МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, Кафедра безопасности информационных систем**
Курс: **3**
Семестр: **5**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	Всего	Единицы
1	Лекции	36	36	часов
2	Практические занятия	28	28	часов
3	Всего аудиторных занятий	64	64	часов
4	Из них в интерактивной форме	18	18	часов
5	Самостоятельная работа	44	44	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 5 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 23.08.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск 2018

Согласована на портале № 29204

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 15 » 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 16.11.2016 года, рассмотрена и одобрена на заседании кафедры БИС «___» _____ 20__ года, протокол №_____.

Разработчик:

Доцент каф. БИС _____ О. О. Евсютин

Заведующий обеспечивающей каф. БИС _____ Р. В. Мещеряков

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. БИС _____ Р. В. Мещеряков

Эксперты:

Доцент каф. БИС _____ А. Ю. Исхаков

Доцент каф. КИБЭВС _____ К. С. Сарин

Согласована на портале № 29204

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.10) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра, Геометрия, Дискретная математика, Информатика, Основы информационной безопасности.

Последующими дисциплинами являются: Прикладная криптография.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач;

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
		5 семестр
Аудиторные занятия (всего)	64	64
Лекции	36	36
Практические занятия	28	28
Из них в интерактивной форме	18	18
Самостоятельная работа (всего)	44	44
Выполнение индивидуальных заданий	20	20
Проработка лекционного материала	10	10

Согласована на портале № 29204

Подготовка к практическим занятиям, семинарам	14	14
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	Ле к., ч	ра к. за	м. ра б.,	в (б ез	ир уе м ые ко м
5 семестр					
1 Основные цели и задачи криптографии	2	0	1	3	ОПК-2
2 Математические основы криптографии	8	8	8	24	ОПК-2
3 Историческая криптография	2	4	5	11	ОПК-2
4 Симметричное шифрование	8	2	4	14	ОПК-2
5 Хеширование	4	0	1	5	ОПК-2
6 Криптография с открытым ключом	8	8	4	20	ОПК-2
7 Электронная подпись	4	0	1	5	ОПК-2
8 Защита индивидуальных заданий	0	6	20	26	ОПК-2
Итого за семестр	36	28	44	108	
Итого	36	28	44	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	ое мк ос	м ые ко
5 семестр			
1 Основные цели и задачи криптографии	Криптографические методы защиты информации: шифрование, хеширование, электронная подпись.	2	ОПК-2
	Итого	2	
2 Математические основы криптографии	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.	8	ОПК-2
	Итого	8	
3 Историческая криптография	Математическая модель шифра. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования.	2	ОПК-2
	Итого	2	
4 Симметричное	ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р	8	ОПК-2

Согласована на портале № 29204

шифрование	34.13-2015. DES. AES.		
	Итого	8	
5 Хеширование	Криптографические хеш-функции. ГОСТ Р 34.11-2012. SHA-3.	4	ОПК-2
	Итого	4	
6 Криптография с открытым ключом	Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистема Рабина. Алгоритмы работы с большими числами.	8	ОПК-2
	Итого	8	
7 Электронная подпись	Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. DSS. Инфраструктура открытого ключа.	4	ОПК-2
	Итого	4	
Итого за семестр		36	

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
Предшествующие дисциплины								
1 Алгебра		+						
2 Геометрия		+						
3 Дискретная математика		+						
4 Информатика								+
5 Основы информационной безопасности	+							
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.	Практ. зан.	Самост. раб.	
ОПК-2	+	+	+	Домашнее задание, Отчет по индивидуальному заданию, Экзамен, Защита отчета, Опрос на занятиях, Тест

6. Интерактивные методы и формы организации обучения

Согласована на портале № 29204

Технологии интерактивного обучения при разных формах занятий приведены в таблице 6.1.

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий

Методы	Интерактивные практические занятия, ч	Интерактивные лекции, ч	Всего, ч
5 семестр			
Мини-лекция	8		8
Презентации с использованием слайдов с обсуждением		10	10
Итого за семестр:	8	10	18
Итого	8	10	18

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
5 семестр			
2 Математические основы криптографии	Алгебраические структуры. Группы. Циклические группы.	2	ОПК-2
	Кольца, кольца классов вычетов.	2	
	Конечные поля, поля Галуа.	2	
	Теоретико-числовые алгоритмы, используемые в криптографии	2	
	Итого	8	
3 Историческая криптография	Простейшие шифры и их криптоанализ.	4	ОПК-2
	Итого	4	
4 Симметричное шифрование	Современные симметричные шифры	2	ОПК-2
	Итого	2	
6 Криптография с открытым ключом	Протокол Диффи-Хеллмана	2	ОПК-2
	Криптосистема RSA	2	
	Криптосистема Эль-Гамаля	2	
	Криптосистема Рабина	2	
	Итого	8	
8 Защита индивидуальных заданий	Защита индивидуального задания по теме «Программная реализация простейшего шифра»	2	ОПК-2
	Защита индивидуального задания по теме «Программная реализация симметричного шифра»	2	
	Защита индивидуального задания по теме «Программная реализация асимметричного шифра»	2	
	Итого	6	
Итого за семестр		28	

Согласована на портале № 29204

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,	Формируемые комп	Формы контроля
5 семестр				
1 Основные цели и задачи криптографии	Проработка лекционного материала	1	ОПК-2	Опрос на занятиях, Экзамен
	Итого	1		
2 Математические основы криптографии	Подготовка к практическим занятиям, семинарам	6	ОПК-2	Домашнее задание, Опрос на занятиях, Экзамен
	Проработка лекционного материала	2		
	Итого	8		
3 Историческая криптография	Подготовка к практическим занятиям, семинарам	4	ОПК-2	Домашнее задание, Защита отчета, Отчет по индивидуальному заданию, Экзамен
	Проработка лекционного материала	1		
	Итого	5		
4 Симметричное шифрование	Подготовка к практическим занятиям, семинарам	2	ОПК-2	Домашнее задание, Защита отчета, Опрос на занятиях, Отчет по индивидуальному заданию, Экзамен
	Проработка лекционного материала	2		
	Итого	4		
5 Хеширование	Проработка лекционного материала	1	ОПК-2	Опрос на занятиях, Экзамен
	Итого	1		
6 Криптография с открытым ключом	Подготовка к практическим занятиям, семинарам	2	ОПК-2	Домашнее задание, Защита отчета, Опрос на занятиях, Отчет по индивидуальному заданию, Экзамен
	Проработка лекционного материала	2		
	Итого	4		
7 Электронная подпись	Проработка лекционного материала	1	ОПК-2	Опрос на занятиях, Экзамен
	Итого	1		
8 Защита индивидуальных заданий	Выполнение индивидуальных заданий	20	ОПК-2	Защита отчета, Отчет по индивидуальному заданию, Экзамен
	Итого	20		
Итого за семестр		44		

Согласована на портале № 29204

	Подготовка и сдача экзамена	36		Экзамен
Итого		80		

10. Курсовая работа (проект)

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
5 семестр				
Домашнее задание	5	5		10
Защита отчета	10	10	10	30
Опрос на занятиях	2	2	1	5
Отчет по индивидуальному заданию	5	5	5	15
Тест			10	10
Итого максимум за период	22	22	26	70
Экзамен				30
Нарастающим итогом	22	44	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)

Согласована на портале № 29204

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] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2016. — 232 с. — Режим доступа: https://e.lanbook.com/book/111098. — Загл. с экрана. [Электронный ресурс] - Режим доступа: https://e.lanbook.com/book/111098, дата обращения: 29.05.2018.

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: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf, дата обращения: 03.06.2018.

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://edu.tusur.ru/ – Научно-образовательный портал ТУСУР.
2. http://fgosvo.ru – Портал Федеральных государственных образовательных стандартов высшего образования.
3. eLIBRARY.RU – Российская научная электронная библиотека, интегрированная с Российским индексом научного цитирования (РИНЦ).
4. Scopus – библиографическая и реферативная база данных.
5. SpringerLink – хранилище электронных копий научных книг и журналов, издаваемых компанией Springer.
6. IEEE Xplore – электронная платформа, содержащая полные тексты публикаций из журналов, материалов конференций, стандартов, издаваемых IEEE и IEE (Institution of Electrical Engineers).

Согласована на портале № 29204

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 программно-аппаратных средств обеспечения информационной безопасности

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

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 405 ауд.

Описание имеющегося оборудования:

- Компьютеры класса не ниже M/B ASUSTeK S-775 P5B i965 / Core 2 Duo E6300 / DDR-II DIMM 2048 Mb / Sapphire PCI-E Radeon 256 Mb / 160 Gb Seagate (15 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Microsoft Windows 7 Pro
- VirtualBox
- Visual Studio
- Криптографическое средство защиты информации КриптоПро CSP

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.

Согласована на портале № 29204

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) $a \cdot a^{-1} = 0 \pmod{n}$
б) $a \cdot a^{-1} = -1 \pmod{n}$
в) $a \cdot a^{-1} = 1 \pmod{n}$
г) $a \cdot a^{-1} = n \pmod{n}$

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 $GF(2^8)$, 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) $x^7 + x^6 + x^3 + x^2 + 1$

Согласована на портале № 29204

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.

Согласована на портале № 29204

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

Согласована на портале № 29204

г) Обеспечение конфиденциальности открытых ключей

14.1.2. Экзаменационные вопросы

Теоретические вопросы:

1. Алгебраические структуры. Свойства алгебраических структур. Группы, подгруппы.
2. Циклические группы.
3. Группы подстановок.
4. Кольца. Кольца классов вычетов.
5. Поля. Поля Галуа.
6. Эллиптические кривые над конечным полем.
7. Цели и задачи криптографии. Основные понятия.
8. Простейшие шифры: простой замены, перестановочный, аффинный.
9. Шифр Хилла.
10. Шифры гаммирования. Шифр Вернама.
11. ГОСТ Р 34.12-2015. Шифр «Магма».
12. ГОСТ Р 34.12-2015. Шифр «Кузнечик».
13. ГОСТ Р 34.13-2015. Режимы гаммирования.
14. ГОСТ Р 34.13-2015. Режимы простой замены, режим выработки имитовставки.
15. Стандарт шифрования DES.
16. Стандарт шифрования AES.
17. Криптография с открытым ключом.
18. Криптосистема RSA.
19. Криптосистема Эль-Гамаля.
20. Протокол Диффи-Хеллмана.
21. Алгоритмы работы с большими числами.
22. Хеш-функции. Свойства хеш-функций.
23. ГОСТ Р 34.11-2012.
24. Коды аутентичности сообщений. Электронная подпись.
25. ГОСТ Р 34.10-2012.

Практические задачи:

1. Изучить свойства данной алгебраической структуры.
2. Пусть G — циклическая группа порядка n с образующим x. Найти все образующие и все подгруппы данной группы.
3. Исследовать кольцо классов вычетов по модулю n.
4. Построить поле Галуа посредством неприводимого многочлена f(x). Найти образующий элемент мультипликативной группы поля.
5. Построить группу точек эллиптической кривой над полем Галуа GF(q) для данных значений параметров a, b.
6. Записать целочисленную линейную комбинацию чисел a и b.
7. Дано сообщение M. Зашифровать его с помощью данного шифра.
8. Дано сообщение M. Сформировать электронную подпись для данного сообщения по ГОСТ Р 34.10-2012, используя данные параметры эллиптической кривой.

14.1.3. Темы домашних заданий

1. Исследовать все свойства данной алгебраической структуры.
2. Исследовать данное кольцо классов вычетов.
3. Исследовать данное поле Галуа.
4. Исследовать данное группу точек эллиптической кривой.
5. Зашифровать данный открытый текст указанным шифром.

14.1.4. Темы опросов на занятиях

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

Алгебраические структуры. Группы. Циклические группы. Кольца, кольца классов вычетов.

Согласована на портале № 29204

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.

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

ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. DES. AES.

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

Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистема Рабина. Алгоритмы работы с большими числами.

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

14.1.5. Темы индивидуальных заданий

1. Программная реализация простейшего шифра.
2. Программная реализация симметричного шифра.
3. Программная реализация асимметричного шифра

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;

Согласована на портале № 29204

– 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.

Согласована на портале № 29204