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

Прикладная криптография

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Безопасность автоматизированных систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **3**
Семестр: **6**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	6 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	36	36	часов
4	Всего аудиторных занятий	72	72	часов
5	Из них в интерактивной форме	20	20	часов
6	Самостоятельная работа	36	36	часов
7	Всего (без экзамена)	108	108	часов
8	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е

Зачет: 6 семестр

Томск 2017

Согласована на портале № 17313

Рассмотрена и одобрена на заседании кафедры
протокол № 3 от «17» 3 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

Программист каф. КИБЭВС _____ И. Ю. Поляков

Доцент каф. КИБЭВС _____ . . Конев

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. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Декан, к.н. каф. КИБЭВС _____ . . Давыдова

Согласована на портале № 17313

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 «Прикладная криптография» (Б1.В.ОД.6) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Криптографические методы защиты информации, Основы информационной безопасности.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

– ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

В результате изучения дисциплины студент 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 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		6 семестр
Аудиторные занятия (всего)	72	72
Лекции	18	18
Практические занятия	18	18
Лабораторные работы	36	36
Из них в интерактивной форме	20	20
Самостоятельная работа (всего)	36	36
Оформление отчетов по лабораторным работам	17	17
Проработка лекционного материала	6	6
Подготовка к практическим занятиям, семинарам	13	13
Всего (без экзамена)	108	108
Общая трудоемкость ч	108	108

Согласована на портале № 17313

Зачетные Единицы	3.0	3.0

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	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
6 семестр						
1 Криптографические протоколы: общие понятия.	2	3	6	10	21	ПК-13, ПК-6
2 Протоколы распределения ключей.	4	5	0	4	13	ПК-6
3 Инфраструктура открытого ключа.	4	4	0	5	13	ПК-13
4 Протоколы идентификации и аутентификации.	4	0	11	4	19	ПК-6
5 Безопасный канал обмена сообщениями.	2	0	0	1	3	ПК-13
6 Практические аспекты реализации средств криптографической защиты информации.	2	6	19	12	39	ПК-13, ПК-6
Итого за семестр	18	18	36	36	108	
Итого	18	18	36	36	108	

5.2. Содержание разделов дисциплины (по лекциям)

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

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
6 семестр			
1 Криптографические протоколы: общие понятия.	Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоколы.	2	ПК-6
	Итого	2	
2 Протоколы распределения ключей.	Управление секретными ключами. Распределение секретных ключей.	4	ПК-6
	Итого	4	

Согласована на портале № 17313

3 Инфраструктура открытого ключа.	Понятие электронной подписи. Управление открытыми ключами. Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытого ключа.	4	ПК-13
	Итого	4	
4 Протоколы идентификации и аутентификации.	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.	4	ПК-6
	Итого	4	
5 Безопасный канал обмена сообщениями.	Построение безопасного коммуникационного канала на основе криптографических алгоритмов.	2	ПК-13
	Итого	2	
6 Практические аспекты реализации средств криптографической защиты информации.	Проблемы реализации криптографических алгоритмов. Генерация случайных чисел. Защита от утечки информации.	2	ПК-13
	Итого	2	
Итого за семестр		18	

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 Криптографические методы защиты информации	+					+
2 Основы информационной безопасности	+					

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

	Виды занятий	Формы контроля

Согласована на портале № 17313

Компетенции	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	
ПК-6	+	+	+	+	Конспект самоподготовки, Собеседование, Отчет по лабораторной работе, Опрос на занятиях, Тест
ПК-13	+	+	+	+	Собеседование, Отчет по лабораторной работе, 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 лабораторные занятия	Интерактивные лекции	Всего
6 семестр				
Презентации с использованием слайдов с обсуждением	3	6	5	14
Презентации с использованием мультимедиа с обсуждением	1	4	1	6
Итого за семестр:	4	10	6	20
Итого	4	10	6	20

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
6 семестр			
1 Криптографические протоколы: общие понятия.	Шифрование диска BitLocker	6	ПК-13
	Итого	6	
4 Протоколы идентификации и аутентификации.	СКЗИ SecretDisk	11	ПК-6
	Итого	11	

Согласована на портале № 17313

6 Практические аспекты реализации средств криптографической защиты информации.	Шифрованная файловая система	4	ПК-6, ПК-13
	Криптопровайдеры	15	
	Итого	19	
Итого за семестр		36	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
6 семестр			
1 Криптографические протоколы: общие понятия.	Анализ уязвимостей простейших протоколов	3	ПК-6
	Итого	3	
2 Протоколы распределения ключей.	Анализ уязвимостей простейших протоколов.	5	ПК-6
	Итого	5	
3 Инфраструктура открытого ключа.	Структура сертификатов открытого ключа	4	ПК-13
	Итого	4	
6 Практические аспекты реализации средств криптографической защиты информации.	Удостоверяющие центры	6	ПК-13
	Итого	6	
Итого за семестр		18	

9. Самостоятельная работа

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

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
6 семестр				
1 Криптографические протоколы: общие понятия.	Подготовка к практическим занятиям, семинарам	3	ПК-6, ПК-13	Опрос на занятиях, Отчет по лабораторной работе, Собеседование
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	6		

Согласована на портале № 17313

	Итого	10		
2 Протоколы распределения ключей.	Подготовка к практическим занятиям, семинарам	3	ПК-6	Конспект самоподготовки, Собеседование, Тест
	Проработка лекционного материала	1		
	Итого	4		
3 Инфраструктура открытого ключа.	Подготовка к практическим занятиям, семинарам	4	ПК-13	Опрос на занятиях, Собеседование
	Проработка лекционного материала	1		
	Итого	5		
4 Протоколы идентификации и аутентификации.	Проработка лекционного материала	1	ПК-6	Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	3		
	Итого	4		
5 Безопасный канал обмена сообщениями.	Проработка лекционного материала	1	ПК-13	Опрос на занятиях
	Итого	1		
6 Практические аспекты реализации средств криптографической защиты информации.	Подготовка к практическим занятиям, семинарам	3	ПК-13, ПК-6	Опрос на занятиях, Отчет по лабораторной работе, Собеседование
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	8		
	Итого	12		
Итого за семестр		36		
Итого		36		

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
6 семестр				
Конспект самоподготовки	5	5	5	15
Опрос на занятиях	5	5	5	15

Согласована на портале № 17313

Отчет по лабораторной работе	10	10	10	30
Собеседование	2	2	2	6
Тест	12	12	10	34
Итого максимум за период	34	34	32	100
Нарастающим итогом	34	68	100	100

11.2. Пересчет баллов в оценки за контрольные точки

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

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

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

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

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

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. 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.)

2. Криптография : учебник для вузов: пер. с англ. / Н. Смарт ; пер. С. А. Кулешов, ред. пер. С. К. Ландо. - М. : Техносфера, 2005. - 525[3] с. : ил. - (Мир программирования ; VIII-05). - Предм. указ.: с. 524-525. - ISBN 5-94836-043-1 : 402.00 р. (наличие в библиотеке ТУСУР - 11 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.)

Согласована на портале № 17313

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]. — 2014. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf
2. Евсютин О.О. Прикладная криптография: методические указания для выполнения лабораторных и самостоятельных работ [Электронный ресурс]. — 2014. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_pk.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. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. Google — поисковая система интернета, принадлежащая корпорации Google Inc.
2. Яндекс — поисковая система интернета, принадлежащий российской корпорации «Яндекс».

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 лекционных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 3 этаж, ауд. 310. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор ViewSonic PJD5151 – 1 шт.; Компьютер лекционный acer travelmate 2300; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP2, Microsoft Powerpoint Viewer; Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 400. Состав оборудования: Учебная мебель; Доска магнитно-маркерная - 1 шт.;

13.1.3. Материально-техническое обеспечение для лабораторных работ

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.

Согласована на портале № 17313

13.1.4. 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 Celeron 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)
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 оценоч-

Согласована на портале № 17313

ных 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 № 17313

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

Прикладная криптография

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Безопасность автоматизированных систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **3**
Семестр: **6**

Учебный план набора 2016 года

Разработчики:
- Программист каф. КИБЭВС И. Ю. Поляков
- Доцент каф. КИБЭВС . . Конев

Зачет: 6 семестр

Томск 2017

Согласована на портале № 17313

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
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Должен знать основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях.; Должен уметь эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах.; Должен владеть навыками использования типовых криптографических алгоритмов.;
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	

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
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПК-13

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

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

Согласована на портале № 17313

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	взаимосвязи отдельных процессов управления информационной безопасностью в рамках общей системы управления	используя современные методы и средства разрабатывать процессы управления информационной безопасностью	навыками управления информационной безопасностью простых объектов
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по лабораторной работе; • Опрос на занятиях; • Собеседование; • Зачет;	• Отчет по лабораторной работе; • Опрос на занятиях; • Собеседование; • Зачет;	• Отчет по лабораторной работе; • Зачет;

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

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Знает в полном объеме взаимосвязи отдельных процессов управления информационной безопасностью в рамках общей системы управления ;	• В полном объеме умеет определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью ;	• В полном объеме владеет навыками управления информационной безопасностью простых объектов ;
Хорошо (базовый уровень)	• Знает на продвинутом уровне взаимосвязи отдельных процессов управления информационной безопасностью в рамках общей системы управления ;	• На продвинутом уровне умеет определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью ;	• На продвинутом уровне владеет навыками управления информационной безопасностью простых объектов ;
Удовлетворительно (пороговый уровень)	• Знает на базовом уровне взаимосвязи отдельных процессов управления информационной безопасностью в рамках общей системы управления ;	• На базовом уровне умеет определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью ;	• На базовом уровне владеет навыками управления информационной безопасностью простых объектов ;

Согласована на портале № 17313

2.2 Компетенция ПК-6

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	основные стандарты, регламентирующие управление информационной безопасностью	определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью	навыками администрирования систем и устройств защиты информации
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по лабораторной работе; • Опрос на занятиях; • Конспект самоподготовки; • Тест; • Собеседование; • Зачет;	• Отчет по лабораторной работе; • Опрос на занятиях; • Конспект самоподготовки; • Тест; • Собеседование; • Зачет;	• Отчет по лабораторной работе; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Знает в полном объеме основные стандарты, регламентирующие управление информационной безопасностью ;	• В полном объеме умеет определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью ;	• В полном объеме умеет навыками администрирования систем и устройств защиты информации ;
Хорошо (базовый уровень)	• Знает на продвинутом уровне основные стандарты, регламентирующие управление ин-	• На продвинутом уровне умеет определять цели и задачи, решаемые разрабатывае-	• На продвинутом уровне умеет навыками администрирования систем и устройств защи-

Согласована на портале № 17313

	формационной безопасностью ;	мыми процессами управления информационной безопасностью ;	ты информации ;
Удовлетворительно (пороговый уровень)	• Знает на базовом уровне основные стандарты, регламентирующие управление информационной безопасностью ;	• На базовом уровне умеет определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью ;	• На базовом уровне умеет навыками администрирования систем и устройств 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 Вопросы на самоподготовку

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

– 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.

3.2 Тестовые задания

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

– Инфраструктура открытых ключей (PKI). Обосновать необходимость подобной инфраструктуры. Перечислить 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 криптографических протоколов.

Согласована на портале № 17313

3.3 Вопросы на собеседование

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

– Инфраструктура открытых ключей (PKI). Обосновать необходимость подобной инфраструктуры. Перечислить 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 криптографических протоколов.

3.4 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.

– 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.

3.5 Темы лабораторных работ

– Шифрованная файловая система
– Шифрование диска BitLocker
– Криптопровайдеры
– СКЗИ SecretDisk

3.6 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.

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. 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.)

2. Криптография : учебник для вузов: пер. с англ. / Н. Смарт ; пер. С. А. Кулешов, ред. пер.

Согласована на портале № 17313

С. К. Ландо. - М. : Техносфера, 2005. - 525[3] с. : ил. - (Мир программирования ; VIII-05). - Предм. указ.: с. 524-525. - ISBN 5-94836-043-1 : 402.00 р. (наличие в библиотеке ТУСУР - 11 экз.)

4.2. 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.)

4.3. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — 2014. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf
2. Евсютин О.О. Прикладная криптография: методические указания для выполнения лабораторных и самостоятельных работ [Электронный ресурс]. — 2014. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_pk.pdf

4.4. Базы данных, информационно справочные и поисковые системы

1. Google — поисковая система интернета, принадлежащая корпорации Google Inc.
2. Яндекс — поисковая система интернета, принадлежащий российской корпорации «Яндекс».

Согласована на портале № 17313