МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль) / специализация: **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, Кафедра безопасности информационных систем**
Курс: **3**
Семестр: **6**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	6 семестр	Всего	Единицы
1	Лекции	30	30	часов
2	Практические занятия	30	30	часов
3	Всего аудиторных занятий	60	60	часов
4	Самостоятельная работа	48	48	часов
5	Всего (без экзамена)	108	108	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 6 семестр

Томск

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от «26» 11 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.04 Информационно-аналитические системы безопасности, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры БИС «___» _____ 20__ года, протокол №_____.

Разработчик:

И.о. зав. кафедрой каф. БИС _____ Е. Ю. Костюченко

Заведующий обеспечивающей каф. БИС _____ Е. Ю. Костюченко

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Д. В. Кручинин

Заведующий выпускающей каф. БИС _____ Е. Ю. Костюченко

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. А. Конев

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ К. С. Сарин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины «Криптографические методы защиты информации» является формирование у студентов общих представлений о криптографических методах защиты информации, о применении криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности и об основных принципах, лежащих в основе функционирования криптографических средств защиты информации.

1.2. Задачи дисциплины

- дать представление о криптографических методах защиты информации;
- изучить математические основы современной криптографии;
- изучить современные стандарты симметричного шифрования;
- изучить основные криптографические алгоритмы с открытым ключом;
- изучить криптографические функции хеширования;
- сформировать умение применять полученные знания для компьютерной реализации криптографических алгоритмов.

2. Место дисциплины в структуре ОПОП

Дисциплина «Криптографические методы защиты информации» (Б1.Б.03.09) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра, Теория вероятностей и математическая статистика.

Последующими дисциплинами являются: Прикладная криптография.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-2 способностью корректно применять аппарат математического анализа, геометрии, алгебры, дискретной математики, теории вероятностей, математической статистики, численных методов, методов оптимизации для формализации и решения задач в сфере профессиональной деятельности;

В результате изучения дисциплины обучающийся должен:

- **знать** основные виды криптографических методов и алгоритмов; принципы построения криптографических алгоритмов и предъявляемые к ним требования; математические основы современной криптографии; криптографические стандарты и их использование в информационных системах; простейшие методы криптоанализа
- **уметь** эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; применять простейшие методы криптоанализа.
- **владеть** криптографическими методами и средствами защиты информации; простейшими методами криптоанализа; методами оценки стойкости криптографических алгоритмов.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		6 семестр
Аудиторные занятия (всего)	60	60
Лекции	30	30
Практические занятия	30	30
Самостоятельная работа (всего)	48	48

Проработка лекционного материала	36	36
Подготовка к практическим занятиям, семинарам	12	12
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	144	144
Зачетные Единицы	4.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
6 семестр					
1 Математические основы криптографии	2	16	9	27	ОПК-2
2 Основные цели и задачи криптографии	4	0	4	8	ОПК-2
3 Историческая криптография	2	4	6	12	ОПК-2
4 Симметричное шифрование	6	2	7	15	ОПК-2
5 Хеширование	2	0	4	6	ОПК-2
6 Поточное шифрование	2	0	3	5	ОПК-2
7 ГСПЧ и проверка их качества	2	0	3	5	ОПК-2
8 Криптография с открытым ключом	4	8	6	18	ОПК-2
9 Электронная подпись	4	0	3	7	ОПК-2
10 Протоколы	2	0	3	5	ОПК-2
Итого за семестр	30	30	48	108	
Итого	30	30	48	108	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
6 семестр			
1 Математические основы криптографии	Криптографические методы защиты информации: шифрование, хеширование, электронная подпись.	2	ОПК-2
	Итого	2	
2 Основные цели и задачи криптографии	Алгебраические структуры. Группы. Циклические группы. Кольца, кольца классов вычетов. Конечные поля. Поля Галуа. Эллиптические кривые. Понятие наибольшего общего делителя. Алгоритм Ев-	4	ОПК-2

	клида, расширенный алгоритм Евклида. Сравнение первой степени с одним неизвестным. Китайская теорема об остатках. Генерация простых чисел. Тест на простоту. Алгоритмы работы с большими числами.		
	Итого	4	
3 Историческая криптография	Математическая модель шифра. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования.	2	ОПК-2
	Итого	2	
4 Симметричное шифрование	DES. ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. Режимы шифрования, эммитовставка. AES.	6	ОПК-2
	Итого	6	
5 Хеширование	Криптографические хеш-функции. ГОСТ Р 34.11- 2012. SHA-3.	2	ОПК-2
	Итого	2	
6 Поточное шифрование	Принципы поточного шифрования. Типы поточного шифрования. Синхронные и самосинхронизирующиеся шифры. Шифр RC-4 как пример поточного алгоритма шифрования.	2	ОПК-2
	Итого	2	
7 ГСПЧ и проверка их качества	Генерация случайных чисел. Псевдослучайные числа и их отличия от истинно случайных чисел. Подходы к получению псевдослучайных чисел. Критерии качества псевдослучайных чисел. Виды тестов псевдослучайных последовательностей. Тесты NIST.	2	ОПК-2
	Итого	2	
8 Криптография с открытым ключом	Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистема Рабина.	4	ОПК-2
	Итого	4	
9 Электронная подпись	Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. DSS.Инфраструктура открытого ключа.	4	ОПК-2
	Итого	4	
10 Протоколы	Протокол раздельного вручения бита. Протоколы доказательства знания с нулевым разглашением. Протоколы простановки "слепых" подписей. Протоколы голосования. Протоколы безопасных вычислений.	2	ОПК-2

	Итого	2	
Итого за семестр		30	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин									
	1	2	3	4	5	6	7	8	9	10
Предшествующие дисциплины										
1 Алгебра	+	+	+	+	+	+	+	+	+	+
2 Теория вероятностей и математическая статистика	+			+	+	+	+	+	+	
Последующие дисциплины										
1 Прикладная криптография	+	+	+	+	+	+	+	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Прак. зан.	Сам. раб.	
ОПК-2	+	+	+	Экзамен, Опрос на занятиях, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
6 семестр			
1 Математические основы криптографии	Алгебраические структуры. Группы. Циклические группы.	4	ОПК-2
	Кольца, кольца классов вычетов.	4	
	Конечные поля, поля Галуа.	4	
	Теоретико-числовые алгоритмы, используемые в криптографии	4	
	Итого	16	

3 Историческая криптография	Простейшие шифры и их криптоанализ.	4	ОПК-2
	Итого	4	
4 Симметричное шифрование	Современные симметричные шифры	2	ОПК-2
	Итого	2	
8 Криптография с открытым ключом	Протокол Диффи-Хеллмана	2	ОПК-2
	Криптосистема RSA	2	
	Криптосистема Эль-Гамаля	2	
	Криптосистема Рабина	2	
	Итого	8	
Итого за семестр		30	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
6 семестр				
1 Математические основы криптографии	Подготовка к практическим занятиям, семинарам	5	ОПК-2	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	4		
	Итого	9		
2 Основные цели и задачи криптографии	Проработка лекционного материала	4	ОПК-2	Опрос на занятиях, Тест, Экзамен
	Итого	4		
3 Историческая криптография	Подготовка к практическим занятиям, семинарам	2	ОПК-2	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	4		
	Итого	6		
4 Симметричное шифрование	Подготовка к практическим занятиям, семинарам	2	ОПК-2	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	5		
	Итого	7		
5 Хеширование	Проработка лекционного материала	4	ОПК-2	Опрос на занятиях, Тест, Экзамен
	Итого	4		
6 Поточное шифрование	Проработка лекционного материала	3	ОПК-2	Опрос на занятиях, Тест, Экзамен

	Итого	3		
7 ГСПЧ и проверка их качества	Проработка лекционного материала	3	ОПК-2	Опрос на занятиях, Тест, Экзамен
	Итого	3		
8 Криптография с открытым ключом	Подготовка к практическим занятиям, семинарам	3	ОПК-2	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	3		
	Итого	6		
9 Электронная подпись	Проработка лекционного материала	3	ОПК-2	Опрос на занятиях, Тест, Экзамен
	Итого	3		
10 Протоколы	Проработка лекционного материала	3	ОПК-2	Опрос на занятиях, Тест, Экзамен
	Итого	3		
Итого за семестр		48		
	Подготовка и сдача экзамена	36		Экзамен
Итого		84		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
6 семестр				
Опрос на занятиях	5	5	10	20
Отчет по практическому занятию	15	10	15	40
Тест			10	10
Итого максимум за период	20	15	35	70
Экзамен				30
Нарастающим итогом	20	35	70	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5

От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] [Электронный ресурс]: монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линияТелеком, 2016. — 232 с. — Загл. с экрана. — Режим доступа: https://e.lanbook.com/book/111098 (дата обращения: 12.02.2021).

12.2. Дополнительная литература

1. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 479 [1] с. (наличие в библиотеке ТУСУР - 30 экз.)

2. Основы современной криптографии: учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — 2-е изд., перераб. и доп. — М.: Горячая линия-Телеком, 2002. — 176 с. (наличие в библиотеке ТУСУР - 51 экз.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации [Электронный ресурс]: методические указания для выполнения практических и самостоятельных работ — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf (дата обращения: 12.02.2021).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

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

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. https://lib.tusur.ru/
2. https://edu.tusur.ru/
3. Рекомендуется использовать информационные, справочные и нормативные базы данных https://lib.tusur.ru/ru/resursy/bazy-dannyh

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория электротехники, электроники и схемотехники / Лаборатория измерений в телекоммуникационных системах

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 404 ауд.

Описание имеющегося оборудования:

- Доска TraceBoard TS-408L;
- Мультимедийный проектор ViewSonic PJD5154 DLP;
- Компьютеры: GigaByte GA-F2A68HM-DS2 rev1.0 (RTL) / AMD A4-6300 / DDR-III 8Gb/ HDD 1Tb / мышь/ клавиатура/ монитор (10шт.);
- Компьютер: Intel Core i3/ DDR3 4G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;

Стенды для исследования параметров сетевого трафика, включающие:

- структурированную кабельную систему, объединяющую компьютеры аудитории в локальную вычислительную сеть;
- средства анализа сетевого трафика и углубленной проверки сетевых пакетов: анализатор трафика Wireshark, дистрибутив Kali Linux;

Комплексы для создания элементов телекоммуникационных систем на базе:

- одноплатных компьютеров Milestone M-100
- отладочных плат K1986BE92QI;
- отладочных плат Genuino 101$
- платы расширения для организации линий связи посредством: Ethernet, Wi-Fi, GSM, bluetooth, и т.д;

Комплект измерительного оборудования в составе:

- Анализатор кабельных сетей MI 2016 Multi LAN 350;
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2.

Учебно-лабораторные стенды для измерения частотных свойств, форм и временных характеристик сигнала включающие:

- "Исследование законов Ома и Кирхгофа при гармоническом воздействии";
- "Исследование разветвленных цепей переменного тока";
- "Исследование разветвленных цепей постоянного тока";
- "Исследование цепи постоянного тока с одним источником";
- "Резонанс в последовательном колебательном контуре";

- "Резонанс в параллельном колебательном контуре";
- "Исследование разветвленных цепей и магнитосвязанных индуктивностей";
- "Исследование RC-фильтров";
- “Исследование переходных процессов в цепях первого и второго порядков";
- "Исследование длинной линии в стационарном и переходном режимах";

Контрольно-измерительная аппаратура для измерения параметров электрических цепей, частотных свойств, форм и временных характеристик сигналов, исследования параметров телекоммуникационных систем:

- осциллограф универсальный С1-120;
- осциллограф С1-68;
- измерительный блок с мультиметрами UT50C, UT50D и фазометром;
- милливольтметр В3-38;
- вольтметр универсальный В7-26;
- анализатор спектра GW Instek GSP-7730;

DS1052E Цифровой осциллограф, MSO2072A-S Цифровой осциллограф MSO2072A с опцией встроенного генератора.

генератор импульсов ГП-15; генератор UNI-T UTG9002C;

Учебно-лабораторные стенды для изучения работы компонентов узлов и блоков вычислительных устройств на базе отладочных комплектов для микроконтроллеров фирмы Миландр:

- 1886ВЕ5БУ;
- MDR32 F2QI;
- 1901BYIT;
- 1986VE91;
- 1967BYIT;

Отладчики стандарта IEEE 1149. (JTAG) типа J-Link (8 шт.);

Рабочие места разработчиков систем и устройств в системах автоматизированного проектирования:

- NetBeans IDE;
- Arduino IDE;
- LTspice.

3D принтер Felix 3.0 (1 шт.);

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;

- 7-Zip;
- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. Какой криптографический метод защиты информации предназначен для обеспечения конфиденциальности информации?
а) Хеширование
б) Электронная подпись
в) Шифрование
г) Коды аутентичности сообщений
2. Для решения какой задачи обеспечения информационной безопасности предназначено хеширование?
а) Обеспечение конфиденциальности информации
б) Обеспечение неотказуемости
в) Обеспечение контроля целостности данных
г) Проверка подлинности источника данных
3. Каким свойством обладают элементы a и a^-1 в кольце классов вычетов по модулю n?
а) a·a^-1 = 0 (mod n)
б) a·a^-1 = –1 (mod n)
в) a·a^-1 = 1 (mod n)
г) a·a^-1 = n (mod n)
4. В каком случае существует значение a^-1 по модулю n?
а) Если a делит n
б) Если n делит a
в) Если НОД(a, n) = 1
г) Если НОД(a, n) > 1
5. Поставьте в соответствие двоичной последовательности 11001101 элемент поля Галуа GF(28), в виде которого можно представить данную последовательность для проведения над ней криптографических преобразований.
а) x^8 + x^7 + x^4 + x^3 + x
б) x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1

в) x^7 + x^6 + x^3 + x^2 + 1
г) x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1
6. Чем шифр «Магма» отличается от шифра, определенного в стандарте ГОСТ 28147-89?
а) Длиной ключа
б) Это два принципиально разных симметричных блочных шифра
в) Невозможностью использования произвольной таблицы замен
г) Количеством раундов
7. Какова длина секретного ключа в шифре «Кузнечик»?
а) 64 бита
б) 128 бит
в) 256 бит
г) 512 бит
8. Какой из режимов работы симметричных блочных шифров не предназначен для обеспечения конфиденциальности информации?
а) Режим простой замены
б) Режим простой замены с зацеплением
в) Режим выработки имитовставки
г) Режим гаммирования
9. В каком из режимов работы симметричных блочных шифров результат зашифрования очередного блока открытого текста при фиксированном ключе зависит только от порядкового номера данного блока?
а) Режим простой замены
б) Режим гаммирования с обратной связью по выходу
в) Режим гаммирования
г) Режим гаммирования с обратной связью по шифртексту
10. Какой из перечисленных шифров относится к классу асимметричных шифров?
а) Магма
б) Кузнечик
в) RSA
г) AES
11. В чем заключается различие между симметричными и асимметричными криптосистемами?
а) В решаемых задачах защиты информации
б) В показателях криптографической стойкости
в) В количестве и назначении используемых ключей
г) Принципиальных различий нет
12. Почему асимметричные криптосистемы затруднительно использовать для непосредственного шифрования видеотрафика?
а) В связи с недостаточной криптографической стойкостью асимметричных криптосистем
б) В связи с отсутствием соответствующих стандартов
в) В связи с недостаточным быстродействием асимметричных криптосистем
г) Асимметричные криптосистемы используются для непосредственного шифрования видеотрафика
13. Сопоставьте действующие отечественные криптографические стандарты с перечисленными криптографическими методами защиты информации в порядке их перечисления: шифрование, хеширование, электронная подпись.
а) ГОСТ Р 34.12–2015, ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012
б) ГОСТ 28147-89, ГОСТ Р 34.11–2012, ГОСТ Р 34.10–2012
в) ГОСТ Р 34.12–2015, ГОСТ Р 34.11–2012, ГОСТ Р 34.10–2012
г) ГОСТ Р 34.12–2015, ГОСТ Р 34.11–94, ГОСТ Р 34.10–2012
14. На какой вычислительной задаче основана криптосистема RSA?
а) Нахождение наибольшего общего делителя
б) Вычисление модулярно обратного элемента
в) Целочисленная факторизация

г) Дискретное логарифмирование

15. На каком математическом аппарате основана схема электронной подписи, определенная в стандарте ГОСТ Р 34.10–2012?

а) Кольца классов вычетов

б) Поля Галуа

в) Эллиптические кривые

г) Матричные группы

16. Чем код аутентичности отличается от хеш-кода?

а) Это синонимы

б) Хеш-код рассчитывается с использованием секретного ключа, а код аутентичности — без использования секретного ключа

в) Код аутентичности рассчитывается с использованием секретного ключа, а хеш-код — без использования секретного ключа

г) Код аутентичности рассчитывается с использованием закрытого ключа, а хеш-код — с использованием открытого ключа

17. Чем код аутентичности отличается от электронной подписи?

а) Это синонимы

б) Длиной ключа

в) Электронная подпись обеспечивает неотказуемость, а код аутентичности — нет

г) Электронная подпись обеспечивает возможность проверки подлинности источника данных, а код аутентичности — нет

18. Для чего в схемах электронной подписи используются функции хеширования?

а) Для повышения криптографической стойкости схемы электронной подписи

б) Для обеспечения контроля целостности подписываемого сообщения

в) Для представления подписываемого сообщения произвольной длины в виде строки данных фиксированной длины

г) Для представления подписанного сообщения произвольной длины в виде строки данных фиксированной длины

19. Чем схема электронной подписи, определенная в стандарте ГОСТ Р 34.10-2012, отличается от схемы электронной подписи, определенной в стандарте ГОСТ Р 34.10-2001?

а) Перечнем решаемых задач

б) Используемым математическим аппаратом

в) Длиной подписи

г) Ничем не отличается

20. Что является основной проблемой криптографии с открытым ключом?

а) Обеспечение аутентичности закрытых ключей

б) Обеспечение конфиденциальности закрытых ключей

в) Обеспечение аутентичности открытых ключей

г) Обеспечение конфиденциальности открытых ключей

14.1.2. Экзаменационные вопросы

1. Алгебраические структуры. Свойства алгебраических структур. Группы, подгруппы.
2. Циклические группы.
3. Кольца. Кольца классов вычетов.
4. Поля. Поля Галуа.
5. Цели и задачи криптографии. Основные понятия.
6. Простейшие шифры: простой замены, перестановочный, аффинный.
7. Шифр Хилла.
8. Генерация простых чисел.
9. Шифры гаммирования. Шифр Вернама (одноразовый блокнот).
10. ГОСТ Р 34.12-2015. Шифр «Магма».
11. ГОСТ Р 34.12-2015. Шифр «Кузнечик».
12. Генерация псевдослучайных последовательностей и их тесты.
13. Поточное шифрование.
14. Стандарт шифрования DES.

15. Стандарт шифрования AES.
16. Криптография с открытым ключом.
17. Ранцевая криптосистема.
18. Криптосистема RSA.
19. Криптосистема Эль-Гамаля.
20. Протокол Диффи-Хеллмана.
21. Алгоритмы работы с большими числами.
22. Хеш-функции. Свойства хеш-функций.
23. Коды аутентичности сообщений. Электронная подпись.
24. ГОСТ Р 34.10-2012.
25. Протокол передачи бита.
26. Слепые подписи.
27. Протоколы доказательств знания с нулевым разглашением.
28. Протоколы электронного голосования.
29. Протоколы безопасных вычислений.

14.1.3. Темы опросов на занятиях

Криптографические методы защиты информации: шифрование, хеширование, электронная подпись.

Алгебраические структуры. Группы. Циклические группы. Кольца, кольца классов вычетов. Конечные поля. Поля Галуа. Эллиптические кривые. Понятие наибольшего общего делителя. Алгоритм Евклида, расширенный алгоритм Евклида. Сравнение первой степени с одним неизвестным. Китайская теорема об остатках. Генерация простых чисел. Тест на простоту. Алгоритмы работы с большими числами.

Математическая модель шифра. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования.

DES. ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. Режимы шифрования, эммитовставка. AES.

Криптографические хеш-функции. ГОСТ Р 34.11- 2012. SHA-3.

Принципы поточного шифрования. Типы поточного шифрования. Синхронные и самосинхронизирующиеся шифры. Шифр RC-4 как пример поточного алгоритма шифрования.

Генерация случайных чисел. Псевдослучайные числа и их отличия от истинно случайных чисел. Подходы к получению псевдослучайных чисел. Критерии качества псевдослучайных чисел. Виды тестов псевдослучайных последовательностей. Тесты NIST.

Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистема Рабина.

Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. DSS.

Инфраструктура открытого ключа.

Протокол раздельного вручения бита. Протоколы доказательства знания с нулевым разглашением. Протоколы простановки "слепых" подписей. Протоколы голосования. Протоколы безопасных вычислений.

14.1.4. Вопросы для подготовки к практическим занятиям, семинарам

Алгебраические структуры. Группы. Циклические группы.

Кольца, кольца классов вычетов.

Конечные поля, поля Галуа.

Теоретико-числовые алгоритмы, используемые в криптографии

Простейшие шифры и их криптоанализ.

Современные симметричные шифры

Протокол Диффи-Хеллмана

Криптосистема RSA

Криптосистема Эль-Гамаля

Криптосистема Рабина

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

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

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.