

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

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

УТВЕРЖДАЮ

Директор департамента образования

\_\_\_\_\_ П. Е. Троян

«\_\_» \_\_\_\_\_ 20\_\_ г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Криптография в банковском деле**

Уровень образования: **высшее образование - специалитет**

Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**

Направленность (профиль) / специализация: **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 2018

## ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «\_\_» \_\_\_\_\_ 20\_\_ года, протокол № \_\_\_\_\_.

Разработчик:

Доцент каф. КИБЭВС

\_\_\_\_\_ А. А. Конев

Заведующий обеспечивающей каф.  
КИБЭВС

\_\_\_\_\_ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ

\_\_\_\_\_ Е. М. Давыдова

Заведующий выпускающей каф.  
КИБЭВС

\_\_\_\_\_ А. А. Шелупанов

Эксперты:

Доцент каф. КИБЭВС

\_\_\_\_\_ Е. Ю. Костюченко

Доцент каф. КИБЭВС

\_\_\_\_\_ К. С. Сарин

## 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: Криптографические методы защиты информации.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

## 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 обучающийся 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	Лек., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
<b>7 семестр</b>					
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
<b>7 семестр</b>			
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 сертификата открытого ключа, формат списка аннулированных	6	ПСК-5.1

	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	+	+			
Последующие дисциплины					
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	+

### 5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов

занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Прак. зан.	Сам. раб.	
ПСК-5.1	+	+	+	Конспект самоподготовки, Опрос на занятиях, Тест

### 6. Интерактивные методы и формы организации обучения

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

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий

Методы	Интерактивные практические занятия, ч	Интерактивные лекции, ч	Всего, ч
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 систем-ного ПО. Криптопровайдеры. Стандартные интерфейсы криптографических модулей: GSS API, PKCS. Стандарты и форматы серии PKCS: форматы открытых ключей, форматы запросов сертификатов, форматы сертификата открытого ключа, формат списка аннулиро-ванных сертификатов.	6	ПСК-5.1
	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	6	ПСК-5.1

	АБС.		
	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.	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
7 семестр				
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 защиты информации. Практические аспекты обеспечения стойкости криптосистем	Подготовка к практическим занятиям, семинарам	7	ПСК-5.1	Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	3		
	Итого	10		
3 Особенности обеспечения информационной безопасности АБС криптографическими методами	Подготовка к практическим занятиям, семинарам	6	ПСК-5.1	Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	4		
	Итого	10		
4 Системы электронных платежей	Подготовка к практическим занятиям, семинарам	7	ПСК-5.1	Конспект самоподготовки,

платежей. "Электронные деньги"	занятиям, семинарам			Опрос на занятиях
	Проработка лекционного материала	4		
	Итого	11		
5 Криптографические протоколы в электронной коммерции	Подготовка к практическим занятиям, семинарам	6	ПСК-5.1	Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	5		
	Итого	11		
Итого за семестр		52		
	Подготовка и сдача экзамена	36		Экзамен
Итого		88		

### 10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

### 11. Рейтинговая система для оценки успеваемости обучающихся

#### 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 самоподготовки	10	10	10	30
Опрос на занятиях	10	14	16	40
Итого максимум за период	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. Осипян В. О. Криптография в задачах и упражнениях. - М. : Гелиос АРВ , 2004. - 143[1] с. (наличие в библиотеке ТУСУР - 50 экз.)
2. Баричев С. Г. Основы современной криптографии : Учебный курс. - М. : Горячая линия-Телеком , 2002. - 176 с.: Библиотека ТУСУР, (наличие в библиотеке ТУСУР - 51 экз.)

### 12.2. Дополнительная литература

1. Основы криптографии : учебное пособие для вузов. - М. : Гелиос АРВ , 2005. - 479, [1] с. (наличие в библиотеке ТУСУР - 30 экз.)

### 12.3. Учебно-методические пособия

#### 12.3.1. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации [Электронный ресурс]: методические указания для выполнения практических и самостоятельных работ — Режим доступа: [http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin\\_kmzi.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf) (дата обращения: 19.05.2018).
2. Евсютин О.О. Прикладная криптография [Электронный ресурс]: методические указания для выполнения лабораторных и самостоятельных работ — Режим доступа: [http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin\\_pk.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_pk.pdf) (дата обращения: 19.05.2018).

#### 12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

##### Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

##### Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

##### Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

### 12.4. Профессиональные базы данных и информационные справочные системы

1. Copyright for Librarians - Курс на английском языке, бесплатный, интерактивный, с задачами и примерами. Все материалы курса доступны по лицензии Creative Commons, то есть их можно копировать, распространять и изменять. [cyber.law.harvard.edu](http://cyber.law.harvard.edu). Доступ свободный.

2. eLIBRARY.RU - Крупнейший российский информационный портал в области науки, технологии, медицины и образования. [www.elibrary.ru](http://www.elibrary.ru). Доступ свободный.

3. Nano - Ресурс предоставляет данные о более 200 000 наноматериалов и наноустройств, собранные из самых авторитетных научных изданий. [nano.nature.com](http://nano.nature.com). Доступ свободный.

4. Nature - 88 естественно-научных журналов, включая старейший и один из самых авторитетных научных журналов Nature [www.nature.com](http://www.nature.com). Доступ свободный.

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

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

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

### **13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение**

#### **13.1. Общие требования к материально-техническому и программному обеспечению дисциплины**

##### **13.1.1. Материально-техническое и программное обеспечение для лекционных занятий**

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

##### **13.1.2. Материально-техническое и программное обеспечение для практических занятий**

Аудитория моделирования, проектирования и эксплуатации информационных и аналитических систем

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 407 ауд.

Описание имеющегося оборудования:

- Компьютеры класса не ниже: плата Gigabyte GA-H55M-S2mATX/ Intel Original Soc-1156 Core i3 3.06 GHz/ DDR III Kingston CL9 (2 шт.) по 2048 Mb/ SATA-II 250Gb Hitachi / 1024 Mb GeForce GT240 PCI-E (6 шт.);

- Комплект специализированной учебной мебели;

- Рабочее место преподавателя.

Программное обеспечение:

- Microsoft Windows 7 Pro

Лаборатория Безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 804 ауд.

Описание имеющегося оборудования:

- Компьютеры класса не ниже GigaByte GA-F2A68HM-DS2 rev1.0 (RTL) / AMD A4-6300 / DDR-III DIMM 8Gb / SVGARadeon HD 8370D / HDD 1Tb Gb SATA-III Seagate (10 шт.);

- Обучающий стенд локальные компьютерные сети Mikrotik routerboard (2 шт.);
- ViPNET УМК «Безопасность сетей»;
- Коммутатор Mikrotik CRS125-24G-1S-IN (6 шт.);
- Компьютер класса не ниже i5-7400/8DDR4/SSD120G;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 (3 шт.);
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 (2 шт.);
- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 (2 шт.);
- Маршрутизатор Cisco C881-V-K9 (2 шт.);
- Маршрутизатор Check Point CPAP-SG1200R-NGFW (2 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Стенды для изучения средств криптографической защиты информации в банковском деле, включающие:

- абоненские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- средства криптографической защиты информации: программно-аппаратный комплекс шифрования «ФПСУ-IP», программно-аппаратный комплекс шифрования «ФПСУ-IP/Клиент».

Программное обеспечение:

- Microsoft Windows 10

### **13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы**

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

### **13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов**

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с нарушениями слуха предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в

которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с нарушениями зрения предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеовеличителей для комфортного просмотра.

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

#### **14. Оценочные материалы и методические рекомендации по организации изучения дисциплины**

##### **14.1. Содержание оценочных материалов и методические рекомендации**

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

###### **14.1.1. Тестовые задания**

Аудитор — это

- лицо, занимающееся аудитом по стандарту PCI DSS (проверкой соответствия требованиям стандарта) и консультационной деятельностью, связанной с оценкой соответствия требованиям стандарта PCI DSS.

- юридическое лицо, заинтересованное в выполнении исполнителем услуги проверки на соответствие требованиям стандарта PCI DSS.

- член ассоциации эмитентов банковских карт, который устанавливает и поддерживает взаимодействие с предприятиями торгово-сервисной сети, принимающей платежные карты.

- поставщик услуг сканирования, имеющий официальный статус от Совета стандартов безопасности (PCI SSC).

PCI DSS (Payment Card Industry Data Security Standard) - это

- стандарт безопасности данных индустрии платёжных карт;

- поставщик услуг сканирования, имеющий официальный статус от Совета стандартов безопасности (PCI SSC);

- аудит инфраструктуры Заказчика, проводимый аудитором непосредственно на реально функционирующих компонентах;

- компания, сотрудники которой индивидуально прошли тренинги и экзамены, проводимые Советом стандартов безопасности (PCI SSC).

Заказчик — это

- лицо, занимающееся аудитом по стандарту PCI DSS (проверкой соответствия требованиям стандарта) и консультационной деятельностью, связанной с оценкой соответствия требованиям стандарта PCI DSS.

- юридическое лицо, заинтересованное в выполнении исполнителем услуги проверки на соответствие требованиям стандарта PCI DSS.

- член ассоциации эмитентов банковских карт, который устанавливает и поддерживает взаимодействие с предприятиями торгово-сервисной сети, принимающей платежные карты.

- поставщик услуг сканирования, имеющий официальный статус от Совета стандартов безопасности (PCI SSC).

Заказчик — это

- лицо, занимающееся аудитом по стандарту PCI DSS (проверкой соответствия требованиям стандарта) и консультационной деятельностью, связанной с оценкой соответствия требованиям стандарта PCI DSS.

- юридическое лицо, заинтересованное в выполнении исполнителем услуги проверки на соответствие требованиям стандарта PCI DSS.

- член ассоциации эмитентов банковских карт, который устанавливает и поддерживает взаимодействие с предприятиями торгово-сервисной сети, принимающей платежные карты.

- поставщик услуг сканирования, имеющий официальный статус от Совета стандартов безопасности (PCI SSC).

Что не является дополнительной документацией стандарт PCI DSS:

- ASV - Набор документации для поставщиков услуг сканирования (ASV): руководство по программе ASV, список требований ASV, проверка соответствия статусу ASV;
- QSA - Набор документации для квалифицированных экспертов безопасности (QSA): соглашение QSA, список требований QSA;
- PFI - Набор документации для экспертов-криминалистов в индустрии платежных карт (PFI);
- Аттестация соответствия PCI DSS – торговые организации. Версия 2.0 (PCI DSS Attestation of Compliance – Merchants v2.0).

Сколько требований детально описывает стандарт безопасности данных индустрии платежных карт (PCI DSS v2.0):

- 12;
- 14;
- 6;
- 19.

Какой ключ доступен всем для проверки цифровой подписи под документом?

- закрытый;
- открытый;
- внутренний;
- общий.

Что подразумевается под термином аутентичность информации?

- Целостность информации;
- Невозможность отказа от авторства;
- Подлинность авторства;
- Все ответы правильные.

Программа обеспечения безопасности MasterCard:

- Программа Account Information Security (AIS);
- Payment Card Industry Data Security Standard (PCI DSS);
- Программа Site Data Protection (SDP);
- Credit Card Information Security Guidelines.

Программа обеспечения безопасности Visa:

- Программа Account Information Security (AIS);
- Payment Card Industry Data Security Standard (PCI DSS);
- Программа Site Data Protection (SDP);
- Credit Card Information Security Guidelines.

Что входит в пакет документов СТО БР ИББС:

- СТО БР ИББС-1.0-2014. «Общие положения»;
- СТО БР ИББС-1.1-2007. «Аудит информационной безопасности»;
- 1 и 2;
- нет правильного ответа.

Банком России разработаны и введены следующие рекомендации в области стандартизации ИБ, исключите лишний пункт:

- РС БР ИББС-2.0-2007. «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0»;
- РС БР ИББС-2.1-2007. «Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0»;
- РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности»;
- СТО БР ИББС-1.2-2014. «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 (4 редакция)».

В основу системы обеспечения информационной безопасности заложен Цикл Деминга, используемый в управлении качеством, исключите лишний пункт:

- Планирование СОИБ;

- Реализация СОИБ;
- Проверка СОИБ;
- Сертифицирование СОИБ.

Что такое Электронный документ?

- Документ, зафиксированный на электронном носителе и предназначенный для передачи во времени и пространстве с использованием средств вычислительной техники и электросвязи с целью хранения и общественного использования;

- Форма представления информации в целях её подготовки, отправления, получения или хранения с помощью электронных технических средств, зафиксированная на магнитном диске, магнитной ленте, лазерном диске и ином электронном материальном носителе;

- Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

- Все ответы правильные.

Что такое Электронная подпись?

- предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий;

- процедура проверки подлинности;

- это пароль, действительный только для одного сеанса аутентификации;

- реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи.

Что такое Открытый ключ?

- ключ, известный только своему владельцу. Только сохранение пользователем в тайне своего закрытого ключа гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего.

- ключ, который может быть опубликован и используется для проверки подлинности подписанного документа, а также для предупреждения мошенничества со стороны заверяющего лица в виде отказа его от подписи документа.

- ключи, используемые в симметричных алгоритмах (шифрование, выработка кодов аутентичности).

- нет правильного ответа.

Что такое Закрытый ключ?

- ключ, известный только своему владельцу. Только сохранение пользователем в тайне своего закрытого ключа гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего.

- ключ, который может быть опубликован и используется для проверки подлинности подписанного документа, а также для предупреждения мошенничества со стороны заверяющего лица в виде отказа его от подписи документа.

- ключи, используемые в симметричных алгоритмах (шифрование, выработка кодов аутентичности).

- нет правильного ответа.

Что не является протоколом распределения ключей:

- Протокол Нидхем-Шрёдера;

- Протокол Отвея-Рииса;

- Протокол Эль-Гамала;

- Протокол Диффи — Хеллмана.

Что обычно в себя включает схема электронной подписи?

- алгоритм генерации ключевых пар пользователя

- функцию проверки подписи

- ничего из вышперечисленного

- все из вышперечисленного

Как называется преобразование входного массива данных произвольной длины в выходную

битовую строку фиксированной длины? (использует одностороннюю функцию)

- Разбиение входного массива
- Хеширование
- Сжатие
- Сдвиг

#### **14.1.2. 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

#### **14.1.3. 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

#### **14.1.4. 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

### **14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов**

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

### **14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов**

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

#### **Для лиц с нарушениями зрения:**

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

#### **Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

#### **Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.