

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

Документ подписан электронной подписью

Сертификат: 1с6сfa0a-52a6-4f49-aef0-5584d3fd4820

Владелец: Троян Павел Ефимович

Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптография в банковском деле

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: **4**

Семестр: **7**

Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	28	28	часов
3	Всего аудиторных занятий	56	56	часов
4	Из них в интерактивной форме	16	16	часов
5	Самостоятельная работа	52	52	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: 7 семестр

Томск 2017

## 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

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:

Доцент каф. КИБЭВС \_\_\_\_\_ А. А. Конев

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью преподавания дисциплины является изучение основных методов криптографической защиты банковской информации.

### 1.2. Задачи дисциплины

– Задачами преподавания данной дисциплины является изучение основ внедрения криптографии для защиты банковской информации.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Криптография в банковском деле» (Б1.Б.32.1) относится к блоку 1 (базовая часть).

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

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПСК-5.1 способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем;

В результате изучения дисциплины студент должен:

– **знать** основные криптографические протоколы и стандарты, используемые в автоматизированных банковских системах.

– **уметь** проводить инструментальный мониторинг защищенности автоматизированных банковских систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных банковских систем; формировать и эффективно применять комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированных банковских систем.

– **владеть** терминологией и системным подходом построения защищенных автоматизированных банковских систем; навыками формирования и эффективного применения комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированных банковских систем и банковских организаций.

## 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
		7 семестр
Аудиторные занятия (всего)	56	56
Лекции	28	28
Практические занятия	28	28
Из них в интерактивной форме	16	16
Самостоятельная работа (всего)	52	52
Проработка лекционного материала	19	19
Подготовка к практическим занятиям, семинарам	33	33
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
7 семестр					
1 Управление ключами средств криптографической защиты банковской информации.	6	6	10	22	ПСК-5.1
2 Стандартизация методов и средств криптографической защиты информации. Практические аспекты обеспечения стойкости криптосистем	6	6	10	22	ПСК-5.1
3 Особенности обеспечения информационной безопасности АБС криптографическими методами	6	6	10	22	ПСК-5.1
4 Системы электронных платежей. "Электронные деньги"	6	5	11	22	ПСК-5.1
5 Криптографические протоколы в электронной коммерции	4	5	11	20	ПСК-5.1
Итого за семестр	28	28	52	108	
Итого	28	28	52	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
7 семестр			
1 Управление ключами средств криптографической защиты банковской информации.	Стандарт ISO 11770. Комплекс документов RFC международной организации IETF и стандарта ITU X.509.	6	ПСК-5.1
	Итого	6	
2 Стандартизация методов и средств криптографической защиты информации. Практические	Сервисы безопасности в архитектуре системного ПО. Криптопровайдеры. Стандартные интерфейсы криптогра-	6	ПСК-5.1

аспекты обеспечения стойкости криптосистем	фических модулей: GSS API, PKCS. Стандарты и форматы серии PKCS: форматы открытых ключей, форматы запросов сертификатов, форматы сертификата открытого ключа, формат списка аннулированных сертификатов.		
	Итого	6	
3 Особенности обеспечения информационной безопасности АБС криптографическими методами	Номенклатура СКЗИ в АБС. Средства сетевой безопасности. Межсетевые экраны. Виртуальные частные сети. Средства криптографической защиты файловых систем и баз данных. Средства аутентификации и контроля доступа. Администрирование и настройки СКЗИ. Сертифицированные российские аппаратно-программные средства защиты АБС.	6	ПСК-5.1
	Итого	6	
4 Системы электронных платежей. "Электронные деньги"	Модельное представление СЭП. Обобщённый интерфейс прикладного программирования СЭП. Потребительские качества СЭП. Цели обеспечения безопасности информации в СЭП.	6	ПСК-5.1
	Итого	6	
5 Криптографические протоколы в электронной коммерции	Классификация задач электронной коммерции. Модели "электронного рынка" (на примере Европейской модели SEMPER). Роль электронной коммерции в глобализации экономики.	4	ПСК-5.1
	Итого	4	
Итого за семестр		28	

### 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
Предшествующие дисциплины					
1 Криптографические методы защиты информации	+	+			

### 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	
ПСК-5.1	+	+	+	Конспект самоподготовки, 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
7 семестр			
Презентации с использованием мультимедиа с обсуждением	8	8	16
Итого за семестр:	8	8	16
Итого	8	8	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
7 семестр			
1 Управление ключами средств криптографической защиты банковской информации.	Стандарт ISO 11770. Комплекс документов RFC международной организации IETF и стандарта ITU X.509.	6	ПСК-5.1
	Итого	6	
2 Стандартизация методов и средств криптографической защиты информации. Практические аспекты обеспечения стойкости криптосистем	Сервисы безопасности в архитектуре системного ПО. Криптопровайдеры. Стандартные интерфейсы криптографических модулей: GSS API, PKCS. Стандарты и форматы серии PKCS: форматы открытых ключей, форматы запросов сертификатов, форматы сер-	6	ПСК-5.1

	тификата открытого ключа, формат списка аннулированных сертификатов.		
	Итого	6	
3 Особенности обеспечения информационной безопасности АБС криптографическими методами	Номенклатура СКЗИ в АБС. Средства сетевой безопасности. Межсетевые экраны. Виртуальные частные сети. Средства криптографической защиты файловых систем и баз данных. Средства аутентификации и контроля доступа. Администрирование и настройки СКЗИ. Сертифицированные российские аппаратно-программные средства защиты АБС.	6	ПСК-5.1
	Итого	6	
4 Системы электронных платежей. "Электронные деньги"	Модельное представление СЭП. Обобщенный интерфейс прикладного программирования СЭП. Потребительские качества СЭП. Цели обеспечения безопасности информации в СЭП.	5	ПСК-5.1
	Итого	5	
5 Криптографические протоколы в электронной коммерции	Классификация задач электронной коммерции. Модели "электронного рынка" (на примере Европейской модели SEMPER). Роль электронной коммерции в глобализации экономики.	5	ПСК-5.1
	Итого	5	
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
<b>7 семестр</b>				
1 Управление ключами средств криптографической защиты банковской информации.	Подготовка к практическим занятиям, семинарам	7	ПСК-5.1	Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	3		
	Итого	10		
2 Стандартизация методов и средств криптографической	Подготовка к практическим занятиям, семинарам	7	ПСК-5.1	Конспект самоподготовки, Опрос на занятиях

защиты информации. Практические аспекты обеспечения стойкости криптосистем	Проработка лекционного материала	3		
	Итого	10		
3 Особенности обеспечения информационной безопасности АБС криптографическими методами	Подготовка к практиче- ским занятиям, семина- рам	6	ПСК-5.1	Конспект самоподготов- ки, Опрос на занятиях
	Проработка лекционного материала	4		
	Итого	10		
4 Системы электронных платежей. "Электронные деньги"	Подготовка к практиче- ским занятиям, семина- рам	7	ПСК-5.1	Конспект самоподготов- ки, Опрос на занятиях
	Проработка лекционного материала	4		
	Итого	11		
5 Криптографические протоколы в электронной коммерции	Подготовка к практиче- ским занятиям, семина- рам	6	ПСК-5.1	Конспект самоподготов- ки, Опрос на занятиях
	Проработка лекционного материала	5		
	Итого	11		
Итого за семестр		52		
	Подготовка и сдача экза- мена	36		Экзамен
Итого		88		

### 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
7 семестр				
Конспект самоподготов- ки	10	10	10	30
Опрос на занятиях	10	14	16	40
Итого максимум за пери- од	20	24	26	70
Экзамен				30
Нарастающим итогом	20	44	70	100

#### 11.2. Пересчет баллов в оценки за контрольные точки

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



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

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

### 11.3. Пересчет суммы баллов в традиционную и международную оценку

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

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

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
65 - 69		
3 (удовлетворительно) (зачтено)	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. Анохин М. И. и др. Криптография в банковском деле //М.: МИФИ. – 1997. [Электронный ресурс]. - <http://geo.web.ru/db/msg.html?mid=1161287&uri=all.html>
2. Ященко В. В., Варнавский Н. П., Нестеренко Ю. В. Введение в криптографию. – СПб. и др. : Питер, 2001. (наличие в библиотеке ТУСУР - 1 экз.)

### 12.2. Дополнительная литература

1. Ященко В. В. Введение в криптографию. Новые математические дисциплины //М.: МЦ-НМО Питер. – 2001. – Т. 20. (наличие в библиотеке ТУСУР - 1 экз.)
2. 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]. - [http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin\\_kmzi.pdf](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]. - [http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin\\_pk.pdf](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 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 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.

**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**

**Криптография в банковском деле**

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: **4**

Семестр: **7**

Учебный план набора 2013 года

Разработчики:

– Программист каф. КИБЭВС И. Ю. Поляков

Экзамен: 7 семестр

Томск 2017

## 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
ПСК-5.1	способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем	<p>Должен знать основные криптографические протоколы и стандарты, используемые в автоматизированных банковских системах.;</p> <p>Должен уметь проводить инструментальный мониторинг защищенности автоматизированных банковских систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных банковских систем; формировать и эффективно применять комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированных банковских систем. ;</p> <p>Должен владеть терминологией и системным подходом построения защищенных автоматизированных банковских систем; навыками формирования и эффективного применения комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированных банковских систем и банковских организаций. ;</p>

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	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к

		области исследования	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 ПСК-5.1

ПСК-5.1: способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем.

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 стандарты, регламентирующие управление информационной безопасностью	проводить инструментальный мониторинг защищенности автоматизированных банковских систем	терминологией и системным подходом построения защищенных автоматизированных банковских систем
Виды занятий	<ul style="list-style-type: none"> <li>Интерактивные практические занятия;</li> <li>Интерактивные лекции;</li> <li>Практические занятия;</li> <li>Лекции;</li> <li>Самостоятельная работа;</li> </ul>	<ul style="list-style-type: none"> <li>Интерактивные практические занятия;</li> <li>Интерактивные лекции;</li> <li>Практические занятия;</li> <li>Лекции;</li> <li>Самостоятельная работа;</li> </ul>	<ul style="list-style-type: none"> <li>Интерактивные практические занятия;</li> <li>Самостоятельная работа;</li> </ul>
Используемые средства оценивания	<ul style="list-style-type: none"> <li>Опрос на занятиях;</li> <li>Конспект самоподготовки;</li> <li>Экзамен;</li> </ul>	<ul style="list-style-type: none"> <li>Опрос на занятиях;</li> <li>Конспект самоподготовки;</li> <li>Экзамен;</li> </ul>	<ul style="list-style-type: none"> <li>Экзамен;</li> </ul>

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)	<ul style="list-style-type: none"> <li>Знает в полном объеме основные стандарты, регламентирующие управление информационной безопасностью ;</li> </ul>	<ul style="list-style-type: none"> <li>В полном объеме умеет проводить инструментальный мониторинг защищенности автоматизированных банковских систем ;</li> </ul>	<ul style="list-style-type: none"> <li>В полном объеме владеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных банковских систем ;</li> </ul>
Хорошо (базовый уровень)	<ul style="list-style-type: none"> <li>Знает на продвинутом уровне основные стандарты, регламентирующие управление ин-</li> </ul>	<ul style="list-style-type: none"> <li>На продвинутом уровне умеет проводить инструментальный мониторинг защищенно-</li> </ul>	<ul style="list-style-type: none"> <li>На продвинутом уровне владеет разрабатывать предложения по совершенствованию си-</li> </ul>

	формационной безопасностью ;	сти автоматизированных банковских систем ;	стемы управления информационной безопасностью автоматизированных банковских систем ;
Удовлетворительно (пороговый уровень)	<ul style="list-style-type: none"> <li>Знает на базовом уровне основные стандарты, регламентирующие управление информационной безопасностью ;</li> </ul>	<ul style="list-style-type: none"> <li>На базовом уровне умеет проводить инструментальный мониторинг защищенности автоматизированных банковских систем ;</li> </ul>	<ul style="list-style-type: none"> <li>На базовом уровне владеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных банковских систем ;</li> </ul>

### 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

- Управление ключами средств криптографической защиты банковской информации.
- Стандартизация методов и средств криптографической защиты информации. Практические аспекты обеспечения стойкости криптосистем
- Особенности обеспечения информационной безопасности АБС криптографическими методами
- Системы электронных платежей. "Электронные деньги"
- Криптографические протоколы в электронной коммерции

#### 3.2 Темы опросов на занятиях

- Управление ключами средств криптографической защиты банковской информации.
- Стандартизация методов и средств криптографической защиты информации. Практические аспекты обеспечения стойкости криптосистем
- Особенности обеспечения информационной безопасности АБС криптографическими методами
- Системы электронных платежей. "Электронные деньги"
- Криптографические протоколы в электронной коммерции

#### 3.3 Экзаменационные вопросы

- Управление ключами средств криптографической защиты банковской информации.
- Стандартизация методов и средств криптографической защиты информации. Практические аспекты обеспечения стойкости криптосистем
- Особенности обеспечения информационной безопасности АБС криптографическими методами
- Системы электронных платежей. "Электронные деньги"
- Криптографические протоколы в электронной коммерции

### 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 формирования компетенций, согласно п. 12 рабочей программы.

#### 4.1. Основная литература

1. Анохин М. И. и др. Криптография в банковском деле //М.: МИФИ. – 1997. [Электрон-



ный ресурс]. - <http://geo.web.ru/db/msg.html?mid=1161287&uri=all.html>

2. Ященко В. В., Варнавский Н. П., Нестеренко Ю. В. Введение в криптографию. – СПб. и др. : Питер, 2001. (наличие в библиотеке ТУСУР - 1 экз.)

#### **4.2. Дополнительная литература**

1. Ященко В. В. Введение в криптографию. Новые математические дисциплины //М.: МЦ-НМО Питер. – 2001. – Т. 20. (наличие в библиотеке ТУСУР - 1 экз.)

2. 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]. - [http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin\\_kmzi.pdf](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]. - [http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin\\_pk.pdf](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».