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 протоколы и стандарты

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Специализация: **Экономико-правовое обеспечение экономической безопасности**
Направленность (профиль): **Регламентация работы персонала организации при обеспечении экономической и информационной безопасности**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4, 5**
Семестр: **8, 9**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	9 семестр	Всего	Единицы
1	Лекции	2	4	6	часов
2	Лабораторные работы	4	8	12	часов
3	Всего аудиторных занятий	6	12	18	часов
4	Из них в интерактивной форме	2	4	6	часов
5	Самостоятельная работа	66	56	122	часов
6	Всего (без экзамена)	72	68	140	часов
7	Подготовка и сдача зачета	0	4	4	часов
8	Общая трудоемкость	72	72	144	часов
				4.0	З.Е.

Контрольные работы: 9 семестр - 1
Зачет: 9 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 № 29513

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) 38.05.01 Экономическая безопасность, утвержденного 16.01.2017 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

Доцент каф. КИБЭВС _____ А. А. Конев

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ЗиВФ _____ И. В. Осипов

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент каф. КИБЭВС _____ К. С. Сарин

Доцент каф. БИС _____ О. О. Евсютин

Согласована на портале № 29513

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Основная цель дисциплины «Прикладная криптография» — формирование у студентов представлений о практическом использовании криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности.

1.2. Задачи дисциплины

– сформировать представление об основных проблемах, связанных с практическим использование криптографических методов защиты информации; изучить основные криптографические протоколы; изучить инфраструктуру открытого ключа.

2. Место дисциплины в структуре ОПОП

Дисциплина «Криптографические протоколы и стандарты» (Б1.В.ДВ.5.2) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Основы информационной безопасности, Криптографические протоколы и стандарты.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Преддипломная практика, Криптографические протоколы и стандарты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-20 способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;

В результате изучения дисциплины обучающийся должен:

– **знать** основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях.

– **уметь** эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах.

– **владеть** навыками использования типовых 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	
		8 семестр	9 семестр
Аудиторные занятия (всего)	18	6	12
Лекции	6	2	4
Лабораторные работы	12	4	8
Из них в интерактивной форме	6	2	4
Самостоятельная работа (всего)	122	66	56
Подготовка к контрольным работам	61	33	28
Оформление отчетов по лабораторным работам	61	33	28
Всего (без экзамена)	140	72	68
Подготовка и сдача зачета	4	0	4
Общая трудоемкость, ч	144	72	72
Зачетные Единицы	4.0		

Согласована на портале № 29513

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	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
8 семестр					
1 Криптографические протоколы: общие понятия.	1	2	34	37	ПК-20
2 Протоколы распределения ключей.	1	2	32	35	ПК-20
Итого за семестр	2	4	66	72	
9 семестр					
3 Инфраструктура открытого ключа.	1	2	14	17	ПК-20
4 Практические аспекты реализации средств криптографической защиты информации.	1	2	14	17	ПК-20
5 Протокол идентификации и аутентификации	1	2	14	17	ПК-20
6 Безопасный канал обмена сообщениями	1	2	14	17	ПК-20
Итого за семестр	4	8	56	68	
Итого	6	12	122	140	

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
8 семестр			
1 Криптографические протоколы: общие понятия.	Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоколы.	1	ПК-20
	Итого	1	
2 Протоколы распределения ключей.	Управление секретными ключами. Распределение секретных ключей.	1	ПК-20
	Итого	1	
Итого за семестр		2	
9 семестр			
3 Инфраструктура	Понятие электронной подписи. Управление откры-	1	ПК-20

Согласована на портале № 29513

открытого ключа.	тыми ключами. Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытого ключа.		
	Итого	1	
4 Практические аспекты реализации средств криптографической защиты информации.	Проблемы реализации криптографических алгоритмов. Генерация случайных чисел. Защита от утечки информации.	1	ПК-20
	Итого	1	
5 Протокол идентификации и аутентификации	Общие сведения.Парольная идентификация/аутентификация.Протокол идентификации/аутентификации с использованием хеш-функции.Протокол идентификации/аутентификации на основе шифрования с открытым ключом.Сервер аутентификации Kerberos.Идентификация/аутентификация с помощью биометрических данных.Идентификационные карты и электронные ключи.	1	ПК-20
	Итого	1	
6 Безопасный канал обмена сообщениями	ЗащищенныесообщенияДля пересылки защищенных сообщений разработан криптографический протокол OTR (Off-the-Record). Для создания сильного шифрования протокол использует комбинацию алгоритмов AES, симметричного ключа, алгоритма Диффи — Хеллмана и хеш-функции SHA-1.	1	ПК-20
	Итого	1	
Итого за семестр		4	
Итого		6	

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
Предшествующие дисциплины						
1 Основы информационной безопасности	+					
2 Криптографические протоколы и стандарты	+	+	+	+	+	+
Последующие дисциплины						
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	+	+

Согласована на портале № 29513

3 Криптографические протоколы и стандарты	+	+	+	+	+	+

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.	Лаб. раб.	Сам. раб.	
ПК-20	+	+	+	Контрольная работа, Конспект самоподготовки, Отчет по лабораторной работе, Опрос на занятиях, Тест

6. Интерактивные методы и формы организации обучения

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

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий

Методы	Интерактивные лабораторные занятия, ч	Интерактивные лекции, ч	Всего, ч
8 семестр			
Презентации с использованием слайдов с обсуждением	1		1
Презентации с использованием мультимедиа с обсуждением	1		1
Итого за семестр:	2	0	2
9 семестр			
Презентации с использованием слайдов с обсуждением	1	1	2
Презентации с использованием мультимедиа с обсуждением	1	1	2
Итого за семестр:	2	2	4
Итого	4	2	6

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Криптографические протоколы: общие понятия.	Установка и настройка Active Directory Certificate Services.Целью данной лабораторной является ознакомление с процессом установки службы	2	ПК-20

Согласована на портале № 29513

	Active Directory Certificate Services (службы сертификации) и особенностями работы с сертификатами.		
	Итого	2	
2 Протоколы распределения ключей.	Симметричные протоколы:Лягушка с открытым ртом,Протокол Нидхема-Шрёдера,Протокол Kerberos,Протокол Отвея-Рииса.Асимметричные протоколы:Протокол Нидхема-Шрёдера,Описание работы протокола,Ситуация перед началом работы,Период работы протокола.	2	ПК-20
	Итого	2	
Итого за семестр		4	
9 семестр			
3 Инфраструктура открытого ключа.	Защита от атаки «Человек в середине».Сертификаты открытых ключей.Логическая структура и компоненты PKI.	2	ПК-20
	Итого	2	
4 Практические аспекты реализации средств криптографической защиты информации.	Шифрование диска BitLocker.	2	ПК-20
	Итого	2	
5 Протокол идентификации и аутентификации	Общие сведения.Парольная идентификация/аутентификация.Протокол идентификации/аутентификации с использованием хеш-функции.Протокол идентификации/аутентификации на основе шифрования с открытым ключом.Сервер аутентификации Kerberos.Идентификация/аутентификация с помощью биометрических данных.Идентификационные карты и электронные ключи.	2	ПК-20
	Итого	2	
6 Безопасный канал обмена сообщениями	Защищенные сообщенияДля пересылки защищенных сообщений разработан криптографический протокол OTR (Off-the-Record). Для создания сильного шифрования протокол использует комбинацию алгоритмов AES, симметричного ключа, алгоритма Диффи — Хеллмана и хеш-функции SHA-1.	2	ПК-20
	Итого	2	
Итого за семестр		8	
Итого		12	

8. Практические занятия (семинары)

Не предусмотрено РУП.

9. Самостоятельная работа

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

Согласована на портале № 29513

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
8 семестр				
1 Криптографические протоколы: общие понятия.	Оформление отчетов по лабораторным работам	17	ПК-20	Контрольная работа, Отчет по лабораторной работе, Тест
	Подготовка к контрольным работам	17		
	Итого	34		
2 Протоколы распределения ключей.	Оформление отчетов по лабораторным работам	16	ПК-20	Контрольная работа, Отчет по лабораторной работе, Тест
	Подготовка к контрольным работам	16		
	Итого	32		
Итого за семестр		66		
9 семестр				
3 Инфраструктура открытого ключа.	Оформление отчетов по лабораторным работам	7	ПК-20	Контрольная работа, Отчет по лабораторной работе, Тест
	Подготовка к контрольным работам	7		
	Итого	14		
4 Практические аспекты реализации средств криптографической защиты информации.	Оформление отчетов по лабораторным работам	7	ПК-20	Контрольная работа, Отчет по лабораторной работе, Тест
	Подготовка к контрольным работам	7		
	Итого	14		
5 Протокол идентификации и аутентификации	Оформление отчетов по лабораторным работам	7	ПК-20	Контрольная работа, Отчет по лабораторной работе, Тест
	Подготовка к контрольным работам	7		
	Итого	14		
6 Безопасный канал обмена сообщениями	Оформление отчетов по лабораторным работам	7	ПК-20	Контрольная работа, Отчет по лабораторной работе, Тест
	Подготовка к контрольным работам	7		
	Итого	14		
Итого за семестр		56		
	Подготовка и сдача зачета	4		Зачет
Итого		126		

Согласована на портале № 29513

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян. - М. : Гелиос АРВ, 2004. - 143[1] с. : ил. - Загл. обл. : Криптография в упражнениях и задачах. - Загл. на корешке : Криптография в упражнениях и задачах. - Библиогр.: с. 139. - ISBN 5-85438-009-9 : 52.25 р. (наличие в библиотеке ТУСУР - 50 экз.)

12.2. Дополнительная литература

1. Основы криптографии : учебное пособие для вузов / А. П. Алферов [и др.]. - 3-е изд., испр. и доп. - М. : Гелиос АРВ, 2005. - 479, [1] с. : ил. - Библиогр.: с. 469-475. - ISBN 5-85438-137-0 (наличие в библиотеке ТУСУР - 30 экз.)
2. Рябко, Борис Яковлевич. Криптографические методы защиты информации : Учебное пособие для вузов. - М. : Горячая линия-Телеком , 2005. - 229[3] с. (наличие в библиотеке ТУСУР - 30 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 — 2014. [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf (дата обращения: 04.07.2018).
2. Евсютин О.О. Прикладная криптография: методические указания для выполнения лабораторных и самостоятельных работ — 2014. [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_pk.pdf (дата обращения: 04.07.2018).

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. Copyright for Librarians - Курс на английском языке, бесплатный, интерактивный, с задачами и примерами. Все материалы курса доступны по лицензии Creative Commons, то есть их можно копировать, распространять и изменять. cyber.law.harvard.edu. Доступ свободный.
2. eLIBRARY.RU - Крупнейший российский информационный портал в области науки, технологии, медицины и образования. www.elibrary.ru. Доступ свободный.
3. Nano - Ресурс предоставляет данные о более 200 000 наноматериалов и наноустройств, собранные из самых авторитетных научных изданий. nano.nature.com. Доступ свободный.
4. Nature - 88 естественно-научных журналов, включая старейший и один из самых авторитетн научных журналов Nature www.nature.com. Доступ свободный.

Согласована на портале № 29513

5. Polpred.com Обзор СМИ - Обзор средств массовой информации. Ежедневно тысяча новостей, полный текст на русском языке. Миллионы сюжетов информагентств и деловой прессы за 15 лет. www.polpred.com. Доступ свободный.

6. zbMATH - самая полная математическая база данных, охватывающая материалы с конца 19 века. zbMath содержит около 4 000 000 документов, из более 3 000 журналов и 170 000 книг по математике, статистике, информатике, а также машиностроению, физике, естественным наукам и др. zbmath.org. Доступ свободный.

7. Архив журналов РАН - Российская академия наук и издательство «Наука» приняли решение открыть свободный доступ к архивам журналов РАН, включая номера журналов за 2017 год, выпуск которых по контракту с РАН осуществляло издательство «Наука». Бесплатный доступ к электронным версиям журналов РАН будет предоставляться на платформе elibrary.ru и libnauka.ru (электронная библиотека издательства «Наука»). Всего журналов в референтной группе 149. Список журналов. Доступ свободный.

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 лабораторных работ

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:

- Моноблок: Asus V222GAK-BA021D: Intel J5005/ DDR4 4G/ 500Gb/ WiFi / мышь/ клавиатура (30шт.);

- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;

- Комплект специализированной учебной мебели;

- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10

– VirtualBox

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.

Согласована на портале № 29513

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

По принципу Керкгоффса в криптосистеме секретным должно быть:
- ключ
- время шифрования
- сложность алгоритма
- длина ключа

Победитель конкурса AES (Advanced Encryption Standard)?
- DES
- RC6
- Rijndael
- Twofish

Каким свойством должен обладать канал передачи информации в схеме Диффи-Хеллмана
- защищенный от подмены
- защищенный от прослушивания
- закрытый канал
- открытый канал

Что такое диффузия?
- Влияние одного знака открытого ключа на значительное количество знаков шифротекста.
- Влияние одного знака закрытого ключа на значительное количество знаков шифротекста.
- Влияние одного знака открытого текста на значительное количество знаков шифротекста.
- Влияние алгоритма защиты информации на значительное количество знаков шифротекста.

Как называется преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины? (использует одностороннюю функцию)

Согласована на портале № 29513

- Разбиение входного массива
- Хеширование
- Сжатие
- Сдвиг

Виды симметричных криптосистем:
- поточные шифры
- ЭЦП
- криптосистемы с открытым ключом
- нет ответа

Advanced Encryption Standard (AES), также известный как Rijndael имеет размер блока (в битах):
- 64
- 128
- 192
- 256

Advanced Encryption Standard (AES), также известный как Rijndael может иметь ключ (в битах):
- 128
- 192
- 256
- все выше перечисленные

Какая схема лежит в основе DES и ГОСТ 28147-89?
- Цезаря
- Кантора
- Фейстеля
- Виженера

Какие из следующих алгоритмов являются ассимметричными?
- DES
- Эль-Гамаль
- ГОСТ 28147-89
- RC4

На какой труднорешаемой задаче основан алгоритм RSA?
- Факторизации чисел
- Нахождения большого простого числа
- Вычислении обратного элемента
- Дискретного логарифмирования

Какая длина ключа в ГОСТ 28147-89(Магма)? (ответ в битах)
- 64
- 128
- 192
- 256

Что обычно в себя включает схема электронной подписи?
- алгоритм генерации ключевых пар пользователя
- функцию проверки подписи
- ничего из вышеперечисленного
- все из вышеперечисленного

Метод полиалфавитного шифрования буквенного текста с использованием ключевого слова (текстового):
- Шифр Гронсфельда
- Шифр Виженера
- Шифр Цезаря
- Шифр Вернама

Какой ключ доступен всем для проверки цифровой подписи под документом?
- закрытый

Согласована на портале № 29513

- открытый
- внутренний
- общий

Какой шрифт более стойкий к взлому?
- Симметричный
- Асимметричный
- Псевдосимметричный
- Нет правильного ответа

Какой алгоритм шифрования стал прообразом для отечественного ГОСТ28147-89?
- DES
- DSA
- Rijndael
- IDEA

В чем преимущество симметричных систем над асимметричными?
- скорость шифрования
- простота реализации
- изученность
- все ответы правильные

Что подразумевается под термином аутентичность информации?
- Целостность информации
- Невозможность отказа от авторства
- Подлинность авторства
- все ответы правильные

Выберите правильный вариант, зашифрованной с помощью шифра цезаря, строки: шифр цезаря
- ъйхс чёибсб
- щйхс чёибса
- ъкцт шжйвсб
- юоъц ькнёцж

14.1.2. Темы опросов на занятиях

Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоколы.

Понятие электронной подписи. Управление открытыми ключами. Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытого ключа.

Проблемы реализации криптографических алгоритмов. Генерация случайных чисел. Защита от утечки информации.

14.1.3. Зачёт

Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоколы.

Понятие электронной подписи. Управление открытыми ключами. Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытого ключа.

Протоколы идентификации на основе паролей, протоколы «рукопожатия» и типа «запрос-ответ». Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.

Построение безопасного коммуникационного канала на основе криптографических алгоритмов.

Проблемы реализации криптографических алгоритмов. Генерация случайных чисел. Защита от утечки информации.

14.1.4. Вопросы на самоподготовку

Дать содержательное объяснения таких услуг безопасности как конфиденциальность, целостность, подлинность, неотрекаемость и доступность.

Согласована на портале № 29513

Перечислить известные механизмы обеспечения безопасности. Объяснить взаимосвязь услуг безопасности, механизмов и алгоритмов.

Объяснить, что такое совершенная секретность, привести пример совершенного шифра. Объяснить смысл теоремы Шеннона.

Сжато, но осмысленно, пояснить те аспекты алгебры и теории чисел, которые используются в современной криптографии. Мультипликативная группа конечного поля, по модулю составного числа. Теоремы Эйлера и Ферма. Эллиптические кривые. Группа точек эллиптической кривой.

Режимы шифрования. Перечислить и объяснить различия.

Минимальная длина ключа симметричной криптосистемы. Экспортные ограничения на длину ключа.

Метод расширения ключевого пространства. Принцип несепарабельного шифрования. Многоуровневая криптография.

Инфраструктура открытых ключей (PKI). Обосновать необходимость подобной инфраструктуры. Пречислить и объяснить назначение составляющих компонент.

Хэш-функции. Какие типы существуют, в чем их различие. Объяснить свойства. Перечислить области применения. Атаки на хэш-функции. Что такое парадокс «дней рождения»?

Базовые принципы построения криптографичсеских пролтоколов.

Анонимность и неотслеживаемость. Проблема «ужинающих криптогра-фов». «Слепая» подпись Чаума. Объяснить принцип построения протоко-ла для анонимных чеков на основе «слепой» подписи.

Принципы квантовой криптографии. Объяснить квантовый протокол рас-пределения ключей.

14.1.5. Темы контрольных работ

Схемы разделения секрета
Системы электронного голосования
Доказательства с нулевым разглашением
Инфраструктура открытых ключей
Развитые протоколы обмена ключами с аутентификацией
Высокоскоростная система шифрования на базе поточных шифров
Быстродействующий цифровой скремблер

14.1.6. Темы лабораторных работ

Установка и настройка Active Directory Certificate Services
Кросс-сертификация
Использование клиентов электронной почты
Шифрованная файловая система Windows
Шифрование диска BitLocker
Генератор ключей для криптосистемы RSA
Реализовать программу-шифровщик

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)

Согласована на портале № 29513

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.

Согласована на портале № 29513