МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль): **Информационная безопасность финансовых и экономических структур**
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

Томск 2017

Согласована на портале № 16653

Рассмотрена и одобрена на заседании кафедры
протокол № 2 от « 4 » 3 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа 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 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

доцент каф. БИС _____ О. О. Евсютин

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. БИС _____ Р. В. Мещеряков

Эксперты:

доцент каф. КИБЭВС _____ А. А. Конев

Согласована на портале № 16653

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

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: 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 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 студент 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

Согласована на портале № 16653

Самостоятельная работа (всего)	44	44
Выполнение индивидуальных заданий	20	20
Проработка лекционного материала	10	10
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	Лекции	Практические занятия	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
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	Трудоемкость, ч	Формируемые компетенции
5 семестр			
1 Основные цели и задачи криптографии	Криптографические методы защиты информации: шифрование,	2	ОПК-2

Согласована на портале № 16653

	хеширование, электронная подпись.		
	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 шифрование	ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. DES. AES.	8	ОПК-2
	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								

Согласована на портале № 16653

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 и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий			Формы контроля
	Лекции	Практические занятия	Самостоятельная работа	
ОПК-2	+	+	+	Домашнее задание, Отчет по индивидуальному заданию, Экзамен, Защита отчета, Опрос на занятиях

6. Интерактивные методы и формы организации обучения

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

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные практические занятия	Интерактивные лекции	Всего
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.

Согласована на портале № 16653

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	

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

Согласована на портале № 16653

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		
	Подготовка и сдача экзамена	36		Экзамен
Итого		80		

Согласована на портале № 16653

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

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	5	15
Защита отчета	10	10	10	30
Опрос на занятиях	4	3	3	10
Отчет по индивидуальному заданию	5	5	5	15
Итого максимум за период	24	23	23	70
Экзамен				30
Нарастающим итогом	24	47	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)

Согласована на портале № 16653

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Рябко Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. — 2-е изд. — М.: Горячая линия – Телеком, 2013. — 232 с. [Электронный ресурс]. — Режим доступа: http://e.lanbook.com/view/book/63244/ [Электронный ресурс]. - http://e.lanbook.com/view/book/63244/
2. Введение в теоретико-числовые методы криптографии: учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — СПб.: Издательство «Лань», 2011. — 400 с. [Электронный ресурс]. — Режим доступа: http://e.lanbook.com/view/book/68466/ [Электронный ресурс]. - http://e.lanbook.com/view/book/68466/

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 - 28 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. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа 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. Ресурсы сети Интернет

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. 1. Виртуальная операционная система Microsoft Windows XP SP3 (VirtualBox, доступ из локальной сети каф. КИБЭВС. URL: file://cesir/vm/WinXPBasic).
2. 2. Интегрированная среда разработки программного обеспечения Microsoft Visual Studio 2012.

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое 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 наглядные пособия в виде презентаций по лекционным разделам дисциплины.

Согласована на портале № 16653

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 402. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Мультимедийный проектор Benq – 1 шт.; Компьютеры класса не ниже AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb. с широкополосным доступом в Internet, – 15 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 2 этаж, ауд. 204. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Ce1егоп D336 2.8ГГц. - 7 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

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

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **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 удаленного просмотра.

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

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	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 № 16653

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 средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ 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.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов 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 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 обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 16653

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Криптографические методы защиты информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль): **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **3**
Семестр: **5**

Учебный план набора 2016 года

Разработчики:
- доцент каф. БИС О. О. Евсютин

Экзамен: 5 семестр

Томск 2017

Согласована на портале № 16653

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования 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	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.; Должен уметь эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; применять простейшие методы криптоанализа.; Должен владеть криптографическими методами и средствами защиты информации; простейшими методами криптоанализа; методами оценки стойкости криптографических алгоритмов.;

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительн	Обладает базовыми	Обладает основными	Работает при прямом

Согласована на портале № 16653

о (пороговый уровень)	общими знаниями	умениями, требуемыми для выполнения простых задач	наблюдении

2 Реализация компетенций

2.1 Компетенция ОПК-2

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.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	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.	эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; применять простейшие методы криптоанализа.	криптографическими методами и средствами защиты информации; простейшими методами криптоанализа; методами оценки стойкости криптографических алгоритмов.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Домашнее задание; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Домашнее задание; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Домашнее задание; • Отчет по индивидуальному заданию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть

Согласована на портале № 16653

Отлично (высокий уровень)	• Знает направления современной криптографии и понимает связи между ними; знает принципы построения криптографических алгоритмов и криптографические стандарты; знает простейшие методы криптоанализа.;	• Умеет обоснованно применять криптографические методы и средства защиты информации для решения задач обеспечения информационной безопасности; умеет применять простейшие методы криптоанализа.;	• Владеет криптографическими методами и средствами защиты информации; владеет методами оценки стойкости криптографических алгоритмов.;
Хорошо (базовый уровень)	• Знает направления современной криптографии и основные криптографические стандарты.;	• Умеет применять криптографические методы и средства защиты информации для решения задач обеспечения информационной безопасности.;	• Владеет основными криптографическими методами и средствами защиты информации.;
Удовлетворительно (пороговый уровень)	• Знает направления современной криптографии.;	• Имеет представление о применении криптографических методов и алгоритмов для решения задач обеспечения информационной безопасности.;	• Владеет некоторыми методами и средствами защиты информации.;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 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.

3.2 Темы индивидуальных заданий

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

3.3 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.

– 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.

Согласована на портале № 16653

– 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.

3.4 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.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Рябко Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. — 2-е изд. — М.: Горячая линия – Телеком, 2013. — 232 с. [Электронный ресурс]. — Режим доступа: http://e.lanbook.com/view/book/63244/ [Электронный ресурс]. - http://e.lanbook.com/view/book/63244/

2. Введение в теоретико-числовые методы криптографии: учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — СПб.: Издательство «Лань», 2011. — 400 с. [Электронный ресурс]. — Режим доступа: http://e.lanbook.com/view/book/68466/ [Электронный ресурс]. - http://e.lanbook.com/view/book/68466/

4.2. 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 - 28 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.)

4.3. 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. [Электронный ресурс]. -

Согласована на портале № 16653

http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf

4.4. Ресурсы сети Интернет

4.4. Базы данных, информационно справочные и поисковые системы

1. 1. Виртуальная операционная система Microsoft Windows XP SP3 (VirtualBox, доступ из локальной сети каф. КИБЭВС. URL: file://cesir/vm/WinXPBasic).
2. 2. Интегрированная среда разработки программного обеспечения Microsoft Visual Studio 2012.

Согласована на портале № 16653