МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации в банковских системах

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Направленность (профиль) / специализация: **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **5, 6**
Семестр: **10, 11**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	10 семестр	11 семестр	Всего	Единицы
1	Лекции	4	2	6	часов
2	Практические занятия	2	4	6	часов
3	Всего аудиторных занятий	6	6	12	часов
4	Самостоятельная работа	30	26	56	часов
5	Всего (без экзамена)	36	32	68	часов
6	Подготовка и сдача зачета	0	4	4	часов
7	Общая трудоемкость	36	36	72	часов
				2.0	З.Е.

Контрольные работы: 11 семестр - 1
Зачёт: 11 семестр

Томск

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от «26» 11 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 38.05.01 Экономическая безопасность, утвержденного 16.01.2017 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

старший преподаватель Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)	_____	О. В. Кочетков
Заведующий обеспечивающей каф. КИБЭВС	_____	А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ЗиВФ	_____	И. В. Осипов
Заведующий выпускающей каф. КИБЭВС	_____	А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)	_____	А. А. Конев
Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)	_____	К. С. Сарин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

изучение и анализ структуры, технических и программных средств, в том числе используемых в целях обеспечения информационной безопасности, автоматизированных банковских систем (АБС), применяемых в деятельности Банка России и коммерческих банков, изучение принципов и технологий их работы

изучение порядка организации и функционирования системы информационной безопасности, средств и практических методов защиты информации в кредитных организациях

1.2. Задачи дисциплины

– общие принципы построения банковской системы РФ, ее специфические особенности в вопросах обеспечения информационной безопасности

– порядок организации деятельности системы обеспечения информационной безопасности в коммерческих банках, формирования и реализации политики информационной безопасности

– требования нормативно - правовых документов, отраслевых стандартов Банка России по вопросам функционирования системы информационной безопасности кредитных организаций, порядок оценки и самооценки ее соответствия указанным требованиям

– теоретические подходы и состав практических мероприятий, используемых кредитными организациями для обеспечения защиты банковской информации и деятельности автоматизированных банковских систем

2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информации в банковских системах» (Б1.Б.06.06) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Защита информации в банковских системах, Бухгалтерский учет, Деньги, кредит, банки, Защищенный электронный документооборот, Информационные системы в экономике, Контроль и ревизия, Методы и средства защиты информации, Мировая экономика и международные отношения, Надзорные, правоохранительные и финансовые органы, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Основы финансового права, Оценка рисков.

Последующими дисциплинами являются: Защита информации в банковских системах, Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-32 способностью проводить анализ возможных экономических рисков и давать им оценку, составлять и обосновывать прогнозы динамики развития основных угроз экономической безопасности ;

– ПК-34 способностью проводить комплексный анализ угроз экономической безопасности при планировании и осуществлении инновационных проектов;

– ПК-40 способностью осуществлять экспертную оценку факторов риска, способных создавать социально-экономические ситуации критического характера, оценивать возможные экономические потери в случае нарушения экономической и финансовой безопасности, определять необходимые компенсационные резервы ;

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

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		10 семестр	11 семестр
Аудиторные занятия (всего)	12	6	6
Лекции	6	4	2
Практические занятия	6	2	4
Самостоятельная работа (всего)	56	30	26
Проработка лекционного материала	26	12	14
Подготовка к практическим занятиям, семинарам	30	18	12
Всего (без экзамена)	68	36	32
Подготовка и сдача зачета	4	0	4
Общая трудоемкость, ч	72	36	36
Зачетные Единицы	2.0		

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
10 семестр					
1 Предмет дисциплины, история создания и развития банковской системы РФ, автоматизация банковской деятельности. Значение информации и ее защиты, носители информации. Организация деятельности по обеспечению информационной безопасности в кредитных организациях. Модели угроз и нарушителей.	1	0	4	5	ПК-32, ПК-34, ПК-40
2 Формирование и развитие системы расчётов Банка России, элементы платежной системы ЦБ РФ, технологии построения. Характеристика структуры, оценка без-	1	1	8	10	ПК-32, ПК-34, ПК-40

опасности и надёжности централизованной платёжной системы РФ. Сервисы срочных и несрочных платежей, другие платежные системы и сервисы Банка России , требования к кредитным организациям для осуществления деятельности в указанных системах.					
3 Классификация и характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях РФ (платёжные и не платёжные). Задачи ИБ в АБС. Информационная безопасность неплатёжных АБС, телекоммуникационных систем ЦБ РФ и кредитных организаций РФ.	1	1	8	10	ПК-32, ПК-34, ПК-40
4 Стандарты Банка России СТО БР ИББС-2014. История создания и развития, основные положения.	1	0	10	11	ПК-32, ПК-34, ПК-40
Итого за семестр	4	2	30	36	
11 семестр					
5 Служба информационной безопасности коммерческого банка, функции и полномочия, организация деятельности.	1	2	12	15	ПК-32, ПК-34, ПК-40
6 Контроль внедрения и эксплуатации СЗИ банковских информационных систем в соответствии со стандартами ИБ и защиты информации ЦБ РФ. Анализ и отчётность	1	2	14	17	ПК-32, ПК-34, ПК-40
Итого за семестр	2	4	26	32	
Итого	6	6	56	68	

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
10 семестр			
1 Предмет дисциплины, история создания и развития банковской системы РФ, автоматизация банковской деятельности. Значение информации и ее защиты, носители информации. Организация деятельности по обеспечению информационной	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.	1	ПК-32, ПК-34, ПК-40
	Итого	1	

безопасности в кредитных организациях. Модели угроз и нарушителей.			
2 Формирование и развитие системы расчётов Банка России, элементы платежной системы ЦБ РФ, технологии построения. Характеристика структуры, оценка безопасности и надёжности централизованной платёжной системы РФ. Сервисы срочных и несрочных платежей, другие платежные системы и сервисы Банка России , требования к кредитным организациям для осуществления деятельности в указанных системах.	Управление рисками платежной системы Банка России, обеспечение безопасности и надёжности ее функционирования. Сервисы срочных и не срочных платежей ЦБ РФ, система быстрых платежей (СБП) и другие платежные сервисы Банка России, требования Банка России к кредитным организациям для участия в указанных системах, организация их деятельности.	1	ПК-32, ПК-34, ПК-40
	Итого	1	
3 Классификация и характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях РФ (платёжные и не платёжные). Задачи ИБ в АБС. Информационная безопасность неплатёжных АБС, телекоммуникационн ых систем ЦБ РФ и кредитных организаций 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.	1	ПК-32, ПК-34, ПК-40
	Итого	1	
4 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 кредитных организаций в соответствии с указанными нормативными документами.	1	ПК-32, ПК-34, ПК-40

	Итого	1	
Итого за семестр		4	
11 семестр			
5 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.	1	ПК-32, ПК-34, ПК-40
	Итого	1	
6 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.	1	ПК-32, ПК-34, ПК-40
	Итого	1	
Итого за семестр		2	
Итого		6	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин					
	1	2	3	4	5	6
Предшествующие дисциплины						
1 Защита информации в банковских системах	+	+	+	+	+	+
2 Бухгалтерский учет			+			+
3 Деньги, кредит, банки	+		+			+
4 Защищенный электронный документооборот					+	
5 Информационные системы в экономике			+			
6 Контроль и ревизия					+	+
7 Методы и средства защиты информации					+	+

8 Мировая экономика и международные отношения	+					
9 Надзорные, правоохранительные и финансовые органы					+	
10 Организационное и правовое обеспечение информационной безопасности					+	+
11 Основы информационной безопасности					+	+
12 Основы финансового права	+					
13 Оценка рисков				+	+	
Последующие дисциплины						
1 Защита информации в банковских системах	+	+	+	+	+	+
2 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты		+	+	+	+	+
3 Преддипломная практика	+	+	+			+

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.	
ПК-32	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Тест
ПК-34	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Тест
ПК-40	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

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
10 семестр			
2 Формирование и развитие системы расчётов Банка	Структура и элементы, оценка безопасности и надёжности централизованной платёжной системы РФ,управление риска-	1	ПК-32, ПК-34, ПК-40

России, элементы платежной системы ЦБ РФ, технологии построения. Характеристика структуры, оценка безопасности и надёжности централизованной платёжной системы РФ. Сервисы срочных и несрочных платежей, другие платежные системы и сервисы Банка России , требования к кредитным организациям для осуществления деятельности в указанных системах.	ми.		
	Итого	1	
3 Классификация и характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях РФ (платёжные и не платёжные). Задачи ИБ в АБС. Информационная безопасность неплатёжных АБС, телекоммуникационных систем ЦБ РФ и кредитных организаций РФ.	Классификация и характеристики АБС	1	ПК-32, ПК-34, ПК-40
	Итого	1	
Итого за семестр		2	
11 семестр			
5 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	ПК-32, ПК-34, ПК-40
	Итого	2	
6 Контроль внедрения и эксплуатации СЗИ банковских информационных систем в соответствии со	Организация эффективной системы использования и совершенствования средств защиты информации в АБС кредитных организаций обеспечение их соответствия отраслевым стандартам и требованиям Банка России.	2	ПК-32, ПК-34, ПК-40

стандартами ИБ и защиты информации ЦБ РФ. Анализ и отчётность	Итого	2	
Итого за семестр		4	
Итого		6	

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
10 семестр				
1 Предмет дисциплины, история создания и развития банковской системы РФ, автоматизация банковской деятельности. Значение информации и ее защиты, носители информации. Организация деятельности по обеспечению информационной безопасности в кредитных организациях. Модели угроз и нарушителей.	Проработка лекционного материала	4	ПК-32, ПК-34, ПК-40	Опрос на занятиях, Тест
	Итого	4		
2 Формирование и развитие системы расчётов Банка России, элементы платежной системы ЦБ РФ, технологии построения. Характеристика структуры, оценка безопасности и надёжности централизованной платёжной системы РФ. Сервисы срочных	Подготовка к практическим занятиям, семинарам	4	ПК-32, ПК-34, ПК-40	Опрос на занятиях, Тест
	Проработка лекционного материала	4		
	Итого	8		

и несрочных платежей, другие платежные системы и сервисы Банка России , требования к кредитным организациям для осуществления деятельности в указанных системах.				
3 Классификация и характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях РФ (платёжные и не платёжные). Задачи ИБ в АБС. Информационная безопасность неплатёжных АБС, телекоммуникационных систем ЦБ РФ и кредитных организаций РФ.	Подготовка к практическим занятиям, семинарам	4	ПК-32, ПК-34, ПК-40	Опрос на занятиях, Тест
	Проработка лекционного материала	4		
	Итого	8		
4 Стандарты Банка России СТО БР ИББС-2014. История создания и развития, основные положения.	Подготовка к практическим занятиям, семинарам	10	ПК-32, ПК-34, ПК-40	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Итого	10		
Итого за семестр		30		
11 семестр				
5 Служба информационной безопасности коммерческого банка, функции и полномочия, организация деятельности.	Подготовка к практическим занятиям, семинарам	5	ПК-32, ПК-34, ПК-40	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	7		
	Итого	12		
6 Контроль внедрения и эксплуатации СЗИ банковских информационных	Подготовка к практическим занятиям, семинарам	7	ПК-32, ПК-34, ПК-40	Опрос на занятиях, Отчет по индивидуальному заданию, Тест
	Проработка лекционного материала	7		

систем в соответствии со стандартами ИБ и защиты информации ЦБ РФ. Анализ и отчётность	Итого	14		
Итого за семестр		26		
	Подготовка и сдача зачета	4		Зачёт
Итого		60		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

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: https://cbr.ru/statichtml/file/59420/st-10-14.pdf (дата обращения: 18.07.2021).

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: https://cbr.ru/statichtml/file/59420/st-12-14.pdf (дата обращения: 18.07.2021).

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) [Электронный ресурс] [Электронный ресурс]: — Режим доступа: http://www.garant.ru/products/ipo/prime/doc/487314/ (дата обращения: 18.07.2021).

4. Внуков, А. А. Защита информации в банковских системах [Электронный ресурс]: учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — Режим доступа: https://urait.ru/bcode/468273 (дата обращения: 18.07.2021).

12.2. Дополнительная литература

1. Национальная платежная система. Бизнес-энциклопедия / коллектив Н35 авторов; ред. -сост. А.С. Воронин. - М. [Электронный ресурс]: КНОРУС:ЦИПСиР, 2013. - 424 с. ISBN 978-5-406-02526-0: — Режим доступа: https://institutiones.com/download/books/2153-nacionalnaya-platezhnaya-sistema-voronin.html (дата обращения: 18.07.2021).

2. Стратегия развития национальной платежной системы на 2021–2023 годы. Банк России. [Электронный ресурс] [Электронный ресурс]: — Режим доступа: http://www.cbr.ru/Content/Document/File/120210/strategy_nps_2021-2023.pdf (дата обращения: 18.07.2021).

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: 18.07.2021).

2. 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 [Электронный ресурс]: В-Спектр, 2011. – 220с. ISBN 978-5-91191-229-5 [Электронный ресурс] — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-3ch.pdf (дата обращения: 18.07.2021).

3. Защита информации [Электронный ресурс]: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. — Режим доступа: https://edu.tusur.ru/publications/2261 (дата обращения: 18.07.2021).

4. Защита информации [Электронный ресурс]: Методические указания к выполнению лабораторных работ / Спицын В. Г. - 2012. 17 с. — Режим доступа: https://edu.tusur.ru/publications/1822 (дата обращения: 18.07.2021).

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. СПАРК https://www.spark-interfax.ru/
2. При изучении дисциплины рекомендуется обращаться к базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh

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

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 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"
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.

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 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 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:

1.1. Информация о нормативно – правовых актах, затрагивающая права, свободы и обязанности граждан

1.2. Информация об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну).

1.3. Информация о государственных золотовалютных резервах РФ

1.4. Все виды информации, указанные в п.1.1-1.3

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:

2.1. Рыночный риск

2.2. Правовой риск

2.3. Операционный риск

2.4. Кредитный риск

2.5. Риск потери деловой репутации

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

3.1. Универсальные банки

3.2. Инвестиционные банки

3.3. Региональные банки

3.4. Ссудно-сберегательные кассы

3.5. Банки, указанные в п.п.3.1-3.3

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

4.1. Развитие и укрепление банковской системы РФ, повышение доверия к ней

4.2. Достижение адекватности мер защиты реальным угрозам ИБ

4.3. Предотвращение и (или) снижение ущерба от инцидентов ИБ

4.4. Цели, указанные в п.п.4.1-4.2

4.5. Цели, указанные в п.п.4.1-4.3

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

5.1. Судам общей юрисдикции и арбитражным судам

5.2. Налоговым и таможенным органам

5.3. Органам внутренних дел при осуществлении ими функций по выявлению, предупреждению и пресечению налоговых преступлений

5.4. Субъектам, указанных в п.п.5.1-5.2

5. Субъектам, указанным в п.п.1-3

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

6.1. Информация о составе органов управления кредитной организации

6.2. Информация о решениях принятых исполнительными органами кредитной организации

6.3. Годовая бухгалтерская (финансовая) отчетность банка

6.4. Расчет собственных средств (капитала) банка

6.5. Информация, указанная в п.п.6.3-6.4

7. Информация может оцениваться как следующий вид активов компании:

7.1. Внеоборотные активы

7.2. Нематериальные активы

7.3. Оборотные активы

7.4. Товарно -материальные ценности

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

8.1.Уместность

8.2. Надежность

8.3. Важность

8.4. Характеристики, указанные в п.п.8.2-8.3

8.5. Характеристики, указанные в п.п.8.1-8.3

9. Единое информационное пространство банка основывается на следующих принципах:

9.1. Открытости

9.2. Ограничения количества пользователей

9.3. Защищенности

9.4. На принципах, указанных в п.9.1 и п.9.3

9.5. На принципах, указанных в п.п.9.1-9.3

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

10.1. Платежных

10.2. Операционных

10.3. Документарных

10.4. Технологии, указанные в п.п.10.1-10.3

10.5. Технологии, указанные в п.п.10.2-10.3

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

11.1. Четыре

11.2. Пять

11.3. Шесть

11.4. Семь

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

банков:

12.1. Модуль расчетно-кассового обслуживания клиентов

12.2. Модуль кредитных операций клиентов

12.3. Модуль хозяйственных договоров и обеспечения внутрибанковской деятельности

12.4. Функциональные модули, указанные в п.12.1-12.2

12.5. Функциональные модули, указанные в п.12.1-12.3

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

13.1. Несанкционированный доступ к ресурсам и данным системы

13.2. Подмена сетевых адресов

13.3. Отказ в обслуживании

13.4. Атака на уровне приложений

13.5. Все информационные угрозы, указанные в п.п.13.1- 13.4

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

14.1. Отсутствие гарантий конфиденциальности и целостности передаваемых данных

14.2. Утеря актуальности разработанной политики ИБ или некорректная (неполная) реализация

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

14.4. Низкий (непрофессиональный) уровень администрирования АБС и сетевых приложений

14.5. Относятся все причины, указанные в п.п.14.1-14.4

15. Платежная система Банка России является:

15.1. Централизованной

15.2. Децентрализованной

15.3. Распределенной

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

16.1. Система внутрирегиональных электронных расчетов (система ВЭР)

16.2. Система межрегиональных электронных расчетов (система МЭР)

16.3. Система международных электронных расчетов (система МДЭР)

16.4. Система банковских электронных срочных платежей (система БЭСП)

16.5. Входят все системы расчетов, указанные в п.п.16.1-16.4

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

17.1. Работники банка, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий

17.2. 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

17.3. Криминальные элементы и террористы

17.4. Неблагоприятные события природного, техногенного и социального характера

17.5. К основным, относятся все категории угроз, указанные в п.п.17.1-17.4

18. Политика ИБ банка формируется на основе следующих элементов:

18.1. Требований законодательства РФ и нормативных актов ЦБ РФ

18.2. Интересов и бизнес – целей банка

18.3. Накопленного в организации опыта в области обеспечения ИБ

18.4. На основе элементов, указанных в п.18.1 и п.18.3

18.5. На основе элементов, указанных в п.п.18.1-18.3

19. Какой из указанных органов корпоративного управления банка может иметь полномочия

по утверждению Политики информационной безопасности данной кредитной организации:

19.1. Наблюдательный Совет

19.2. Правление

19.3. Председатель Правления

19.4. 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:

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

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

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

20.4. 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:

21.1. Ролей, связанных с проектированием (разработкой) и созданием (модернизацией) объекта информационной инфраструктуры

21.2. Ролей, связанных с эксплуатацией объекта информационной инфраструктуры в части его использования по назначению и в части его технического обслуживания или ремонта

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

21.4. Ролей, указанных в п.21.1 и п.21.3

21.5. Ролей, указанных в п.21.2 и п.21.3

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

22.1. Осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации

22.2. Определять требования к техническим средствам защиты информации и организационным мерам защиты информации

22.3. Определять порядок эксплуатации технических средств защиты информации и соответствующего программного обеспечения

22.4. Полномочиями, указанными в п.п. 22.1-22.2

22.5. Полномочиями, указанными в п.п. 22.1-22.3

14.1.2. 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 защи-

ты

автоматизированных рабочих мест

14.1.3. Зачёт

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 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.

14.1.4. 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.

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

Сервисы срочных и не срочных платежей ЦБ РФ, система быстрых платежей (СБП) и другие платежные сервисы Банка России, требования Банка России к кредитным организациям для участия в указанных системах, 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.

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.

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.

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.