рМИНИСТЕРСТВО 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

Защита информации в банковских системах

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: **5**
Семестр: **9**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	9 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	28	28	часов
4	Всего аудиторных занятий	74	74	часов
5	Из них в интерактивной форме	20	20	часов
6	Самостоятельная работа	34	34	часов
7	Всего (без экзамена)	108	108	часов
8	Подготовка и сдача экзамена	36	36	часов
9	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 9 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 23.08.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск 2018

Согласована на портале № 28254

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 15 » 5 2018 г.

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:

к.т.н. доцент кафедры 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 _____ М. В. Князева

Согласована на портале № 28254

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины является изучение и критический анализ организационной и инженерной структур используемых в банковской системе Российской Федерации (БС РФ) автоматизированных банковских систем (АБС), как платёжных, так и не платёжных, изучение технологии, практических методов и средств защиты информации в АБС.

1.2. Задачи дисциплины

– Задачи дисциплины - дать основы:

– - понимания специфики и идеологии строения банковской системы РФ с точки зрения информационной безопасности;

– - организации защиты банковской информации в АБС, эксплуатирующихся в ЦБ РФ;

– - теории и практики технологии защиты банковской информации, внедряемой ЦБ РФ, использования стандартов информационной безопасности ЦБ РФ;

– - разработки предложений по совершенствованию подсистем информационной безопасности АБС, используемых в банковских организациях РФ;

– - организации контроля уровня информационной безопасности организаций БС РФ.

2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информации в банковских системах» (Б1.Б.32.3) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Нормативная база обеспечения информационной безопасности банковской организации.

Последующими дисциплинами являются: Безопасность систем пластиковых карт.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПСК-5.5 способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы;

– ПСК-5.4 способностью участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных банковских систем;

– ПСК-5.3 способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью автоматизированных банковских систем;

– ПСК-5.2 способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем;

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

В результате изучения дисциплины обучающийся должен:

– **знать** − основы организационного и технического обеспечения мер и средств защиты информации в АБС, используемых в БС РФ; − особенности технологии защиты информации и обеспечения ИБ БС РФ; − организацию работы и нормативные документы в области обеспечения защиты информации и сертификации средств и систем защиты информации, используемых в БС РФ; − информационные технологии и существующие нормы при построении и использовании подсистем информационной безопасности в АБС РФ.

– **уметь** − анализировать уровень информационной безопасности АБС, в соответствии с требованиями стандартов, нормативных актов, методических документов в области обеспечения ИБ БС РФ; − контролировать уровень выполнения требований зашиты информации в банковской организации БС РФ; − разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации в организациях БС РФ.

– **владеть** − профессиональной терминологией в области ИБ БС РФ; − навыками работы с технической документацией по обеспечению информационной безопасности БС РФ; − знаниями по оперативному управлению деятельностью служб защиты информации в организации БС РФ; −

Согласована на портале № 28254

методами формирования требований по защите информации в рамках нормативной базы ИБ БС РФ.

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
		9 семестр
Аудиторные занятия (всего)	74	74
Лекции	28	28
Практические занятия	18	18
Лабораторные работы	28	28
Из них в интерактивной форме	20	20
Самостоятельная работа (всего)	34	34
Оформление отчетов по лабораторным работам	16	16
Проработка лекционного материала	11	11
Подготовка к практическим занятиям, семинарам	7	7
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	ра к. за	б. ра б.,	м. ра б.,	в (б ез	ре ме ко м
9 семестр						
1 Предмет дисциплины, история создания и развития банковской системы РФ, автоматизация банковской деятельности	4	0	0	2	6	ПСК-5.1, ПСК-5.2, ПСК-5.3
2 Значение информации и ее защиты, носители информации.	2	0	2	3	7	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
3 Классификация и характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях (БО) РФ (Платёжные и не платёжные). Задачи ИБ в АБС	4	2	4	4	14	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
4 Организация деятельности по обеспечению информационной безопасности в кредитных организациях. Модели угроз и	4	2	4	4	14	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4,

Согласована на портале № 28254

нарушителей.						ПСК-5.5
5 Формирование и развитие системы расчётов Банка России, элементы платежной системы ЦБ РФ, технологии построения.	2	2	0	2	6	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
6 Характеристика структуры, оценка безопасности и надёжности централизованной платёжной системы РФ, основанной на базе системы - РАБИС-НП. Банковские электронные срочные платежи (БЭСП), требования к кредитным организациям для вхождения и работе в системе БЭСП	4	4	4	4	16	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
7 Стандарты Банка России СТО БР ИББС-2014. История создания и развития, основные положения.	2	0	4	3	9	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
8 Служба информационной безопасности коммерческого банка, функции и полномочия, организация деятельности.	2	2	4	4	12	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
9 Информационная безопасность неплатёжных АБС, телекоммуникационных систем ЦБ РФ и кредитных организаций РФ	2	2	2	4	10	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
10 Контроль внедрения и эксплуатации СЗИ банковских информационных систем в соответствии со стандартами ИБ и защиты информации ЦБ РФ. Анализ и отчётность	2	4	4	4	14	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
Итого за семестр	28	18	28	34	108	
Итого	28	18	28	34	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 лекционных занятий	Компетенции
9 семестр			
1 Предмет дисциплины, история создания и развития банковской системы РФ, автоматизация банковской деятельности	Цели и задачи курса "Защита информации в банковских системах". История возникновения банковской системы России в новейшей истории, автоматизация и компьютеризации деятельности кредитных организаций. Создание специализированной структур и подразделений кредитных организаций, занимающихся вопросами безопасности и защиты информации в	4	ПСК-5.1, ПСК-5.2, ПСК-5.3

Согласована на портале № 28254

	банковской системе РФ.		
	Итого	4	
2 Значение информации и ее защиты, носители информации.	Роль информации в современном мире, виды носителей информации. Актуальность защиты информации, промышленный шпионаж. Характеристики информации	2	ПСК-5.1, ПСК-5.2, ПСК-5.4, ПСК-5.5
	Итого	2	
3 Классификация и характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях (БО) РФ (Платёжные и не платёжные). Задачи ИБ в АБС	Единое информационное пространство банка. Классификация и основные характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях. Элементы и модули АБС, информационные технологии используемые для их построения, уязвимости.	4	ПСК-5.1, ПСК-5.2, ПСК-5.5
	Итого	4	
4 Организация деятельности по обеспечению информационной безопасности в кредитных организациях. Модели угроз и нарушителей.	Организация и функционирования системы обеспечения информационной безопасности в коммерческих банках. Объекты защиты, виды угроз и типы нарушителей, менеджмент системы информационной безопасности	4	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	4	
5 Формирование и развитие системы расчётов Банка России, элементы платежной системы ЦБ РФ, технологии построения.	История формирования и развития, модернизации, эксплуатации и модернизации платежной системы Банка России, элементы входящие в ее состав. Региональная автоматизированная банковская информационная система "РАБИС-НП", принципы и порядок функционирования.	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	2	
6 Характеристика структуры, оценка безопасности и надёжности централизованной платёжной системы РФ, основанной на базе системы - РАБИС-НП. Банковские электронные срочные платежи (БЭСП), требования к кредитным организациям для вхождения и работе в системе БЭСП	Управление рисками платежной системы Банка России, обеспечение безопасности и надёжности ее функционирования. Система банковских электронные срочные платежи (БЭСП), требования Банка России к кредитным организациям для участия в системе, организация их деятельности.	4	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	4	
7 Стандарты Банка России СТО БР ИББС-2014. История создания и развития, основные положения.	Отраслевые стандарты Банка России по обеспечению информационной безопасности коммерческих банков, состав (обязательные и рекомендательные элементы), основные положения и требования, порядок оценки	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5

Согласована на портале № 28254

	кредитных организаций в соответствии с указанными нормативными документами.		
	Итого	2	
8 Служба информационной безопасности коммерческого банка, функции и полномочия, организация деятельности.	Порядок организации деятельности специализированного подразделения деятельности коммерческого банка - службы информационной безопасности. Роль, функции полномочия и ответственность службы информационной безопасности, нормативные документы, регламентирующие деятельность подразделения и уполномоченных сотрудников.	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	2	
9 Информационная безопасность неплатёжных АБС, телекоммуникационных систем ЦБ РФ и кредитных организаций РФ	Анализ средств защиты информации в неплатёжных автоматизированных банковских системах, телекоммуникационных системах ЦБ РФ и кредитных организаций, организация деятельности и используемая нормативная база.	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	2	
10 Контроль внедрения и эксплуатации СЗИ банковских информационных систем в соответствии со стандартами ИБ и защиты информации ЦБ РФ. Анализ и отчётность	Способы и методы организации контроля внедрения, эксплуатации и модернизации СЗИ банковских информационных систем, анализ возможных проблем и уязвимостей, отчетность уполномоченным органам. Использование и разработка нормативной базы кредитной организации в соответствии со стандартами по информационной безопасности и защите информации Банка России.	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	2	
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	6	7	8	9	10
Предшествующие дисциплины										
1 Нормативная база обеспечения информационной безопасности банковской организации	+		+	+	+	+		+	+	
Последующие дисциплины										
1 Безопасность систем пластиковых карт			+	+	+	+		+		

Согласована на портале № 28254

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.	Практ. зан.	Лаб. раб.	Сам. раб.	
ПСК-5.5	+	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Реферат
ПСК-5.4	+	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Реферат
ПСК-5.3	+	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Реферат
ПСК-5.2	+	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Реферат
ПСК-5.1	+	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Реферат

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 лабораторные занятия, ч	Интерактивные лекции, ч	Всего, ч
9 семестр				
Работа в команде	2			2
IT-методы		4	8	12
Решение ситуационных задач	2	4		6
Итого за семестр:	4	8	8	20

Согласована на портале № 28254

Итого	4	8	8	20

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость (в часах)	Компетенции
9 семестр			
2 Значение информации и ее защиты, носители информации.	Основные направления и объекты защиты информации в кредитных организациях, используемые методы и способы указанной деятельности.	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	2	
3 Классификация и характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях (БО) РФ (Платёжные и не платёжные). Задачи ИБ в АБС	Автоматизированные банковские системы, принципы построения и организации функционирования, потенциальные уязвимости, мероприятия по обеспечению их защиты.	4	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	4	
4 Организация деятельности по обеспечению информационной безопасности в кредитных организациях. Модели угроз и нарушителей.	Классификация и ранжирование объектов защиты, определение видов угроз и типов нарушителей информационной безопасности, организация системы менеджмента и функционирования системы информационной безопасности.	4	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	4	
6 Характеристика структуры, оценка безопасности и надёжности централизованной платёжной системы РФ, основанной на базе системы - РАБИС-НП. Банковские электронные срочные платежи (БЭСП), требования к кредитным организациям для вхождения и работе в системе БЭСП	Система платежей Банка России, банковские электронные срочные платежи (БЭСП). Обеспечение информационной безопасности и защиты информации в платежной системе Банка России.	4	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	4	
7 Стандарты Банка России СТО БР ИББС-2014. История создания и развития, основные положения.	Отраслевые стандарты Банка России по обеспечению информационной безопасности, их реализации в практической деятельности кредитных организаций	4	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	4	
8 Служба информационной безопасности	Организация практической деятельности службы информационной безопасности в кредитной организации, должностные обязанности,	4	ПСК-5.1, ПСК-5.2, ПСК-5.3,

Согласована на портале № 28254

коммерческого банка, функции и полномочия, организация деятельности.	ответственность ее руководителя и сотрудников.		ПСК-5.4, ПСК-5.5
	Итого	4	
9 Информационная безопасность неплатёжных АБС, телекоммуникационных систем ЦБ РФ и кредитных организаций РФ	Организация систем защиты информации в неплатёжных и телекоммуникационных банковских системах, особенности создания и использования.	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	2	
10 Контроль внедрения и эксплуатации СЗИ банковских информационных систем в соответствии со стандартами ИБ и защиты информации ЦБ РФ. Анализ и отчётность	Использование средств защиты информации в АБС кредитных организаций, практическая реализация мероприятий, направленных на обеспечение информационной безопасности.	4	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	4	
Итого за семестр		28	

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 (в часах)	Формируемые компетенции
9 семестр			
3 Классификация и характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях (БО) РФ (Платёжные и не платёжные). Задачи ИБ в АБС	Классификация и характеристики АБС	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	2	
4 Организация деятельности по обеспечению информационной безопасности в кредитных организациях. Модели угроз и нарушителей.	Особенности разработки, внедрения и практического использования методов и средств защиты информации (СЗИ)	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	2	
5 Формирование и развитие системы расчётов Банка России, элементы платежной системы ЦБ РФ, технологии построения.	Организация и функционирование платежной системы Банка России, частных платежных систем, принципы и порядок деятельности	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	2	
6 Характеристика структуры, оценка	Структура и элементы, оценка безопасности и надёжности централизованной платёжной	4	ПСК-5.1, ПСК-5.2,

Согласована на портале № 28254

безопасности и надёжности централизованной платёжной системы РФ, основанной на базе системы - РАБИС-НП. Банковские электронные срочные платежи (БЭСП), требования к кредитным организациям для вхождения и работе в системе БЭСП	системы РФ,управление рисками.		ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	4	
8 Служба информационной безопасности коммерческого банка, функции и полномочия, организация деятельности.	Организация деятельности подразделений кредитных организаций, обеспечивающих информационную безопасность, защиту информации и персональных данных. Цели и задачи данных подразделений, полномочия, права и обязанности их сотрудников.	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	2	
9 Информационная безопасность неплатёжных АБС, телекоммуникационных систем ЦБ РФ и кредитных организаций РФ	Обеспечение защиты информации в неплатёжных и телекоммуникационных банковских системах (Банка России, кредитных организации). Принципы организации, порядок функционирования, специфика деятельности.	2	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	2	
10 Контроль внедрения и эксплуатации СЗИ банковских информационных систем в соответствии со стандартами ИБ и защиты информации ЦБ РФ. Анализ и отчётность	Организация эффективной системы использования и совершенствования средств защиты информации в АБС кредитных организаций обеспечение их соответствия отраслевым стандартам и требованиям Банка России.	4	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5
	Итого	4	
Итого за семестр		18	

9. Самостоятельная работа

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

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	трудоемкость,	формируемые компетенции	Формы контроля
9 семестр				
1 Предмет дисциплины, история создания и развития банковской системы РФ, автоматизация банковской	Проработка лекционного материала	2	ПСК-5.1, ПСК-5.2	Опрос на занятиях, Тест
	Итого	2		

Согласована на портале № 28254

деятельности				
2 Значение информации и ее защиты, носители информации.	Проработка лекционного материала	1	ПСК-5.1, ПСК-5.2, ПСК-5.4, ПСК-5.5, ПСК-5.3	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Оформление отчетов по лабораторным работам	2		
	Итого	3		
3 Классификация и характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях (БО) РФ (Платёжные и не платёжные). Задачи ИБ в АБС	Подготовка к практическим занятиям, семинарам	1	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5	Выступление (доклад) на занятии, Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
4 Организация деятельности по обеспечению информационной безопасности в кредитных организациях. Модели угроз и нарушителей.	Подготовка к практическим занятиям, семинарам	1	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
5 Формирование и развитие системы расчётов Банка России, элементы платежной системы ЦБ РФ, технологии построения.	Подготовка к практическим занятиям, семинарам	1	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Итого	2		
6 Характеристика структуры, оценка безопасности и надёжности централизованной платёжной системы РФ, основанной на базе системы - РАБИС-НП. Банковские электронные срочные платежи (БЭСП), требования к кредитным организациям для вхождения и работе в системе БЭСП	Подготовка к практическим занятиям, семинарам	1	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
7 Стандарты Банка России СТО БР ИББС-2014. История создания и развития, основные	Проработка лекционного материала	1	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4,	Опрос на занятиях, Отчет по индивидуальному заданию, Реферат, Тест
	Оформление отчетов по лабораторным работам	2		

Согласована на портале № 28254

положения.	Итого	3	ПСК-5.5	
8 Служба информационной безопасности коммерческого банка, функции и полномочия, организация деятельности.	Подготовка к практическим занятиям, семинарам	1	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
9 Информационная безопасность неплатёжных АБС, телекоммуникационных систем ЦБ РФ и кредитных организаций РФ	Подготовка к практическим занятиям, семинарам	1	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
10 Контроль внедрения и эксплуатации СЗИ банковских информационных систем в соответствии со стандартами ИБ и защиты информации ЦБ РФ. Анализ и отчётность	Подготовка к практическим занятиям, семинарам	1	ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
Итого за семестр		34		
	Подготовка и сдача экзамена	36		Экзамен
Итого		70		

10. Курсовая работа (проект)

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
9 семестр				
Выступление (доклад) на занятии	3	4	5	12
Опрос на занятиях	5	5	5	15
Отчет по индивидуальному заданию	5	5	5	15

Согласована на портале № 28254

Реферат	6	6	6	18
Тест	3	3	4	10
Итого максимум за период	22	23	25	70
Экзамен				30
Нарастающим итогом	22	45	70	100

11.2. Пересчет баллов в оценки за контрольные точки

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

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

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

11.3. Пересчет суммы баллов в традиционную и международную оценку

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

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

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

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. "Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" СТО БР ИББС-1.0-2014" (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399) [Электронный ресурс] [Электронный ресурс]: — Режим доступа: http://www.garant.ru/products/ipo/prime/doc/70567254/ (дата обращения: 19.05.2018).

2. "Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014" СТО БР ИББС-1.2-2014" (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399) [Электронный ресурс] [Электронный ресурс]: — Режим доступа: http://www.garant.ru/products/ipo/prime/doc/70567284/ (дата обращения: 19.05.2018).

3. "Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности" СТО БР ИББС-1.1-2007" (принят и введен в действие Распоряжением Банка России от 28.04.2007 N Р-345)

Согласована на портале № 28254

[Электронный ресурс] [Электронный ресурс]: — Режим доступа: http://www.garant.ru/products/ipo/prime/doc/487314/ (дата обращения: 19.05.2018).

12.2. Дополнительная литература

1. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4 [Электронный ресурс] - Режим доступа: http://znanium.com/catalog/product/402686 , дата обращения: 29.05.2018.
2. Информационная безопасность и защита информации: Учебное пособие. / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380 [Электронный ресурс] - Режим доступа: http://znanium.com/catalog/product/763644 , дата обращения: 29.05.2018.

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Сопов М.А. Учебно-методические указания по практическим, семинарским занятиям по дисциплине «Правовое обеспечение информационной безопасности». 2012. – 6с. [Электронный ресурс] [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/metodicheskie_ukazaniya_k_praktikam.pdf , дата обращения: 29.05.2018.
2. Мирных Ю.Ф. Учебно-методические указания по решению задач по дисциплине «Защита информации в банковских системах». 2013. – 34с. [Электронный ресурс] [Электронный ресурс] - Режим доступа: http://edu.fb.tusur.ru/mod/resource/view.php?id=787 , дата обращения: 29.05.2018.
3. Мирных Ю.Ф. Учебно-методические указания по лабораторным работам по дисциплине «Защита информации в банковских системах». 2013. – 47с [Электронный ресурс] [Электронный ресурс] - Режим доступа: http://edu.fb.tusur.ru/mod/resource/view.php?id=788 , дата обращения: 29.05.2018.
4. Шелупанов А.А., Сопов М.А. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.3. Издание седьмое, перераб. и допол. - Томск : В-Спектр, 2011. – 220с. ISBN 978-5-91191-229-5 [Электронный ресурс] [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-3ch.pdf , дата обращения: 29.05.2018.

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. СПС Консультант+, www.consultant.ru/
2. СПС Гарант, www.garant.ru
3. Центральный Банк РФ, www.cbr.ru/

Согласована на портале № 28254

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 Интернет-технологий и информационно-аналитической деятельности, учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Экран раздвижной;
- Мультимедийный проектор View Sonic PJD5154 DLP;
- Компьютеры AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb (15 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- GPSS Studio;
- Kaspersky endpoint security;
- VirtualBox;
- Visio;
- Visual Studio.

Лаборатория Безопасности сетей ЭВМ и сетевых компьютерных технологий/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 Microtik 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;

Согласована на портале № 28254

- 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:
- Cisco Packet Tracer;
- Система мониторинга Zabbix;
- Kaspersky endpoint security;
- Microsoft Windows 10;
- Visual Studio Essentials 2017;
- Межсетевой экран ИКС Lite.

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория Безопасности сетей ЭВМ и сетевых компьютерных технологий/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 Microtik 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:
- Cisco Packet Tracer;
- Система мониторинга Zabbix;
- Kaspersky endpoint security;
- Microsoft Windows 10;
- Visual Studio Essentials 2017;
- XSpider;
- Межсетевой экран ИКС Lite.

Лаборатория "Интернет-технологий и информационно-аналитической деятельности"

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

Согласована на портале № 28254

типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Экран раздвижной;
- Мультимедийный проектор View Sonic PJD5154 DLP;
- Компьютеры AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb (15 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- GPSS Studio;
- Kaspersky endpoint security;
- Microsoft SQL Server 2014;
- Microsoft Windows 10;
- VirtualBox.

13.1.4. 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 зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей 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

Согласована на портале № 28254

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

1. Какая информация в соответствии с действующим законодательством может быть отнесена к категории общедоступной:

а. информация о нормативно – правовых актах, затрагивающая права, свободы и обязанности граждан;

б. информация об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

в. информация о государственных золотовалютных резервах РФ;

г. все виды информации, указанные в п.п. а-в

2. В соответствии с нормативными актами регулятора – Банка России к какому виду относятся риски банков, связанные с осуществлением контроля информационных потоков и обеспечением информационной безопасности:

а. рыночный риск;

б. правовой риск;

в. операционный риск;

г. кредитный риск;

д. риск потери деловой репутации.

3. Какие виды банков вправе осуществлять свою деятельность на территории РФ в соответствии с действующим законодательством:

а. универсальные банки;

б. инвестиционные банки;

в. региональные банки;

г. ссудно-сберегательные кассы;

д. банки, указанные в п.п. а-в.

4. Какие из указанных целей стандартизации деятельности по обеспечению ИБ кредитных организаций РФ относятся к категории основных:

а. развитие и укрепление банковской системы РФ, повышение доверия к ней;

б. достижение адекватности мер защиты реальным угрозам ИБ;

в. предотвращение и (или) снижение ущерба от инцидентов ИБ;

г. цели, указанные в п.п. а-б;

д. цели, указанные в п.п. а-в.

5. Представителям каких государственных органов могут выдаваться справки по счетам юридических лиц и предпринимателей без образования юридического лица:

а. судам общей юрисдикции и арбитражным судам;

б. налоговым и таможенным органам;

в. органам внутренних дел при осуществлении ими функций по выявлению, предупреждению и пресечению налоговых преступлений;

г. субъектам, указанных в п.п. а-б;

д. субъектам, указанным в п.п. а-в.

6. Какая из указанной информации не подлежит обязательному раскрытию банками неограниченному кругу пользователей в соответствии с действующими нормативными актами банка России:

а. информация о составе органов управления кредитной организации;

б. информация о решениях принятых исполнительными органами кредитной организации;

в. годовая бухгалтерская (финансовая) отчетность банка;

г. расчет собственных средств (капитала) банка;

д. информация, указанная в п.п. в-г.

Согласована на портале № 28254

7. Информация может оцениваться как следующий вид активов компании:

а. внеоборотные активы;

б. нематериальные активы;

в. оборотные активы;

г. товарно -материальные ценности;

8. К основным характеристикам финансовой информации могут быть отнесены следующие:

а.уместность;

б. надежность;

в. важность;

г. характеристики, указанные в п.п. а-б;

д. характеристики, указанные в п.п. а-в.

9. Единое информационное пространство банка основывается на следующих принципах:

а. открытости;

б. ограничения количества пользователей;

в. защищенности;

г. на принципах, указанных в п.а и п.в;

д. на принципах, указанных в п.п.а-в.

10. Автоматизированные банковские системы могут быть построены на основе следующих технологий:

а. платежных;

б. операционных;

в. документарных;

г. технологий, указанных в п.п. а-в;

д. технологий, указанных в п.п. б-в.

11. К настоящему времени экспертами выделяются следующее количество поколений российских автоматизированных банковских систем (АБС):

а. четыре;

б. пять;

в. шесть;

д. семь.

12. Какие функциональные модули, как правило, включаются в состав АБС коммерческих банков:

а. модуль расчетно-кассового обслуживания клиентов;

б. модуль кредитных операций клиентов;

в. модуль хозяйственных договоров и обеспечения внутрибанковской деятельности;

г. функциональные модули, указанные в п. а-б;

д. функциональные модули, указанные в п. а-в.

13. Какие информационные угрозы могут быть характерны доступным компонентам АБС:

а. несанкционированный доступ к ресурсам и данным системы

б. подмена сетевых адресов;

в. отказ в обслуживании;

г. атака на уровне приложений;

д. все информационные угрозы, указанные в п.п. а- г.

14. Что из указанного не относится к возможным причинам появления уязвимостей АБС:

а. отсутствие гарантий конфиденциальности и целостности передаваемых данных;

б. утеря актуальности разработанной политики ИБ или некорректная (неполная) ее реализация;

в. отсутствие или недостаточный уровень защиты от несанкционированного доступа (антивирусы, организация и функционирование системы контроля доступа, систем обнаружения атак);

г. низкий (непрофессиональный) уровень администрирования АБС и сетевых приложений;

д. относятся все причины, указанные в п.п. а-г.

15. Платежная система Банка России является:

а. централизованной;

Согласована на портале № 28254

б. децентрализованной;

в. распределенной.

16. Какая из систем расчетов (элементов) не входит в состав платежной системы Банка России:

а. система внутрирегиональных электронных расчетов (система ВЭР);

б. система межрегиональных электронных расчетов (система МЭР);

в. система международных электронных расчетов (система МДЭР);

г. система банковских электронных срочных платежей (система БЭСП);

д. входят все системы расчетов, указанные в п.п. а-г.

17. Какие из указанных источников угроз информационной безопасности (ИБ) Банка не относятся к категории основных:

а. работники банка, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий;

б. работники банка, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками банка, но осуществляющие попытки несанкционированного доступа в АБС;

в. криминальные элементы и террористы;

г. неблагоприятные события природного, техногенного и социального характера;

д. к основным, относятся все категории угроз, указанные в п.п. а-г..

18. Политика ИБ банка формируется на основе следующих элементов:

а. требований законодательства РФ и нормативных актов ЦБ РФ;

б. интересов и бизнес – целей банка;

в. накопленного в организации опыта в области обеспечения ИБ;

г. на основе элементов, указанных в п.а и п.в;

д. на основе элементов, указанных в п.п. а-в.

19. Какой из указанных органов корпоративного управления банка может иметь полномочия по утверждению Политики информационной безопасности данной кредитной организации:

а. Наблюдательный Совет;

б. Правление;

г. Председатель Правления;

д. любой из указанных органов управления.

20. Какой из указанных документов, входящих в пакет стандарта СТО БР ИББС (5-актуальная версия) имеет рекомендательный характер для использования кредитными организациями:

а. БР ИББС-1.0-2014. «Общие положения» (5 редакция);

б. БР ИББС-1.1-2017. «Аудит информационной безопасности» СТО БР ИББС-1.0-2014. «Общие положения» (5 редакция);

в. БР ИББС-2.2-2009 «Методика оценки рисков нарушения информационной безопасности»;

г. БР ИББС-1.2-2014 «Методика оценки соответствия информационной безопасности организаций банковской системы РФ требованиям СТО БР ИББС-1.0-2014 (4 редакция).

21. В соответствии с нормативными документами Банка России оператор по переводу денежных средств – банк обеспечивает реализацию запрета выполнения одним лицом в один момент времени следующих ролей:

а. ролей, связанных с проектированием (разработкой) и созданием (модернизацией) объекта информационной инфраструктуры;

б. ролей, связанных с эксплуатацией объекта информационной инфраструктуры в части его использования по назначению и в части его технического обслуживания или ремонта;

в. Ролей, связанных с созданием (модернизацией) объекта информационной инфраструктуры и его эксплуатации;

г. ролей, указанных в п.а и п.б;

д. ролей, указанных в п.б и п.в.

22. В соответствии с требованиями нормативных документов ЦБ РФ служба информационной безопасности банка при осуществлении переводов денежных средств должна

Согласована на портале № 28254

быть наделена следующими полномочиями:

а. осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации;

б. определять требования к техническим средствам защиты информации и организационным мерам защиты информации;

в. определять порядок эксплуатации технических средств защиты информации и соответствующего программного обеспечения;

г. полномочиями, указанными в п.п. а-б;

д. полномочиями, указанными в п.п. а-в.

14.1.2. Экзаменационные вопросы

1. Предмет и задачи дисциплины «Защита информации в банковских системах». Нормативно – правовые документы, регламентирующие вопросы защиты информации и информационной безопасности.

2. Банк России как регулятор деятельности коммерческих банков. Нормативная база обеспечения деятельности банков в вопросах защиты информации и информационной безопасности.

3. Операционный риск в деятельности кредитных организаций. Порядок управления и оценки указанным видом риска.

4. Виды информации, возможные ограничения ее использования и распространения. Перечень сведений, который может быть отнесен к банковской тайне, порядок их представления сторонним лицам.

5. Информация, ее роль в современном мире, носители информации и их виды. Порядок защиты носителей информации, его отличия от мероприятий по защите информации.

6. Требования к кредитным организациям при осуществлении переводов денежных средств (Положение ЦБ РФ № 382-П).

7. Информация как нематериальные активы компании, показатели оценки информации как соответствующих ресурсов.

8. Финансовая информация (понятие, цели получения, виды классификации).

9. История развития (поколения) АБС в банковской системе РФ, общие характеристики автоматизированных банковских систем, используемых в кредитных организациях.

10. Элементы и программно - функциональные модули АБС, виды информационных банковских технологий, используемых при создании АБС.

11. Уязвимости АБС, архитектура систем защиты и способы защиты от неправомерных действий.

12. Платежная система РФ, цели и основные элементы, участники, нормативно – правовая база регламентирующие соответствующие вопросы.

13. Платежная система Банка России - история развития, основные задачи, отдельные элементы и системы расчетов, входящие в ее состав.

14. Система банковских электронных срочных платежей (БЭСП) Банка России – порядок, условия и принципы функционирования, требования к участникам.

15. Региональная автоматизированная банковская информационная система (РАБИС – НП) - назначение, принципы построения, участники расчетов и пользователи, распределение функций.

16. Отраслевые стандарты по информационной безопасности Банка России СТО БР ИББС. Основные положения, разделы и элементы, история развития.

17. Формирование перечня конфиденциальных сведений и информации банка, модели угроз и нарушителей информационной безопасности.

18. Определение потенциальных каналов утечки (перехвата) конфиденциальной информации банка, перечня и состава прикладных методов защиты информации.

19. Ответственность, полномочия и права службы информационной безопасности банка, ее сотрудников и руководителя.

20. Организация системы обеспечения информационной безопасности банка (система информационной безопасности, система менеджмента информационной безопасности).

21. Обработка кредитными организациями информации, содержащей персональные данные. Обеспечение информационной безопасности соответствующих банковских технологических

Согласована на портале № 28254

процессов.

22. Аудит информационной безопасности кредитных организаций (концепция, основные принципы, менеджмент программы, последовательность и этапы проведения).

23. Организация системы информационной безопасности для защиты информации при осуществлении кредитными организациями дистанционного банковского обслуживания (ДБО) своих клиентов.

24. Применение средств защиты (антивирусных программ) от вредоносного кода (ВК) в целях защиты информации при осуществлении банковской деятельности.

14.1.3. Темы индивидуальных заданий

- организационные основы банковской деятельности, функции подразделений безопасности банков, вопросы соблюдения прав и свобод личности при решении задач обеспечения безопасности;
- правовые основы охраны коммерческой тайны и защиты конфиденциальной банковской информации;
- источники и угрозы утечки конфиденциальной информации в банке;
- методы защиты банковской информации в автоматизированных системах обработки;
- принципы защиты персональных платежей, в том числе с использованием электронных пластиковых карт, и обеспечения безопасности электронных межбанковских расчётов;
- технические и инженерно-технические средства защиты информации;
- административные и аппаратно-программные методы защиты, в том числе системы защиты

автоматизированных рабочих мест.

14.1.4. Темы рефератов

1. Основные направления и перспективы развития национальной платежной системы РФ, глобальные вызовы и угрозы.
2. Обеспечение безопасности операций по переводу денежных средств и соответствующей информации при проведении платежей через расчетную сеть Банка России
3. Отраслевые стандарты Банка России СТО БР ИББС-2014, порядок проведение банками самооценки соответствия требованиям указанных документов.
4. Основные мероприятия, меры и способы защиты, используемые кредитными организациями России, в целях предотвращения несанкционированных действий и проникновения в автоматизированные банковские системы.
5. История развития частных платежных систем в новейшей истории России.
6. Организация деятельности служб и подразделений кредитных организаций, обеспечивающих информационную безопасность и защиту информации в банковских системах, требования к их руководителям и сотрудникам.
7. Мировой опыт использования средств защиты информации в практической деятельности коммерческих банков.

14.1.5. Темы докладов

1. Надзор Банка России за деятельностью платежных систем в РФ, обеспечение информационной безопасности критически важной инфраструктуры экономики.
2. Аудит информационной безопасности в кредитных организациях.
3. Использование типовых моделей угроз и нарушителей информационной безопасности, определенных отраслевыми стандартами ЦБ РФ, в практической деятельности коммерческих банков.
4. Обеспечение защиты персональных данных клиентов кредитных организаций при использовании системы интернет - банкинга.
5. Использование объектных технологий при создании и совершенствовании автоматизированных банковских систем.
6. Дистанционное банковское обслуживание клиентов кредитными организациями, обеспечение безопасности проводимых операций и защиты соответствующей информации.
7. Организация системы мероприятий, применение отдельных мер защиты от вредоносного кода (ВК) в целях предотвращения сбоев в работе автоматизированных банковских систем.

Согласована на портале № 28254

14.1.6. Темы опросов на занятиях

Цели и задачи курса "Защита информации в банковских системах". История возникновения банковской системы России в новейшей истории, автоматизация и компьютеризации деятельности кредитных организаций. Создание специализированной структур и подразделений кредитных организаций, занимающихся вопросами безопасности и защиты информации в банковской системе РФ.

Единое информационное пространство банка. Классификация и основные характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях. Элементы и модули АБС, информационные технологии используемые для их построения, уязвимости.

Организация и функционирования системы обеспечения информационной безопасности в коммерческих банках. Объекты защиты, виды угроз и типы нарушителей, менеджмент системы информационной безопасности

История формирования и развития, модернизации, эксплуатации и модернизации платежной системы Банка России, элементы входящие в ее состав. Региональная автоматизированная банковская информационная система "РАБИС-НП", принципы и порядок функционирования.

Управление рисками платежной системы Банка России, обеспечение безопасности и надёжности ее функционирования.

Система банковских электронные срочные платежи (БЭСП), требования Банка России к кредитным организациям для участия в системе, организация их деятельности.

Порядок организации деятельности специализированного подразделения деятельности коммерческого банка - службы информационной безопасности. Роль, функции полномочия и ответственность службы информационной безопасности, нормативные документы, регламентирующие деятельность подразделения и уполномоченных сотрудников.

Анализ средств защиты информации в неплатёжных автоматизированных банковских системах, телекоммуникационных системах ЦБ РФ и кредитных организаций, организация деятельности и используемая нормативная база.

Способы и методы организации контроля внедрения, эксплуатации и модернизации СЗИ банковских информационных систем, анализ возможных проблем и уязвимостей, отчетность уполномоченным органам. Использование и разработка нормативной базы кредитной организации в соответствии со стандартами по информационной безопасности и защите информации Банка России.

Роль информации в современном мире, виды носителей информации. Актуальность защиты информации, промышленный шпионаж. Характеристики информации

Отраслевые стандарты Банка России по обеспечению информационной безопасности коммерческих банков, состав (обязательные и рекомендательные элементы), основные положения и требования, порядок оценки кредитных организаций в соответствии с указанными нормативными документами.

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.

Согласована на портале № 28254

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

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.

Согласована на портале № 28254