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
_____П.В. Сенченко
«30» _____06_____ 2021 г.

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: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **5**
Семестр: **9**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	9 семестр	Всего	Единицы
Лекционные занятия	30	30	часов
Практические занятия	30	30	часов
Самостоятельная работа	12	12	часов
Общая трудоемкость (включая промежуточную аттестацию)	72	72	часов
	2	2	з.е.

Формы промежуточной аттестация	Семестр
Зачет	9

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 30.06.2021
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 63119

1. Общие положения

1.1. Цели дисциплины

1. 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.

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

1.2. Задачи дисциплины

1. Изучение общих принципов построения банковской системы РФ, специфических особенностей в вопросах обеспечения информационной безопасности.

2. Изучение порядка организации деятельности системы обеспечения информационной безопасности в коммерческих банках, формирования и реализации политики информационной безопасности.

3. Изучение требований нормативно - правовых документов, отраслевых стандартов Банка России по вопросам функционирования системы информационной безопасности кредитных организаций, порядка оценки и самооценки ее соответствия указанным требованиям.

4. Изучение теоретических подходов и состава практических мероприятий, используемых кредитными организациями для обеспечения защиты банковской информации и деятельности автоматизированных банковских систем.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Обязательная часть.

Модуль дисциплин: Модуль специальности (special hard skills - SHS).

Индекс дисциплины: Б1.О.03.25.

Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		

Согласована на портале № 63119

ОПК-4. Способен разрабатывать и принимать экономически и финансово обоснованные организационно-управленческие решения, планировать и организовывать профессиональную деятельность, осуществлять контроль и учет ее результатов	ОПК-4.1. Знает принципы формирования политики информационной безопасности в организациях кредитно-финансовой сферы и систему организационных мер, направленных на обеспечение экономической безопасности в организации	Знает нормативные документы, организационные и технические меры защиты информации в АБС, требования и процедуры сертификации средств и систем защиты информации, используемых в БС РФ
	ОПК-4.2. Умеет осуществлять расчет аналитических показателей, необходимых для решения поставленной экономической задачи	Умеет рассчитывать финансовые и кадровые ресурсы, необходимые для повышения степени зрелости процессов обеспечения информационной безопасности на основании рекомендаций Банка России
	ОПК-4.3. Владеет методами количественной оценки экономических показателей деятельности предприятия с целью принятия обоснованных экономических решений	Владеет навыками работы с технической документацией, методами формирования требований по обеспечению информационной безопасности, методиками расчета рисков организации банковской системы

Согласована на портале № 63119

ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-7.1. Знает принципы работы современных информационных технологий, назначение, функции и обобщённую структуру операционных систем и типовые операционные системы, в том числе отечественного производства	Знает нормативные документы, организационные и технические меры защиты информации в АБС, требования и процедуры сертификации средств и систем защиты информации, используемых в БС РФ
	ОПК-7.2. Умеет классифицировать компьютерные системы, виды информационного взаимодействия и обслуживания, основы построения информационно-вычислительных систем	Умеет пользоваться методикой анализа параметров и характеристик состояния АБС на разных стадиях их жизненного цикла
	ОПК-7.3. Владеет средствами информационно-коммуникационных технологий, в том числе текстовыми редакторами и электронными таблицами, при решении задач профессиональной деятельности	Владеет методикой расчета банковских нормативов, умеет пользоваться стандартными формулами электронных таблиц для их оценки
Профессиональные компетенции		
-	-	-

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 2 зачетных единиц, 72 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		9 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	60	60
Лекционные занятия	30	30
Практические занятия	30	30
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	12	12
Подготовка к тестированию	4	4
Подготовка к зачету	4	4
Подготовка к контрольной работе	4	4
Общая трудоемкость (в часах)	72	72

Согласована на портале № 63119

Общая трудоемкость (в з.е.)	2	2

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
9 семестр					
1 Формирование и развитие мировой и национальной платежной системы, ее актуальные проблемы	6	6	2	14	ОПК-4, ОПК-7
2 Организация деятельности по обеспечению информационной безопасности в кредитных организациях.	10	10	4	24	ОПК-4, ОПК-7
3 Комплекс Банка России по обеспечению информационной безопасности банковской системы СТО БР ИББС	8	8	4	20	ОПК-4, ОПК-7
4 Служба информационной безопасности коммерческого банка	6	6	2	14	ОПК-4, ОПК-7
Итого за семестр	30	30	12	72	
Итого	30	30	12	72	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
9 семестр			
1 Формирование и развитие мировой и национальной платежной системы, ее актуальные проблемы	Процессы цифровой трансформации экономики. Роль информации в современном мире. Актуальность обеспечения защиты информации, хищение данных и промышленный шпионаж. Характеристики информации. Современное состояние и перспективы развития мировой и российской банковской системы. Формирование экосистем российскими банками.	6	ОПК-4, ОПК-7
	Итого	6	

Согласована на портале № 63119

2 Организация деятельности по обеспечению информационной безопасности в кредитных организациях.	Организация и функционирования системы обеспечения информационной безопасности в коммерческих банках. Объекты защиты, виды угроз и типы нарушителей, менеджмент системы информационной безопасности, использование сквозных цифровых технологий. Модели угроз и нарушителей. Разработка и внедрение методов и средств защиты информации. Классификация и характеристики АБС.	10	ОПК-4, ОПК-7
	Итого	10	
3 Комплекс Банка России по обеспечению информационной безопасности банковской системы СТО БР ИББС	Отраслевые стандарты Банка России по обеспечению информационной безопасности коммерческих банков, состав (обязательные и рекомендательные элементы), основные положения и требования, порядок оценки кредитных организаций.	8	ОПК-4, ОПК-7
	Итого	8	
4 Служба информационной безопасности коммерческого банка	Порядок организации деятельности специализированного подразделения деятельности коммерческого банка - службы информационной безопасности. Роль, функции, полномочия и ответственность службы, нормативные документы, регламентирующие деятельность подразделения и уполномоченных сотрудников. Аудит информационной безопасности, анализ и отчётность.	6	ОПК-4, ОПК-7
	Итого	6	
Итого за семестр		30	
Итого		30	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.

Таблица 5.3 – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
9 семестр			

Согласована на портале № 63119

1 Формирование и развитие мировой и национальной платежной системы, ее актуальные проблемы	Организация и функционирование платежной системы Банка России, международных, частных платежных систем, принципы и порядок деятельности, условия и услуги, требования к участникам. Автоматизация и информационные технологии в деятельности кредитных организаций. Управление рисками банковской системы России, обеспечение безопасности и надёжности ее функционирования.	6	ОПК-4, ОПК-7
	Итого	6	
2 Организация деятельности по обеспечению информационной безопасности в кредитных организациях.	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 и угрозы различных компонентов АБС. Организация эффективной системы использования и совершенствования средств защиты информации. Использование СКЗИ.	10	ОПК-4, ОПК-7
	Итого	10	
3 Комплекс Банка России по обеспечению информационной безопасности банковской системы СТО БР ИББС	Способы и методы организации контроля, внедрения, эксплуатации и модернизации средств защиты информации банковских информационных систем, анализ возможных проблем и уязвимостей, отчетность уполномоченным органам. Использование и разработка нормативной базы кредитной организации в соответствии со стандартами информационной безопасности Банка России.	8	ОПК-4, ОПК-7
	Итого	8	

Согласована на портале № 63119

4 Служба информационной безопасности коммерческого банка	Организация деятельности подразделений кредитных организаций, обеспечивающих информационную безопасность, защиту информации и персональных данных. Цели и задачи данных подразделений, функции и полномочия, права и обязанности их сотрудников. Анализ средств защиты информации в платёжных и неплатёжных автоматизированных банковских системах, телекоммуникационных системах ЦБ РФ и кредитных организаций, применение СКЗИ, организация деятельности и используемая нормативная база.	6	ОПК-4, ОПК-7
	Итого	6	
	Итого за семестр	30	
	Итого	30	

5.4. Лабораторные занятия

Не предусмотрено учебным планом

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
9 семестр				
1 Формирование и развитие мировой и национальной платежной системы, ее актуальные проблемы	Подготовка к тестированию	1	ОПК-4, ОПК-7	Тестирование
	Подготовка к зачету	1	ОПК-4, ОПК-7	Зачёт
	Итого	2		
2 Организация деятельности по обеспечению информационной безопасности в кредитных организациях.	Подготовка к тестированию	1	ОПК-4, ОПК-7	Тестирование
	Подготовка к зачету	1	ОПК-4, ОПК-7	Зачёт
	Подготовка к контрольной работе	2	ОПК-4, ОПК-7	Контрольная работа
	Итого	4		

Согласована на портале № 63119

3 Комплекс Банка России по обеспечению информационной безопасности банковской системы СТО БР ИББС	Подготовка к тестированию	1	ОПК-4, ОПК-7	Тестирование
	Подготовка к зачету	1	ОПК-4, ОПК-7	Зачёт
	Подготовка к контрольной работе	2	ОПК-4, ОПК-7	Контрольная работа
	Итого	4		
4 Служба информационной безопасности коммерческого банка	Подготовка к тестированию	1	ОПК-4, ОПК-7	Тестирование
	Подготовка к зачету	1	ОПК-4, ОПК-7	Зачёт
	Итого	2		
Итого за семестр		12		
Итого		12		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Прак. зан.	Сам. раб.	
ОПК-4	+	+	+	Зачёт, Контрольная работа, Тестирование
ОПК-7	+	+	+	Зачёт, Контрольная работа, Тестирование

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	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				
Зачёт	10	10	10	30
Контрольная работа	10	10	20	40
Тестирование	10	10	10	30
Итого максимум за период	30	30	40	100
Нарастающим итогом	30	60	100	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4

Согласована на портале № 63119

От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	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)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Положение Центрального Банка РФ №719-П от 04.06.2020 "О требованиях к обеспечению защиты информации при осуществлении Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств" [Электронный ресурс] [Электронный ресурс]: — Режим доступа: https://base.garant.ru/74709682/.

2. Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов. Банк России, М.2021 [Электронный ресурс] [Электронный ресурс]: — Режим доступа: https://cbr.ru/Content/Document/File/131360/oncfr_2022-2024.pdf.

3. 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.

4. "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] [Электронный ресурс]: — Режим доступа: https://cbr.ru/Crosscut/LawActs/File/448.

5. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/490278.

7.2. Дополнительная литература

1. Основные типы компьютерных атак в кредитно – финансовой сфере в 2019-2020гг. Обзор. Банк России. М.2021 [Электронный ресурс] [Электронный ресурс]: — Режим доступа: https://cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf.

2. "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] [Электронный ресурс]: — Режим доступа: https://cbr.ru/Crosscut/LawActs/File/447.

Согласована на портале № 63119

3. "Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты ИБ при осуществлении переводов денежных средств. " СТО БР ИББС-1.3-2016" (принят и введен в действие Распоряжением Банка России от 30.11.2016 N ОД -4234) [Электронный ресурс] [Электронный ресурс] [Электронный ресурс]: — Режим доступа: https://cbr.ru/Crosscut/LawActs/File/449.

4. Логинов, Б. Б. Международный банковский бизнес : учебное пособие для вузов / Б. Б. Логинов. — Москва : Издательство Юрайт, 2022. — 179 с. — (Высшее образование). — ISBN 978-5-534-00740-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/490232.

5. Гамза, В. А. Безопасность банковской деятельности : учебник для вузов / В. А. Гамза, И. Б. Ткачук, И. М. Жилкин. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 455 с. — (Высшее образование). — ISBN 978-5-534-13582-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/489071.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Специальные технологии баз данных в информационных системах: Методические указания для выполнения лабораторных и самостоятельных работ / К. С. Сарин - 2018. 146 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/7637.

2. Деньги, кредит, банки: Методические указания к выполнению практических заданий и самостоятельной работы / Е. Г. Алдохина - 2018. 13 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/7161.

3. Защита информации в инфокоммуникационных системах и сетях: Сборник лабораторных работ / А. М. Голиков - 2012. 374 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/1050.

7.3.2. 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.

7.4. Современные профессиональные базы данных и информационные справочные системы

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

8. Материально-техническое и программное обеспечение дисциплины

8.1. 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 достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие

Согласована на портале № 63119

тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория программно-аппаратных средств обеспечения информационной безопасности: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 405 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Усилитель Roxton AA-60M;
- Потолочный громкоговоритель Roxton PA-20T;
- Аппаратные средства аутентификации пользователя "eToken Pro";
- Программно-аппаратный комплекс защиты информации: ПАК ViPNet Coordinator HW100 C 4.x, ПАК ViPNet Coordinator HW1000 4.x;
- Устройства чтения смарт-карт и радиометок: адаптер компьютерный для считывания и передачи в ПК серийных номеров бесконтактных идентификаторов IronLogic Z-2 USB;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

8.3. 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.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

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

8.4. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

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

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

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

Согласована на портале № 63119

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.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Формирование и развитие мировой и национальной платежной системы, ее актуальные проблемы	ОПК-4, ОПК-7	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
2 Организация деятельности по обеспечению информационной безопасности в кредитных организациях.	ОПК-4, ОПК-7	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
3 Комплекс Банка России по обеспечению информационной безопасности банковской системы СТО БР ИББС	ОПК-4, ОПК-7	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
4 Служба информационной безопасности коммерческого банка	ОПК-4, ОПК-7	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков

Согласована на портале № 63119

3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

1. Какая информация в соответствии с действующим законодательством может быть отнесена к категории общедоступной:
   1.1. Перечень кредитных организаций, предоставляющих услуги по проведению платежей в РФ.
   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

Согласована на портале № 63119

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.
5.5. Субъектам, указанным в п.п.5.1-5.3.

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 один из указанных видов 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

Согласована на портале № 63119

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 являются наиболее актуальными 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. Укажите субъекты финансового рынка, которые не относятся к категории кредитных организаций в соответствие с действующим законодательством РФ и нормативными документами Банка России:
15.1. Коммерческие банки.
15.2. Небанковские кредитные организации.
15.3. Кредитно – потребительские кооперативы.
15.4. Относятся все субъекты, указанные в п.п.15.1-15.3.

16. В практической деятельности в кредитной организации возможно использование средства криптографической защиты информации (СКЗИ) сторонних разработчиков, отвечающие следующим условиям:
16.1. Допускают встраивание в технологические процессы, обеспечивают взаимодействие на уровне обработки запросов на криптографические преобразования и выдачи результатов.
16.2. Обладают полным комплектом эксплуатационной документации, предоставляемой разработчиком СКЗИ.
16.3. Сертифицированы уполномоченным государственным органом либо имеют разрешение ФСБ РФ.
16.4. СКЗИ, которые одновременно отвечают условиям, указанным в п.п.16.1-16.3.

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

Согласована на портале № 63119

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. Неблагоприятные события природного, техногенного и социального характера.
17.3. Неблагоприятные события природного, техногенного и социального характера.
17.4. К основным, относятся все категории угроз, указанные в п.п.17.1-17.3.

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 и компетенций 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 банка.
19.3. Председатель Правления.
19.4. Любой из указанных органов управления банка.

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.

9.1.2. Перечень вопросов для зачета

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. Риски в деятельности платежных систем, системы управления ими. Операционный риск. Деятельность Банка России по контролю организации и функционирования систем управления рисками кредитных организаций.
4. Виды информации, возможные ограничения ее использования и распространения.

Согласована на портале № 63119

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. Использование сквозных цифровых технологий (Big Data, искусственный интеллект и других) для функционирования систем защиты информации. Порядок и процедуры защиты носителей информации.
6. Требования Банка России к кредитным организациям при осуществлении переводов денежных средств (Положение ЦБ РФ № 382-П и другие нормативные документы ЦБ РФ).
7. Информация как нематериальные активы компании, показатели оценки информации как соответствующих ресурсов.
8. Финансовая информация (понятие, цели получения, виды классификации).
9. Биометрическая идентификация – направления использования в деятельности участников финансового рынка, применяемые сквозные цифровые технологии для обеспечения ее функционирования.
10. Общие характеристики автоматизированных банковских систем, используемых в кредитных организациях. Элементы и программно - функциональные модули АБС, виды информационных банковских технологий, используемых при создании АБС.
11. Уязвимости и угрозы компонентам АБС, архитектура систем защиты, методы и способы защиты от неправомерных действий, противоправных 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. Надзор ЦБ РФ за деятельностью платежных систем (функции, полномочия формы контроля и другие).
14. Единая биометрическая система РФ (ЕБС РФ). Нормативные документы, регламентирующие деятельность, участники, порядок работы, перспективы и направления развития.
15. Цифровые валюты центральных банков (CBDC), мировой опыт использования. Цифровой рубль – роль и перспективы использования, риски для финансовой системы РФ.
16. Структура отраслевых стандартов СТО БР ИБСС (обязательные компоненты и рекомендации). Роль и актуальность указанных отраслевых стандартов в обеспечении информационной безопасности кредитных организаций и платежных систем в РФ.
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, функции, полномочия и права службы информационной безопасности банка, ее сотрудников и руководителя. Нормативное обеспечение и регулирование их деятельности.
20. Организация системы обеспечения информационной безопасности банка (система информационной безопасности, система менеджмента информационной безопасности).
21. Внутреннее организационное и документальное обеспечение деятельности кредитных организаций по вопросам информационной безопасности (состав и структура внутренних документов, требования к осуществлению деятельности, планирование и проведение указанных мероприятий).
22. Внутреннее организационное и документальное обеспечение деятельности кредитных организаций по вопросам информационной безопасности (состав и структура внутренних документов, требования к осуществлению деятельности, планирование и проведение указанных мероприятий).
23. Цифровые и дистанционные форматы предоставления финансовых услуг кредитными организациями и платежными системами, использование цифровых инструментов взаимодействия и коммуникаций (биометрическая и многофакторная идентификация, цифровые помощники и ассистенты, персонализация услуг, тарифов и условий). Обеспечение информационной безопасности участников.
24. Массовые платежные системы (пластиковые карты, электронные кошельки, системы

Согласована на портале № 63119

переводов, платежи по QR –кодам): условия, порядок функционирования, особенности, требования к участникам, риски, применяемые операционные и технические средства, информационные и сквозные цифровые технологии.

9.1.3. Примерный перечень вариантов (заданий) контрольных работ

1. организационные основы банковской деятельности, функции подразделений безопасности банков, вопросы соблюдения прав и свобод личности при решении задач обеспечения безопасности;
2. правовые основы охраны коммерческой тайны и защиты конфиденциальной банковской информации;
3. источники и угрозы утечки конфиденциальной информации в банке;
4. 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;
5. технические и инженерно-технические средства защиты информации;
6. административные и аппаратно-программные методы защиты, в том числе системы защиты автоматизированных рабочих мест

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. 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 9.2.

Таблица 9.2 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения

Согласована на портале № 63119

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, определяющимися исходя из состояния обучающегося на момент проверки

9.4. 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 № 63119

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 5 от « 5 » 5 2021 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	К.С. Сарин	Согласовано, 68c81ca0-0954-467a-8d01-f93a0d553669

РАЗРАБОТАНО:

Старший преподаватель, каф. КИБЭВС	П.А. Протасов	Разработано, b6728068-5230-4e16-828d-fa10611c692b
Старший преподаватель, каф. КИБЭВС	О.В. Кочетков	Разработано, 3b44f54b-af6d-450b-846a-0120582a20fb

Согласована на портале № 63119