А. Никитина

Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой компьютерной безопасности и прикладной алгебры

Протокол заседания № 13 от «27» июля 2020 г.

Заведующий кафедрой _____ А.Н. Ручай

Автор (составитель):
Зав.кафедрой, канд.физ.-мат. наук, доцент _____ А.Н. Ручай

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «05» декабря 2018 г. № 678-1

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Криптографические протоколы» является:

-изучение принципов построения и алгоритмов протоколов, обеспечивающих конфиденциальность, целостность и аутентичность информации;

-формирование у студентов представления о криптографических примитивах, основных направлениях современной криптографии, основных типах криптосистем, а также протоколах, которые имеют дело с этими криптосистемами;

-формирование у студентов представления об области применения криптографических протоколов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.Б.1.42

2.1 Требования к предварительной подготовке обучающегося:

Изучение данной дисциплины базируется на следующих курсах общей и специальной подготовки:

Алгебра

Модели безопасности компьютерных систем

Теоретико-числовые методы в криптографии

Криптографические методы защиты информации

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Знания и практические навыки, полученные в курсе «Криптографические протоколы», расширяют профессиональный кругозор, используются обучающимися при разработке дипломных работ.

Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-2: способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретике-числовых методов

Знать:

– основы основные определения и понятия; воспроизводить основные математические факты; распознавать математические объекты; понимать связь между различными математическими объектами.

Уметь:

– выбирать метод и алгоритм для решения конкретной типовой задачи, аргументировать свой выбор;
– строить простейшие математические модели реальных процессов и ситуаций;
– применять компьютерные математические программы для решения задач.

Владеть:

– математическим языком предметной области: основными терминами, понятиями, определениями математических разделов; основными способами представления математической информации (аналитическим, графическим, символьным, словесным и др.).

ПК-5: способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации

Знать:

– основные понятия и классификацию средств криптографической защиты информации;
– различия между стеганографией и криптографией;
– основные методы симметричного шифрования;
– классификацию методов симметричного шифрования;
– основные свойства симметричных криптосистем;
– 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 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.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– основные понятия и классификацию средств криптографической защиты информации;
3.1.2	– основные методы симметричного шифрования;
3.1.3	– классификацию методов симметричного шифрования;
3.1.4	– понятие хеш-функции;
3.1.5	– основные понятия, основные алгоритмы электронной цифровой подписи;
3.1.6	– основные стандарты на алгоритмы цифровой подписи;
3.1.7	– основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты.
3.2	**Уметь:**
3.2.1	– использовать блочные алгоритмы шифрования для формирования хеш-функции;
3.2.2	– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;
3.2.3	– использовать односторонние функции в целях построения криптосистем;
3.2.4	– использовать алгоритмы генерации, хранения и распределения ключей;
3.2.5	– проектировать и использовать системы электронной цифровой подписи;
3.2.6	– применять на практике алгоритмы управления открытыми ключами.
3.3	**Владеть:**
3.3.1	– в области симметричного шифрования; формирования хеш-функций;
3.3.2	– применения асимметричных криптосистем; управления ключами в системах с открытым ключом;
3.3.3	– обеспечения безопасной работы в сети Интернет.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**4 ЗЕТ**
Часов по учебному плану : 144 в том числе : аудиторные занятия : 72 самостоятельная работа : 45 часов на контроль : 27	Виды контроля в семестрах: экзамены 9

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Основы криптографических протоколов			
1.1	Понятие криптографического протокола /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
1.2	Классификация протоколов и их примеры /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
1.3	Основы криптографических протоколов /Ср/	9	5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 2. Протоколы электронной цифровой подписи			

2.1	Криптографическая хеш-функция /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.2	Протоколы электронной цифровой подписи /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.3	Стандарты электронной цифровой подписи /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.4	Протоколы электронной цифровой подписи. Основы построения и особенности реализации /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.5	Протоколы электронной цифровой подписи. Разработка протоколов /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.6	Протоколы электронной цифровой подписи. Реализация протоколов /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.7	Протоколы электронной цифровой подписи. Коллоквиум /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.8	Протоколы электронной цифровой подписи /Ср/	9	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 3. Протоколы аутентификации			
3.1	Обзор протоколов аутентификации /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
3.2	Протоколы с нулевым разглашением /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
3.3	Стандарты протоколов аутентификации /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
3.4	Протоколы аутентификации. Основы построения и особенности реализации. /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
3.5	Протоколы аутентификации. Разработка и реализация протокола /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
3.6	Протоколы аутентификации. Коллоквиум /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
3.7	Протоколы аутентификации /Ср/	9	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 4. Протоколы распределения ключей			
4.1	Протоколы открытого распределения ключей /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
4.2	Протоколы с аутентифицированной передачей ключей /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
4.3	Протоколы предварительного распределения ключей /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
4.4	Протоколы распределения ключей. Основы построения и особенности реализации /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4

4.5	Протоколы распределения ключей. Разработка и реализация протокола /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
4.6	Протоколы распределения ключей. Коллоквиум /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
4.7	Протоколы распределения ключей /Ср/	9	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 5. Прикладные протоколы			
5.1	Прикладные протоколы /Лек/	9	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.2	Протокол IPSec /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.3	Прикладные протоколы. Основы построения и особенности реализации /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.4	Прикладные протоколы. Протокол электронной коммерции и почты /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.5	Прикладные протоколы. Протокол электронные выборы и игровые протоколы /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.6	Прикладные протоколы. TLS, SSL /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.7	Прикладные протоколы. IPSec /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.8	Прикладные протоколы /Ср/	9	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 6. Анализ уязвимостей и защита протоколов			
6.1	Управление ключами /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
6.2	Уязвимости и защита протоколов /Лек/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
6.3	Анализ уязвимостей и защита протоколов. Основы построения и особенности реализации /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
6.4	Анализ уязвимостей и защита протоколов. Разработка и реализация протокола /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
6.5	Анализ уязвимостей и защита протоколов. Коллоквиум /Пр/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
6.6	Анализ уязвимостей и защита протоколов /Ср/	9	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 7. Экзамен			
7.1	/Экзамен/	9	27	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Практические работы.
Коллоквиум.
Вопросы для экзамена.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Список теоретических вопросов к коллоквиуму:
№ п/п Формулировка вопроса
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.
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.

Список 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
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
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)
19. Общий с (1, ms, -r')
20. Общий с (ms, 1,mr')

21. Общий с (mr', 1, -s)

Практическая работа №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

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 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

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Список теоретических вопросов к экзамену:
№ п/п Формулировка вопроса
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) = Ek(x + H), f(x, H) = Ex(H), f(x, H) = EH(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.

6.4. Критерии оценивания

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
2	Экзамен (теоретический вопрос)	3x10=30
3	Итого	100

Критерии оценивания теоретического вопроса (для коллоквиума и экзамена)
Максимальный балл за ответ на теоретический вопрос – 10 баллов.
Отлично/зачтено/9-10 баллов - Обучающийся отлично знает материал, понимает терминологию криптографических протоколов. Обучающийся практически не допускает ошибок.
Хорошо/зачтено/7-8 баллов - Обучающийся хорошо знает материал, понимает терминологию криптографических протоколов. Обучающийся допускает незначительные ошибки.
Удовлетворительно/зачтено/5-6 баллов - Обучающийся знаком с материалом, владеет терминологией криптографических протоколов. Обучающийся допускает фактические ошибки.
Неудовлетворительно/незачтено/0-4 балла - 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.

Критерии оценивания практической работы
Практическая работа выполняется на любом доступном студенту языке программирования.
Максимальный балл за практическую работу – 10 баллов.
Отлично/зачтено/9-10 баллов - Практическая работа выполнена правильно, в срок, обучающийся отлично знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу.
Хорошо/зачтено/7-8 баллов - Выполнено 3/4 практической работы, обучающийся хорошо знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу, но допускает незначительные ошибки.
Удовлетворительно/зачтено/5-6 баллов - Выполнено 1/2 практической работы, либо работа сдана значительно позднее, чем предполагалось, при этом обучающийся знает материал, но допускает ошибки.
Неудовлетворительно/незачтено/0-4 балла - 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.

При подведении итогов учитываются результаты текущей аттестации. Получен-ные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации:
0 – 59 баллов – неудовлетворительно (2);
60 – 74 баллов – удовлетворительно (3);
75 – 90 баллов – хорошо (4);
91 – 100 баллов – отлично (5).

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Лапонина О. Р.	Криптографические основы безопасности (http://biblioclub.ru/index.php?page=book&id=429092)	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л1.2	Ищукова Е. А., Лобова Е. А.	Криптографические протоколы и стандарты: учебное пособие (http://biblioclub.ru/index.php?page=book&id=493059)	Таганрог : Южный федеральный университет, 2016	ЭБС
Л1.3	Фороузан Б. А.	Математика криптографии и теория шифрования (http://biblioclub.ru/index.php?page=book&id=428998)	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Шубович В. Г., Капитанчук В. В., Знаенко Н. С., Титаренко Ю. И.	Разработка моделей криптографической защиты информации: монография (http://biblioclub.ru/index.php?page=book&id=278070)	Ульяновск : Ульяновский государственный педагогический университет (УлГПУ), 2013	ЭБС
Л2.2	Зубов А. Ю.	Криптографические методы защиты информации. Совершенные шифры: Учебное пособие	М.: Гелиос АРВ, 2005	
Л2.3	Смарт Н., Кулешова С. А., Ландо С. К.	Криптография	М.: Техносфера, 2006	
Л2.4	Аграновский А. В., Хади Р. А.	Практическая криптография: алгоритмы и их программирование: учебное пособие (http://biblioclub.ru/index.php?page=book&id=117663)	Москва : СОЛОН-ПРЕСС, 2009	ЭБС

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Adobe Reader

Octave

VirtualBox

Visual Studio

Notepad++

MS Office365

7.3.2 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/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины 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.

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

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении данной дисциплины используются лекционные, практические занятия и самостоятельная работа студента. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.
На практических занятиях рассматриваются разработка и реализация протоколов электронной цифровой подписи, протоколов аутентификации, протоколов распределения ключей, прикладных протоколов, а также анализ уязвимостей и защита протоколов. Рекомендуется перед каждым практическим занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на лабораторных 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, видеохостинг YouYube, форумы, электронная почта и др.).
Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты 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 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.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.

1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «ElBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.

2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-РСМ» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.

3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.

При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации NVDA, речевые синтезаторы, экранные лупы).

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.

Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).

Учебно-методические материалы для 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 шрифтом 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.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине 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 шрифтом 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 шрифтом Брайля, с использованием услуг ассистента, устно).
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. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.
Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.