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 - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **3**
Семестр: **6**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	6 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	36	36	часов
3	Всего аудиторных занятий	54	54	часов
4	Из них в интерактивной форме	16	16	часов
5	Самостоятельная работа	18	18	часов
6	Всего (без экзамена)	72	72	часов
7	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е

Зачет: 6 семестр

Томск 2017

Согласована на портале № 17464

Рассмотрена и одобрена на заседании кафедры
протокол № 3 от «21» 3 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем, 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 № 17464

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.8) 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-3 способностью проводить анализ защищенности автоматизированных систем;

– ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

– ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;

– ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы;

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 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		6 семестр
Аудиторные занятия (всего)	54	54
Лекции	18	18
Практические занятия	36	36
Из них в интерактивной форме	16	16
Самостоятельная работа (всего)	18	18
Оформление отчетов по лабораторным работам	4	4
Проработка лекционного материала	6	6
Подготовка к практическим занятиям, семинарам	8	8
Всего (без экзамена)	72	72

Согласована на портале № 17464

Общая трудоемкость ч	72	72
Зачетные Единицы	2.0	2.0

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
6 семестр					
1 Криптографические протоколы: общие понятия.	2	6	5	13	ПК-14, ПК-26, ПК-3
2 Протоколы распределения ключей.	4	10	3	17	ПК-14, ПК-25
3 Инфраструктура открытого ключа.	4	8	3	15	ПК-14, ПК-25, ПК-26
4 Протоколы идентификации и аутентификации.	4	0	2	6	ПК-26
5 Безопасный канал обмена сообщениями.	2	0	1	3	
6 Практические аспекты реализации средств криптографической защиты информации.	2	12	4	18	ПК-14, ПК-25, ПК-26, ПК-3
Итого за семестр	18	36	18	72	
Итого	18	36	18	72	

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-14
	Итого	2	
2 Протоколы распределения ключей.	Управление секретными ключами. Распределение секретных ключей.	4	

Согласована на портале № 17464

	Итого	4	
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	
	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	
	Итого	4	
5 Безопасный канал обмена сообщениями.	Построение безопасного коммуникационного канала на основе криптографических алгоритмов.	2	
	Итого	2	
6 Практические аспекты реализации средств криптографической защиты информации.	Проблемы реализации криптографических алгоритмов. Генерация случайных чисел. Защита от утечки информации.	2	
	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 № 17464

Компетенции	Лекции	Практические занятия	Самостоятельная работа	
ПК-3		+	+	Собеседование, Отчет по лабораторной работе
ПК-14	+	+	+	Собеседование, Опрос на занятиях, Тест
ПК-25		+	+	Собеседование
ПК-26		+	+	Собеседование, Отчет по лабораторной работе

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
6 семестр			
Презентации с использованием слайдов с обсуждением	3	5	8
Презентации с использованием мультимедиа с обсуждением	7	1	8
Итого за семестр:	10	6	16
Итого	10	6	16

7. Лабораторные работы

Не предусмотрено РУП

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
6 семестр			
1 Криптографические протоколы: общие понятия.	Анализ уязвимостей простейших протоколов	6	ПК-26, ПК-3
	Итого	6	
2 Протоколы распределения ключей.	Анализ уязвимостей простейших протоколов.	10	ПК-14, ПК-25
	Итого	10	

Согласована на портале № 17464

3 Инфраструктура открытого ключа.	Структура сертификатов открытого ключа	8	ПК-14, ПК-26
	Итого	8	
6 Практические аспекты реализации средств криптографической защиты информации.	Удостоверяющие центры	12	ПК-14, ПК-3
	Итого	12	
Итого за семестр		36	

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-3	Опрос на занятиях, Отчет по лабораторной работе, Собеседование
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	1		
	Итого	5		
2 Протоколы распределения ключей.	Подготовка к практическим занятиям, семинарам	2	ПК-14	Конспект самоподготовки, Собеседование, Тест
	Проработка лекционного материала	1		
	Итого	3		
3 Инфраструктура открытого ключа.	Подготовка к практическим занятиям, семинарам	2	ПК-25	Опрос на занятиях, Собеседование
	Проработка лекционного материала	1		
	Итого	3		
4 Протоколы идентификации и аутентификации.	Проработка лекционного материала	1	ПК-26	Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	1		
	Итого	2		
5 Безопасный канал обмена сообщениями.	Проработка лекционного материала	1		Опрос на занятиях

Согласована на портале № 17464

	Итого	1		
6 Практические аспекты реализации средств криптографической защиты информации.	Подготовка к практическим занятиям, семинарам	1	ПК-25, ПК-26	Опрос на занятиях, Отчет по лабораторной работе, Собеседование
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
Итого за семестр		18		
Итого		18		

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
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.

Согласована на портале № 17464

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.)

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.

Согласована на портале № 17464

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 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, пере-

Согласована на портале № 17464

чень 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 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 № 17464

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 - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **3**
Семестр: **6**

Учебный план набора 2012 года

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

Зачет: 6 семестр

Томск 2017

Согласована на портале № 17464

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-26	способностью администрировать подсистему информационной безопасности автоматизированной системы	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-25	способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	
ПК-14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	
ПК-3	способностью проводить анализ защищенности автоматизированных систем	

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-26

ПК-26: способностью администрировать подсистему информационной безопасности автоматизированной системы.

Согласована на портале № 17464

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	Знать как администрировать подсистему информационной безопасности автоматизированной системы	Уметь администрировать подсистему информационной безопасности автоматизированной системы	Владеть способностью администрировать подсистему информационной безопасности автоматизированной системы
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	• Отчет по лабораторной работе; • Собеседование; • Зачет;	• Отчет по лабораторной работе; • 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 знать как администрировать подсистему информационной безопасности автоматизированной системы. ;	• В полном объеме умеет администрировать подсистему информационной безопасности автоматизированной систем.;	• В полном объеме владеет способностью администрировать подсистему информационной безопасности автоматизированной системы. ;
Хорошо (базовый уровень)	• Знает на продвинутом уровне знать как администрировать подсистему информационной безопасности автоматизированной системы. ;	• На продвинутом уровне умеет администрировать подсистему информационной безопасности автоматизированной системы. ;	• На продвинутом уровне владеет способностью администрировать подсистему информационной безопасности автоматизированной системы. ;
Удовлетворительно (пороговый уровень)	• Знает на базовом уровне знать как администрировать подсистему информационной безопасности автоматизированной системы. ;	• На базовом уровне умеет администрировать подсистему информационной безопасности автоматизированной системы. ;	• На базовом уровне владеет способностью администрировать подсистему информационной безопасности автоматизированной системы. ;

2.2 Компетенция ПК-25

ПК-25: способностью обеспечить эффективное применение средств защиты информаци-

Согласована на портале № 17464

онно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций.

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	методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем.	восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях.	поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем.
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	• Собеседование; • Зачет;	• Собеседование; • Зачет;	• 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)	• В полном объеме умеет восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях. ;	• В полном объеме умеет восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях. ;	• В полном объеме владеет навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем. ;
Хорошо (базовый уровень)	• На продвинутом уровне умеет восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях. ;	• На продвинутом уровне умеет восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях. ;	• На продвинутом уровне владеет навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем. ;
Удовлетворительно (пороговый уровень)	• На базовом уровне умеет восстанавливать	• На базовом уровне умеет восстанавливать	• На базовом уровне владеет навыками под-

Согласована на портале № 17464

	работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях. ;	работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях. ;	держания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем. ;

2.3 Компетенция ПК-14

ПК-14: способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических 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 7.

Таблица 7 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Знать как выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем.	Уметь выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем	Владеть способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем
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	• Опрос на занятиях; • Тест; • Собеседование; • Зачет;	• Опрос на занятиях; • Тест; • Собеседование; • Зачет;	• Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 8.

Таблица 8 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• В полном объеме знает как выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и	• В полном объеме умеет выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и	• В полном объеме владеет способностью выполнять установку, настройку и обслуживание, диагностику, экс-

Согласована на портале № 17464

	восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем. ;	восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем. ;	плуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем.;
Хорошо (базовый уровень)	• На продвинутом уровне знает как выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем. ;	• На продвинутом уровне умеет выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем. ;	• На продвинутом уровне владеет способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем.;
Удовлетворительно (пороговый уровень)	• На базовом уровне знает как выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем. ;	• На базовом уровне умеет выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем. ;	• На базовом уровне владеет способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем.;

2.4 Компетенция ПК-3

ПК-3: способностью проводить анализ защищенности автоматизированных систем.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 9.

Таблица 9 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем.	исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений.	способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного обору-

Согласована на портале № 17464

			дования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем .
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	• Отчет по лабораторной работе; • Собеседование; • Зачет;	• Отчет по лабораторной работе; • Собеседование; • Зачет;	• Отчет по лабораторной работе; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 10.

Таблица 10 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Знает в полном объеме каковы методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем. ;	• В полном объеме умеет выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем .;	• В полном объеме владеет способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем. ;
Хорошо (базовый уровень)	• Знает на продвинутом уровне каковы методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем. ;	• На продвинутом уровне умеет выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем .;	• На продвинутом уровне владеет способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем.;

Согласована на портале № 17464

Удовлетворительно (пороговый уровень)	• Знает на базовом уровне каковы методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем. ;	• На базовом уровне умеет выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем ;	• На базовом уровне владеет способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем.;

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. Пере-

Согласована на портале № 17464

числить области применения. Атаки на хэш-функции. Что такое парадокс «дней рождения»?

– Базовые принципы построения криптографических протоколов.

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

– 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

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.

Согласована на портале № 17464

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. 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 № 17464