Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
_____ 2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«БЕЗОПАСНОСТЬ БАНКОВСКИХ И ПЛАТЕЖНЫХ ИС»

Специальность: 38.05.01 «Экономическая безопасность»
Специализация: «Экономико-правовое обеспечение экономической безопасности»
Уровень высшего образования: специалитет
Квалификация (степень) выпускника: экономист
Форма обучения очная, заочная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: к.т.н., доцент Вихров А.П., Рабочая программа дисциплины: «Безопасность банковских и платежных ИС». – Королев МО: ФГБОУ ВО «Технологический университет», 2023.

Рецензент: к.в.н., доцент Воронов А.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 «Экономическая безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол **№ 9 от 11 апреля 2023 г.**

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Сапожников В.В., к.в.н., доцент				
Год утверждения (переутверждения)	2023	2024	2025	2026	2027
Номер и дата протокола заседания кафедры	№ 8 от 29.03.2023 г.				

Рабочая программа согласована:
Руководитель ОПОП _____ Коба Е.Е., к.э.н., доцент

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024	2025	2026	2027
Номер и дата протокола заседания УМС	№ 5 от 11.04.2023 г.				

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целями изучения дисциплины являются:

1. Формирование у студентов специализированной базы знаний по основным понятиям в области информационной безопасности банковской деятельности;
2. Приобретение студентами первичных навыков по практическому формированию документов, составляющих правовую базу защиты информации в банковской сфере.
3. Повышение уровня специальных знаний в области защиты информационно - телекоммуникационной инфраструктуры и компьютерной информации в банковской сфере.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общепрофессиональные компетенции

- ОПК-6 - Способен использовать современные информационные технологии и программные средства при решении профессиональных задач;
- ОПК-7 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Профессиональные компетенции

- ПК-4 - Способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-информационному обеспечению системы стратегического управления рисками

Основными **задачами** дисциплины являются:

- ознакомление студентов с основами информационной безопасности банковской деятельности на основе действующего российского законодательства;
- ознакомление с описанием угроз безопасности кредитно-финансовой деятельности;
- изучение основы организации противодействия угрозам информационной безопасности в кредитно-финансовой сфере;
- освоение основных инструментов защиты информации в банковских и платежных системах;
- формирование системы знаний в области защиты информации в кредитно-финансовой сфере.
- ознакомление с методами и средствами защиты информации функциональных и контролирующих подразделений финансово – кредитных организаций.

Показатели освоения компетенций отражают следующие индикаторы:

Трудовые действия:

ОПК-6. И-1. Использует современные специализированные программные средства коммуникации и справочные системы для решения профессиональных задач

ОПК-7. И-1. Имеет представление, понимает принципы работы современных информационных технологий в экономике, программных средств для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач

ПК-4. И-1. Создает организационно-управленческую и информационную структуру интегральной системы управления рисками, разрабатывает проекты нормативных и методических материалов, регламентирующих работу по защите информации, предлагает технологии защиты информации, безопасную систему внутренней и внешней коммуникации и отчетности

ПК-4. И-3. Использует современные принципы, методы и технологии работы с информацией, принципы и методы управления проектами, положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности

Необходимые умения:

ОПК-6. И-1. У-1. Умеет использовать современные специализированные программные средства коммуникации и справочные системы для решения профессиональных задач (СПС Консультант+, Гарант, TrueConf Server, Zoom, Яндекс. Телемост и др.)

ОПК-7. И-1. У-1. Умеет осуществлять поиск, аккумулирование, хранение, обработку, анализ, планирование, оценку и передачу данных при решении профессиональных задач с использованием современных информационных технологий

ПК-4. И-1. У-1. Умеет создавать организационно-управленческую и информационную структуру интегральной системы управления рисками;

ПК-4. И-1. У-2. Умеет разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации,

ПК-4. И-1. У-3. Умеет осуществлять выбор средств и технологий защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности

ПК-4. И-3. У-1. Умеет использовать современные принципы, методы и технологии работы с информацией,

ПК-4. И-3. У-2. Умеет применять принципы и методы управления проектами,

ПК-4. И-3. У-3. Умеет использовать положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности

Необходимые знания:

ОПК-6. И-1. З-1. Знает методы работы с современными специализированными программными средствами коммуникации и справочными системами для решения профессиональных задач
ОПК-7. И-1. З-1. Знает принципы работы современных информационных технологий в экономике и программных средств
ПК-4. И-1. З-1. Знает принципы создания организационно-управленческой и информационной структуры интегральной системы управления рисками;
ПК-4. И-1. З-2. Знает методические материалы, регламентирующие работу по защите информации,
ПК-4. И-1. З-3. Знает технологии защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности
ПК-4. И-3. З-1. Знает современные принципы, методы и технологии работы с информацией
ПК-4. И-3. З-2. Знает принципы и методы управления проектами
ПК-4. И-3. З-3. Знает положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Безопасность банковских и платежных ИС» относится к дисциплинам специализации базовой части Блока 1 модуля «Информационные технологии и экономическая безопасность» основной профессиональной образовательной программы подготовки специалистов по направлению 38.05.01 «Экономическая безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Безопасность электронного документооборота», «Защита конфиденциальной информации», «Информационная безопасность предприятия», «Информационная безопасность операционных систем и баз данных» и компетенциях УК-1; ОПК-6; ОПК-7; ПК-4.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при изучении дисциплин: «Экономическая безопасность», «Обеспечение экономической безопасности региона» и выполнении выпускной квалификационной работы специалиста.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и заочной формы составляет 3 зачетных единицы, 108 часов.

Таблица 1-Объем дисциплины и виды учебной работы

Виды занятий	Всего часов	Семестр	Семестр А	Семестр 8	Семестр …
Общая трудоемкость	**108**		**108**	**108**	
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**48**			**48**	
Лекции (Л)	**16**			**16**	
Практические занятия (ПЗ)	**32**			**32**	
Лабораторные работы (ЛР)	**-**			**-**	
Практическая подготовка	**-**			**-**	
Самостоятельная работа	**60**			**60**	
КСР	-			-	
Курсовые работы (проекты)	**-**			**-**	
Расчетно-графические работы	**-**			**-**	
Контрольная работа, домашнее задание	+ -			+ -	
Текущий контроль знаний	**Тесты**			**Тесты**	
Вид итогового контроля	**Зачет**			**Зачет**	
ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**12**		**12**		
Лекции (Л)	**8**		**8**		
Практические занятия (ПЗ)	**8**		**8**		
Лабораторные работы (ЛР)	**-**		**-**		
Практическая подготовка	**-**		**-**		
Самостоятельная работа	**92**		**92**		
Курсовые работы (проекты)	**-**		**-**		
Расчетно-графические работы	**-**		**-**		
Контрольная работа, домашнее задание	+ -		+ -		
Текущий контроль знаний	+		+		
Вид итогового контроля	**Зачет**		**Зачет**		

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2-Темы дисциплины и виды занятий

Наименование тем	Лекции, час. Очное/Заочное	Практические занятия, час Очное/Заочное	Лабораторные занятия, час Очное/ Заочное	Занятия в интерактивной форме, час Очно/заоч	Практическая подг. Очно/заоч	Код компетенций
Раздел I. Основы информационной безопасности банковской деятельности						
Тема 1. Концептуальные основы информационной безопасности банка	1.5/0.25	3/0,5	-	2/0,5	-	ОПК-6; ОПК-7; ПК-4
Тема 2. Правовые основы информационной безопасности банка	1.5/0.25	3/0,5	-	2/0,5	-	ОПК-6; ОПК-7; ПК-4
Тема 3. Стандарты информационной безопасности банка	1.5/0.25	3/0,5	-	2/1	-	ОПК-6; ОПК-7; ПК-4
Тема 4. Организационные основы информационной безопасности банка	1.5/0.25	3/0,5	-	2/1	-	ОПК-6; ОПК-7; ПК-4
Тема 5. Техника обеспечения информационной безопасности банка	1.5/0.5	3/1	-	2/1	-	ОПК-6; ОПК-7; ПК-4
Тема 6. Защита от информационных преступлений, посягающих на собственность банка	1.5/0.5	3/1	-	2/1	-	ОПК-6; ОПК-7; ПК-4
Раздел II. Технологии защиты информации в банковской деятельности						
Тема 7. Защита от хищения денежных средств и иного имущества с использованием векселей (информационный аспект)	1.5/0.5	3/1	-	2/1	-	ОПК-6; ОПК-7; ПК-4
Тема 8. Защита от информационных преступлений, посягающих на информационную безопасность функционирования банка	2/0.5	4/1	-	2/0,5	-	ОПК-6; ОПК-7; ПК-4
Тема 9. Организация	1.5/0.5	3/1	-	2/1	-	ОПК-6;

противодействия отмыванию преступных доходов и финансированию терроризма (информационный аспект)						ОПК-7; ПК-4
Тема 10. Комплексное обеспечение информационной безопасности банка	2/1	4/1	-		-	ОПК-6; ОПК-7; ПК-4
Итого:	16/8	32/8	-	22/8	-	

4.2. Содержание тем дисциплины

Раздел I. Основы информационной безопасности банковской деятельности

Тема 1. Концептуальные основы безопасности банка

Понятия и концепция безопасности банка. Банк как объект противоправных посягательств. Система угроз безопасности банка. Банк как субъект борьбы с противоправными посягательствами.

Тема 2. Правовые основы информационной безопасности банка

Система правового обеспечения безопасности банка. Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания. Банковское законодательство. Нормативные акты Банка России. Внутренние нормативные акты. Содержание аудита по ИБ технических средств обработки информации.

Тема 3. Стандарты информационной безопасности банка

О Стандарте Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации». Общие положения.

Основные цели и задачи стандарта Банка России при обеспечении информационной безопасности.

Основные направления работы по дальнейшему сопровождению и доработке Стандарта в рамках специально созданного Подкомитетом 3 “Защита информации в кредитно-финансовой сфере” Технического комитета 362 “Защита информации” Федерального агентства по техническому регулированию и метрологии.

Аудит информационной безопасности банка.

Стандарты Банка России СТО БР ИББС-1.0-2014, СТО БР ИББС-1.2-2014.

Система технических средств безопасности банка. Технические средства охраны. Технические средства охраны банковских операций и продуктов. Технико – криминалистические средства.

Тема 4. Организационные основы информационной безопасности банка

Организация системы безопасности банка. Субъекты обеспечения безопасности банка. Средства и методы обеспечения безопасности банка. Организация внутреннего контроля банка. Организация службы безопасности банка.

Тема 5. Техника обеспечения информационной безопасности банка

Система технических средств безопасности банка. Технические средства охраны. Технические средства охраны банковских операций и продуктов. Технико – криминалистические средства.

Тема 6. Защита от информационных преступлений, посягающих на собственность банка

Хищения денежных средств, при совершении кредитных операций. Хищения денежных средств с незаконным использованием пластиковых карт. Хищения денежных средств с использованием аккредитивов. Хищение денежных средств с использованием чеков. Хищение денежных средств с использованием платежных поручений.

Раздел II. Технологии защиты информации в банковской деятельности

Тема 7. Защита от хищения денежных средств и иного имущества с использованием векселей (информационный аспект)

Правовая характеристика векселя. Риски в сфере вексельного обращения. Преступления против собственности, в которых вексель является предметом посягательств. Преступления против собственности, в которых вексель является средством совершения преступления. Меры предупреждения преступлений в сфере вексельного обращения.

Тема 8. Защита от информационных преступлений, посягающих на информационную безопасность функционирования банка

Злоупотребления полномочиями. Коммерческий подкуп. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка. Противоправные посягательства на кадровое обеспечение банка. Противоправные посягательства на нематериальные активы банка.

Тема 9. Организация противодействия отмыванию преступных доходов и финансированию терроризма (информационный аспект)

Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем. Криминалистическая характеристика легализации и отмывания преступных доходов. Система мер

предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

Тема 10. Комплексное обеспечение информационной безопасности банка

Информация, использующая в целях обеспечения безопасности банка, и ее источники. Бюро кредитных историй. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность банка

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

Методические указания для самостоятельной работы обучающихся по освоению дисциплины представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Безопасность банковских и платежных ИС» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Гамза В. А. Безопасность банковской деятельности: учебник для вузов / В. А. Гамза, И. Б. Ткачук, И. М. Жилкин. — 5 изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 455 с. — (Высшее образование). ISBN 978-5-534-13582-4

2. Кибербезопасность в условиях электронного банкинга: Практическое пособие / Под ред. П.В. Ревенкова. — М.: Прометей, 2020. — 522 с.: ISBN 978-5-907244-61-0 https://znanium.com/catalog/document?id=374846

3. Ясенев В.Н. Информационные системы в экономике: учебное пособие / В.Н. Ясенев, О.В. Ясенев. — Москва: КНОРУС, 2021. — 428 с. — (Бакалавриат). ISBN 978-5-406-05416-1 https://www.knorus.ru/catalog/informatika/591769-informacionnye-sistemy-v-ekonomike-bakalavriat-uchebnoe-posobie/

Дополнительная литература:

1. 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

2. Национальная платежная система. Бизнес-энциклопедия / под ред. А.С. Воронин. - М. :ЦИПСиР, 2018. - 422 с. - ISBN 978-5-406-02526-0https://biblioclub.ru/index.php?page=book&id=235075

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал.
3. **www.wikIsec.ru**- Энциклопедия информационной безопасности.
4. **www.biblioclub.ru** - Университетская библиотека онлайн.
5. **www.rucont.ru**- ЭБС «Руконт».
6. **http://www.academy.it.ru/–** академия АЙТИ.
7. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации**.**
9. **http://www.fsb.ru/ -** Официальный сайт Федеральной Службы Безопасности
10. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды МГОТУ.
2. Рабочая программа и методическое обеспечение по дисциплине: «Безопасность банковских и платежных информационных систем»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«БЕЗОПАСНОСТЬ БАНКОВСКИХ И ПЛАТЕЖНЫХ ИС»

(Приложение 1 к рабочей программе)

Специальность: 38.05.01 Экономическая безопасность

Специализация: Экономико-правовое обеспечение экономической безопасности

Квалификация (степень) выпускника: экономист

Форма обучения: очная, заочная

Королев
2023

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	Код и наименование индикатора достижения универсальной компетенции		
				Трудовые действия	**Необходимые умения**	**Необходимые знания**
1	ОПК-6	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.	Тема 1-10	ОПК-6. И-1. Использует современные специализированные программные средства коммуникации и справочные системы для решения профессиональных задач	ОПК-6. И-1. У-1. Умеет использовать современные специализированные программные средства коммуникации и справочные системы для решения профессиональных задач (СПС Консультант+, Гарант, TrueConf Server, Zoom, Яндекс.Телемост и др.)	ОПК-6. И-1. З-1. Знает методы работы с современными специализированными программными средствами коммуникации и справочными системами для решения профессиональных задач
2	ОПК-7	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	Тема 1-10	ОПК-7. И-1. Имеет представление, понимает принципы работы современных информационных технологий в экономике, программных средств для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач	ОПК-7. И-1. У-1. Умеет осуществлять поиск, аккумулирование, хранение, обработку, анализ, планирование, оценку и передачу данных при решении профессиональных задач с использованием современных информационных технологий	ОПК-7. И-1. З-1. Знает принципы работы современных информационных технологий в экономике и программных средств
3	ПК-4	Способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять	Тема 1-10	ПК-4. И-1. Создает организационно-управленческую и информационную структуру интегральной системы управления рисками, разрабатывает проекты нормативных и методических	ПК-4. И-1. У-1. Умеет создавать организационно-управленческую и информационную структуру интегральной системы управления рисками; ПК-4. И-1. У-2. Умеет разрабатывать проекты нормативных и	ПК-4. И-1. З-1. Знает принципы создания организационно-управленческой и информационной структуры интегральной системы управления рисками; ПК-4. И-1. З-2. Знает

		координацию работ по технико-информационному обеспечению системы стратегического управления рисками		материалов, регламентирующих работу по защите информации, предлагает технологии защиты информации, безопасную систему внутренней и внешней коммуникации и отчетности	методических материалов, регламентирующих работу по защите информации, ПК-4. И-1. У-3. Умеет осуществлять выбор средств и технологий защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности	методические материалы, регламентирующие работу по защите информации, ПК-4. И-1. З-3. Знает технологии защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности
				ПК-4. И-3. Использует современные принципы, методы и технологии работы с информацией, принципы и методы управления проектами, положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности	ПК-4. И-3. У-1. Умеет использовать современные принципы, методы и технологии работы с информацией, ПК-4. И-3. У-2. Умеет применять принципы и методы управления проектами, ПК-4. И-3. У-3. Умеет использовать положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности	ПК-4. И-3. З-1. Знает современные принципы, методы и технологии работы с информацией ПК-4. И-3. З-2. Знает принципы и методы управления проектами ПК-4. И-3. З-3. Знает положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности
				ПК-4. И-6. Решает поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации	ПК-4. И-6. У-1. Умеет решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации	ПК-4. И-6. З-1. Знает принципы и требования обеспечения сохранения государственной и коммерческой тайны и конфиденциальной информации. ПК-4. И-6. З-2. Знает принципы работы в системах электронного документооборота; ПК-4. И-6. З-3. Знает действующее российское законодательство в сфере защиты государственной и коммерческой тайны и конфиденциальной информации

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Этапы и показатель оценивания компетенции	Шкала и критерии оценки
ОПК-6 ОПК-7 ПК-4	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ОПК-6 ОПК-7 ПК-4	Контрольная работа	А) полностью сформирована 5 баллов В) частично сформирована 3-4 балла С) не сформирована 2 балла	Проводится письменно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной

			презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Понятия и концепция информационной безопасности банка.
2. Банк как объект защиты информации.
3. Система информационных угроз безопасности банка.
4. Банк как субъект борьбы с противоправными посягательствами (информационный аспект).
5. Система правового обеспечения информационной безопасности банка.
6. Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания.
7. Банковское законодательство: Нормативные акты Банка России и стандарт ИБ банка России.
8. Содержание аудита по ИБ технических средств обработки информации.
9. Организация системы информационной безопасности банка.
10. Субъекты обеспечения информационной безопасности банка.
11. Средства и методы обеспечения безопасности банка.
12. Организация внутреннего контроля банка (аспект ЗИ).
13. Организация службы информационной безопасности банка.
14. Система технических средств информационной безопасности банка.
15. Технические средства охраны банковских операций и продуктов.
16. Технико – криминалистические средства защиты информации банка.
17. Защита от хищения денежных средств при совершении кредитных операций.
18. Защита от хищения денежных средств с незаконным использованием пластиковых карт.
19. Защита от хищения денежных средств с использованием аккредитивов.
20. Защита от хищения денежных средств с использованием чеков.
21. Защита от хищения денежных средств с использованием платежных поручений.
22. Правовая характеристика векселя и особенности ее защиты.
23. Риски в сфере вексельного обращения и их информационная безопасность.
24. Преступления против собственности, в которых вексель является предметом посягательств (аспект ЗИ).
25. Меры предупреждения преступлений в сфере вексельного обращения (аспект ЗИ).

26. Злоупотребления полномочиями (аспект ЗИ).
27. Коммерческий подкуп (аспект ЗИ).
28. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну (аспект ЗИ).
29. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка (аспект ЗИ).
30. Противоправные посягательства на кадровое обеспечение банка. Противоправные посягательства на нематериальные активы банка (аспект ЗИ).
31. Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем (аспект ЗИ).
32. Криминалистическая характеристика легализации отмывания преступных доходов (аспект ЗИ).
33. Информационная безопасность и система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.
34. Информация, использующая в целях обеспечения информационной безопасности банка, и ее источники.
35. Бюро кредитных историй (аспект ЗИ).
36. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на информационную безопасность банка.

Примерная тематика заданий на контрольную работу:

1. Средства и методы обеспечения безопасности банка.
2. Организация внутреннего контроля банка (аспект ЗИ).
3. Организация службы информационной безопасности банка.
4. Система технических средств информационной безопасности банка.
5. Технические средства охраны банковских операций и продуктов.
6. Технико – криминалистические средства защиты информации банка.
7. Защита от хищения денежных средств при совершении кредитных операций.
8. Защита от хищения денежных средств с незаконным использованием пластиковых карт.
9. Защита от хищения денежных средств с использованием аккредитивов.
10. Защита от хищения денежных средств с использованием чеков.
11. Защита от хищения денежных средств с использованием платежных поручений.
12. Преступления против собственности, в которых вексель является предметом посягательств (аспект ЗИ).
13. Меры предупреждения преступлений в сфере вексельного обращения (аспект ЗИ).
14. Злоупотребления полномочиями (аспект ЗИ).
15. Коммерческий подкуп (аспект ЗИ).
16. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну (аспект ЗИ).
17. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка (аспект ЗИ).
18. Противоправные посягательства на кадровое обеспечение банка.
19. Противоправные посягательства на нематериальные активы банка (аспект ЗИ).
20. Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем (аспект ЗИ).
21. Криминалистическая характеристика легализации отмывания преступных доходов (аспект ЗИ).

22. Информационная безопасность и система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.
23. Информация, использующая в целях обеспечения информационной безопасности банка, и ее источники.
24. Бюро кредитных историй (аспект ЗИ).
25. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на информационную безопасность банка.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Программой предусмотрены следующие виды контроля: два текущих контроля в форме тестирования, промежуточный контроль в форме зачета и контрольной работы.

Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
тестирование	ОПК-6 ОПК-7 ПК-4	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
тестирование	ОПК-6 ОПК-7 ПК-4	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Зачет	ОПК-6 ОПК-7 ПК-4	3 вопроса	Зачет проводится	Результаты предоставляю	Критерии оценки: «**Отлично**»:

			в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	тся в день проведения зачета	• знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на

					практических занятиях; «**Неудовлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся, согласно приказу «О внедрении новой балльно-рейтинговой системы контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся» № 01-04/428 от 25 сентября 2020 г.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1) Из какого материала производят банковские карточки?

(!) бумажные;
(!) пластиковые;
(?) деревянные;
(!) металлические.

2) В какое время появились карточки с магнитной полосой?

(?) В 40-е гг XX столетия;
(?) в 50-е гг XX столетия;
(!) в 60-е гг XX столетия;
(?) в 70-е гг XX столетия.

1) Какая операция проводится эмитентом в случае утери карты:

(?) Держателю карты выносят штраф;
(!) Номер карты заносится в стоп-лист;
(?) Эмитент отказывается от сотрудничества с держателем карты.
(?) Все из вышеперечисленного.

2) **Какую операцию выполняет кассир (сотрудник предприятия торговли) при оплате картой в магазине:**

(!) Идентификацию;
(?)Аутентификацию;
(!) Авторизацию;
(?) Все эти операции.

3) Под дебетовой картой понимают?

(!) карта позволяющая рассчитываться в пределах остатка на счете:
(?) карта позволяющая рассчитываться в пределах установленных лимитов:
(?) карта позволяющая рассчитываться в пределах как установленных лимитов так и в пределах остатка на счете:
(?) карта при выдаче которой записывается базовый остаток и дата его возобновления:

4) «защищенный остаток» памяти микропроцессора предназначен?

(!) для хранения крупных денежных сумм и проведения расходных операций с предъявлением ПИНа:
(?) для хранения небольших денежных сумм:
(?) для пополнения счета карта без предъявления ПИНа:
(?) память микропроцессора не содержит «защищенный остаток»:

5) Каким количеством способов может быть проведен этап авторизации при оплате заказных товаров у интернет-магазина?

(!) 2
(?) 3
(?) 5
(!) 6

6) Хранящиеся на сервере копии электронных документов по всем операциям доступны

(!)продавцам и покупателям в любой момент времени
(?) только продавцам в течении 48часов после проведения операции расчета
(?)только покупателям в течении 48часов после проведения операции расчета
(?)продавцам в любой момент времени

7) Платежная интернет-система ASSIST позволяет

(!) в реальном времени проводить авторизацию и процессинг платежей, совершаемых при помощи кредитных карт с любого компьютера, подключенного к интернет
(?)в реальном времени проводить авторизацию при помощи кредитных карт с любого компьютера, подключенного к интернет
(?)в реальном времени проводить процессинг платежей, совершаемых при помощи кредитных карт с любого компьютера, подключенного к интернет
(?) верный ответ не представлен

8) Что понимается под системой «Клиент-Банк»:

(!) комплекс, используемый клиентами коммерческого банка и автоматизации документооборота между банком и его клиентами;
(?) комплекс, используемый клиентами некоммерческого банка и автоматизации документооборота
(?) комплекс, не используемый клиентами банка
(?) нет верного варианта

9) Основное назначение системы «Клиент-Банк»:

(!)сократить число визитов клиента в офис банка и формализовать процесс обмена документами
(?) увеличить число визитов клиента в офис банка и формализовать процесс обмена документами
(?) формализовать процесс обмена документами
(?)увеличить количество клиентов

10) Что имеет наибольшее значение для клиента банка в системе:

(!) простота эксплуатации
(!)функциональная полнота системы
(?) простота внедрения
(?) защищенность от НСД

11) Что имеет наибольшее значение для банка при функционировании системы

(?)простота эксплуатации
(?)функциональная полнота системы
(!) простота внедрения
(!) защищенность от НСД

12) Принципиальная особенность системы «Клиент-Банк» на основе технологии «тонкого клиента»:

(!) вся информация передается в банк по мере её ввода клиентом
(?) информация не передаётся в банк по мере ввода клиентом
(?) клиент не вводит информацию в банк
(?) нет верного ответа

13) Что под собой подразумевает WAP-банкинг:

(!) использование в качестве клиентской части системы мобильного протокола

(?)использование в качестве серверной части системы мобильного протокола

(?) использование в качестве клиентской части системы транспортного протокола

(?) нет правильного варианта

14) Что такое WAP?

(!) протокол, с помощью которого информация из Интернет передаётся на небольшой дисплей мобильного телефона

(?)протокол, с помощью которого информация из Интернет не передаётся на дисплей мобильного телефона

(?) устройство, с помощью которого информация из Интернет передаётся на небольшой дисплей мобильного телефона

(?) протокол, с помощью которого информация передаётся со стационарного телефона на небольшой дисплей мобильного телефона

15) Выбор организации работы клиента с коммерческим банком зависит от факторов:

(?)удаленность клиента от офиса банка

(?)наличие коммуникационных каналов

(?)удобство эксплуатации клиентской части системы

(!) количество клиентов банка

16) Расшифруйте аббревиатуру WAP:

(!)Wireless Application Protocol

(?)Wireless Application Prototype

(?)Wireless Application Protection

(?)Windows Application Protocol

17) Что в общем случае подразумевается под интернет-банкингом:

(!)оказание банковских услуг через интернет

(?)оказание банковских услуг через терминал

(?) оказание банковских услуг физическим лицам

(?)оказание банковских услуг юридическим лицам

18) В системе «Клиент-Банк» возможно использование информационных технологий:

(!)тонкий клиент

(!)толстый клиент

(?)умеренный клиент

(?)полный клиент

19) Два основных типа каналов связи:

(!)коммутируемый

(!) выделенный

(?) забронированный

(?)воздушный

20) Типы уровней доступных операций взаимодействия клиента с банком:

(!) информационный

(!)транзакционный

(?) биологический

(?)социальный

21) Что подразумевается под SMS-банкингом:

(!)возможность заказывать и получать информацию посредством SMS-сообщений одного из провайдеров мобильной связи

(?) возможность блокировать информацию посредством SMS-сообщений одного из провайдеров мобильной связи

(?) возможность только заказывать и получать денежные средства посредством SMS-сообщений одного из провайдеров мобильной связи

(?) нет правильного ответа

22) Что подразумевается под переводом в валюты:

(!)ввод формы для осуществления валютного перевода

(?)вывод формы для осуществления валютного перевода

(?)ввод формы для осуществления текстового перевода

(?) ввод формы для осуществления оплаты услуг ЖКХ

23) Что подразумевается под обменными операциями:

(!) операции по конвертации из одной валюты в другую

(?)операции по конвертации из одной валюты в ту же валюту

(?)операции по конвертации валового продукта

(?)нет правильного варианта

24) Что подразумевается под регулярными платежами:

(!) возможность заказа регулярных платежей со своего счёта на другие счета

(?) возможность заказа регулярных платежей с чужого счёта

(?) не возможность заказа регулярных платежей со своего счёта на другие

(?)возможность периодического пополнения своего счета

25) Уровни поддержки решений для интернет - банкинга:

(?) Базовый

(?)Расширенный

(?)Полная

(!)все варианты верны

26) Суть классической системы «Клиент-Банк» с «толстым клиентом»:

(!)на стороне клиента устанавливается специальное программное обеспечение, которое является частью БИС

(?) на стороне банка устанавливается специальное программное обеспечение, которое является частью БИС

(?)на стороне клиента устанавливается антивирусное программное обеспечение
(?)нет правильного варианта

27) Расшифруйте аббревиатуру БИК:

(!)банковский идентификационный код
(?) банковский интернет-клиент
(?) банковские, информационный коммуникации
(?) белорусский интернет-клиент

28) Под расчётами, в рамках какой-либо коммерческой сделки, заключаемой в устрой или письменной форме понимается:

(!)технология проведения оплаты.
(?)способ передачи денежных средств
(?)способ взаимодействия клиента с банком
(?)технология проведения расчётов

29) Межбанковский расчёт отличается от межхозяйственных:

(!)количественными и качественными характеристиками (?)
(?)формой проведения
(?)суммой денег, вовлечённых в расчёт
(?)участием банка в операции

30) Безналичный расчёт осуществляется через:

(!)Посредника
(?)Брокера
(?)Юриста
(?)Банк

31) Безналичные расчёты бывают:

(!)С платёжным поручением
(!)С платёжным требованием
(?)С платёжными транзакциями
(?)С платёжными рисками

32) Телефонный банкинг выделяется за счёт:

(!)Использования базовых телефонных функций
(?)Возможностью мобильного использования банка
(?)Использования базовых компьютерных функций
(?)Развития информационных технологий

33) Система клиент-банк организует:

(!)Электронный документооборот между банками и его клиентами
(?)Электронный документооборот между банками
(?)Электронный документооборот между клиентами
(?)Электронный документооборот между контрагентами

34) Система клиент-банк основывается на технологии:

(!)Тонкий клиент
(!)Толстый клиент
(?)Платёжный клиент

(?)Онлайн клиент

35) Электронный чек отличается от бумажного:

(!)Формой представления
(?)Информативностью
(?)Идентификаторами
(?)Всем вышеперечисленным

36) Какие факторы в большей степени влияют на платёжные интернет-системы:

(!)Экономические потребности
(?)Технологические возможности
(?)Правовая база
(?)Состоянием экономики

37) В традиционных формах расчёта все формы безналичных расчётов выполняются через:

(!)Финансового посредника
(?)Маклера
(?)Брокера
(?)Банк

38) В основе внешних информационных взаимодействий коммерческого банка лежат:

(!)Компьютерные сети
(?)Телефонные сети
(?)Банковские сети
(?)Телекоммуникационные сети

39) Международные расчёты выполняются через систему:

(!)SWIFT
(?)RINET
(?)EDIFER
(?)OEDIPE

40) При разработке «Стандарты публикации финансовой отчётности коммерческих банков» в качестве начального стандарта была выбрана спецификация языка:

(!)XBRL
(?)XLRB
(?)LBRL
(?)RBXL

4.2. Типовые вопросы, выносимые на зачет

1. Назначение и содержание политики информационной безопасности на примере КБ «Максима» (ООО)
2. Основные направления развития ИБ кредитно-финансовой сферы на период 2021–2023 гг.

3. Предпосылки и тренды развития ИБ кредитно-финансовой сферы
4. Задачи и основные направления деятельности ЦБ в области ИБ
5. Общие положениям обеспечения ИБ кредитно-финансовой сферы
6. Правовое регулирование обеспечения ИБ кредитно-финансовой сферы
7. Обеспечение ИБ и киберустойчивости инфраструктуры кредитно-финансовой сферы
8. Обеспечение ИБ и киберустойчивости прикладного программного обеспечения
9. Обеспечение ИБ и киберустойчивости технологий обработки данных
10. Обеспечение ИБ и киберустойчивости финансовых технологий
11. Подготовка кадров и обеспечение доверия граждан к цифровой среде
12. Международное сотрудничество по вопросам ИБ кредитно-финансовой сферы
13. Национальная программа «Цифровая экономика РФ» и вопросы ИБ кредитно-финансовой сферы
14. Центр компетенций по обеспечению ИБ и противодействию кибератакам в кредитно-финансовой сфере
15. Контрольно-надзорные полномочия Банка России в сфере ИБ и киберустойчивости
16. Национальный стандарт Российской Федерации ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 № 822-ст)
17. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента ИБ Банка (ФинЦЕРТ Банка России).
18. Положение Банка России от 4 июня 2020 г. № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» и внесенные изменения.
19. Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
20. Положение Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»

21. Приказ Росстандарта от 21.08.2017 № 1759 «Об организации деятельности технического комитета по стандартизации «Стандарты финансовых операций».
22. Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»
23. Требования по защите информации при обмене электронными сообщениями в платежной системе Банка России.
24. Внешний аудит ИБ банковской сферы.
25. Варианты проведения оценки соответствия ИБ кредитно-финансовой сферы.
26. Организационные мероприятия по реализации требований к СКЗИ кредитно-финансовой сферы.
27. Технические решения, необходимые для реализации требований к СКЗИ кредитно-финансовой сферы.
28. Основные аутсорсинговые услуги, предоставляемые банкам по ИБ.
29. Стандарт Банка России СТО БР ИББС-1.4-2018 «Обеспечение ИБ организаций банковской системы Российской Федерации. Управление рисками нарушения ИБ при аутсорсинге»
30. Стратегия развития ИБ финансовой сферы 2020-2022. Доклад Зампредседателя Банка России Дмитрия Скобелкина на XII Уральском форуме.

Приложение 2

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«БЕЗОПАСНОСТЬ БАНКОВСКИХ И ПЛАТЕЖНЫХ ИС»

(Приложение 2 к рабочей программе)

Специальность: 38.05.01 Экономическая безопасность

Специализация: Экономико-правовое обеспечение экономической безопасности

Квалификация (степень) выпускника: экономист

Форма обучения: очная, заочная

Королев
2023

1. Общие положения

Целями изучения дисциплины являются:

1. Формирование у студентов специализированной базы знаний по основным понятиям в области информационной безопасности банковской деятельности;
2. Приобретение студентами первичных навыков по практическому формированию документов, составляющих правовую базу защиты информации в банковской сфере.
3. Повышение уровня специальных знаний в области защиты информационно - телекоммуникационной инфраструктуры и компьютерной информации в банковской сфере.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общепрофессиональные компетенции

- ОПК-6 - Способен использовать современные информационные технологии и программные средства при решении профессиональных задач;
- ОПК-7 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Профессиональные компетенции

- ПК-4 - Способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-информационному обеспечению системы стратегического управления рисками

Основными **задачами** дисциплины являются:

- ознакомление студентов с основами информационной безопасности банковской деятельности на основе действующего российского законодательства;
- ознакомление с описанием угроз безопасности кредитно-финансовой деятельности;
- изучение основы организации противодействия угрозам информационной безопасности в кредитно-финансовой сфере;
- освоение основных инструментов защиты информации в банковских и платежных системах;
- формирование системы знаний в области защиты информации в кредитно-финансовой сфере.
- ознакомление с методами и средствами защиты информации функциональных и контролирующих подразделений финансово – кредитных организаций.

2. Указания по проведению практических занятий

Тема 1. Концептуальные основы информационной безопасности банка

Практическое занятие 1.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности банка.

Основные положения темы занятия:

1. базовые составляющие концепции информационной безопасности банка.

2. основные направления обеспечения информационной безопасности банковской деятельности.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Понятия и концепция информационной безопасности банка.
2. Банк как объект противоправных посягательств.
3. Система информационных угроз безопасности банка.
4. Банк как субъект борьбы с противоправными посягательствами.

Продолжительность занятия – 1.25/0.25 часа.

Тема 2. Правовые основы информационной безопасности банка

Практическое занятие 2.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности банка в соответствии с требованиями законодательства.

Основные положения темы занятия:

1. базовые составляющие правого обеспечения информационной безопасности банка.

2. стратегия информационной безопасности типового банка.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Система правового обеспечения безопасности банка.
2. Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания.
3. Банковское законодательство.
4. Нормативные акты Банка России.
5. Внутренние нормативные акты.
6. Содержание аудита по информационной безопасности технических средств обработки информации.

Продолжительность занятия – 1.25/0.25 часа.

Тема 3. Организационные основы информационной безопасности банка

Практическое занятие 3.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки организации работы типовых структурных подразделений службы безопасности банка.

Основные положения темы занятия:

1. базовые составляющие организационного обеспечения информационной безопасности банка.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Организация системы безопасности банка.
2. Субъекты обеспечения безопасности банка.
3. Средства и методы обеспечения безопасности банка. Организация внутреннего контроля банка.
4. Организация службы безопасности банка.

Продолжительность занятия – 1.25/0.25 часа.

Тема 4. Техника обеспечения информационной безопасности банка

Практическое занятие 4.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки организации работы типовых структурных подразделений службы безопасности банка.

Основные положения темы занятия:

1. технические средства охраны банка.
2. безопасность банковских расчетов

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Система технических средств информационной безопасности банка. Технические средства охраны.
2. Технические средства охраны банковских операций и продуктов.
3. Технико – криминалистические средства.

Продолжительность занятия – 1.25/0.25 часа.

Тема 5. Защита от информационных преступлений, посягающих на собственность банка

Практическое занятие 5.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки организации работы службы безопасности по проведению расследований инцидентов информационной безопасности.

Основные положения темы занятия:

1. Характеристика преступлений связанных с хищением денежных средств.
2. безопасность банковских расчетов

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Хищения денежных средств при совершении кредитных операций.
2. Хищения денежных средств с незаконным использованием пластиковых карт.
3. Хищения денежных средств с использованием аккредитивов.
4. Хищение денежных средств с использованием чеков. Хищение денежных средств с использованием платежных поручений.

Продолжительность занятия – 1.5/0.5 часа.

Тема 6. Стандарты информационной безопасности банка

Практическое занятие 6.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки организации учета требований стандартов информационной безопасности банка.

Основные положения темы занятия:

1. Характеристика российских и международных стандартов банковской деятельности.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. О Стандарте Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.
2. Основные цели и задачи стандарта Банка России при обеспечении информационной безопасности.
3. Основные направления работы по дальнейшему сопровождению и доработке Стандарта в рамках специально созданного Подкомитетом 3 “Защита информации в кредитно-финансовой сфере” Технического комитета 362 “Защита информации” Федерального агентства по техническому регулированию и метрологии.
4. Аудит информационной безопасности банка.
5. Преимущества и недостатки выполнения работ по защите ПДн в рамках Стандарт Банка России СТО БР ИББС 1.0-2014.

Продолжительность занятия – 1.5/0.5 часа.

Тема 7. Хищения денежных средств и иного имущества с использованием векселей (информационный аспект) Практическое занятие 7.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в противодействии хищения денежных средств в сфере вексельного обращения.

Основные положения темы занятия:

1. Противодействие хищению денежных средств и иного имущества с использованием векселей.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Правовая характеристика векселя. Риски в сфере вексельного обращения.
2. Преступления против собственности, в которых вексель является предметом посягательств.
3. Преступления против собственности, в которых вексель является средством совершения преступления.
4. Меры предупреждения преступлений в сфере вексельного обращения.

Продолжительность занятия – 1.5/0.5 часа.

Тема 8. Защита от информационных преступлений, посягающих на информационную безопасность функционирования банка Практическое занятие 8.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в защите от информационных преступлений.

Основные положения темы занятия:

1. Противодействие преступлениям, посягающим на информационную безопасность банка.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Злоупотребления полномочиями.

2. Коммерческий подкуп.

3. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну.

4. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка.

5. Противоправные посягательства на кадровое обеспечение банка.

6. Противоправные посягательства на нематериальные активы банка.

Продолжительность занятия – 1.5/0.5 часа.

Тема 9. Организация противодействия отмыванию преступных доходов и финансированию терроризма (информационный аспект)

Практическое занятие 9.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в противодействии отмыванию доходов полученных преступным путем.

Основные положения темы занятия:

1. Противодействие преступлениям, с вязанных с отмыванием доходов полученных преступным путем и финансированием терроризма.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем.
2. Криминалистическая характеристика легализации (отмывания преступных доходов).
3. Система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

Продолжительность занятия – 1.5/0.5 часа.

Тема 10. Комплексное обеспечение информационной безопасности банка

Практическое занятие 10.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в формировании комплексной системы информационной безопасности банка.

Основные положения темы занятия:

1. Основные требования предъявляемые к системе обеспечения банковской деятельности.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Информация, использующая в целях обеспечения безопасности банка, и ее источники.
2. Бюро кредитных историй.

3. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность банка.

Продолжительность занятия – 1.5/0.5 часа.

3. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области существующих современных аппаратных средств вычислительной техники;

2) привить навыки самостоятельного решения нестандартных задач в области аппаратных средств вычислительной техники.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная/заочная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	**60/92**
Вопросы, выносимые на самостоятельное изучение	10/20
Подготовка к практическим занятиям	20/26
Подготовка к лабораторным занятиям	-
Подготовка докладов	20/26
Выполнение практических заданий	10/20

Вопросы, выносимые на самостоятельное изучение
для очной формы обучения:

1. Информационные технологии управления в банке и роль информационной безопасности при их применении.
2. Состав и свойства информационных объектов банка.
3. Информационная безопасность при оказании услуг и выполнении операций в кредитном учреждении.
4. Организационные структуры и управленческие функции в банке.
5. Информационное взаимодействие управленческой и аналитической служб банка.
6. Роль и место службы информационной безопасности банка.
7. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.
8. Информационная безопасность подсистемы работы с банковскими картами.

9. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.
10. Информационная безопасность подсистемы операций с ценными бумагами.
11. Информационная безопасность подсистемы инкассации и подсистемы межбанковского взаимодействия.
12. Информационная безопасность подсистемы управления ресурсами (дилинга).
13. Информационная безопасность в подсистеме обеспечения безопасности.
14. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.
15. Информационная безопасность подсистемы удаленного банковского обслуживания.
16. Информационная безопасность подсистемы обеспечения внутренней деятельности банка как субъекта экономики.
17. Информационная безопасность системы электронного документооборота банка.
18. Информационная безопасность традиционных технологий расчетов.
19. Информационная безопасность и архитектура системы «Клиент – банк».
20. Информационная безопасность и способы передачи информации до компьютерной сети банка.
21. Информационная безопасность системы телефонного банкинга.

Вопросы, выносимые на самостоятельное изучение для заочной формы обучения:

1. Национальная программа «Цифровая экономика РФ» и вопросы ИБ кредитно-финансовой сферы.
2. Центр компетенций по обеспечению ИБ и противодействию кибератакам в кредитно-финансовой сфере.
3. Контрольно-надзорные полномочия Банка России в сфере ИБ и киберустойчивости.
4. Национальный стандарт Российской Федерации ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 № 822-ст).
5. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента ИБ Банка (ФинЦЕРТ Банка России).

6. Положение Банка России от 4 июня 2020 г. № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» и внесенные изменения.

7. Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

8. Положение Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

9. Приказ Росстандарта от 21.08.2017 № 1759 «Об организации деятельности технического комитета по стандартизации «Стандарты финансовых операций».

10. Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

11. Требования по защите информации при обмене электронными сообщениями в платежной системе Банка России.

12. Внешний аудит ИБ банковской сферы.

13. Варианты проведения оценки соответствия ИБ кредитно-финансовой сферы.

14. Организационные мероприятия по реализации требований к СКЗИ кредитно-финансовой сферы.

15. Технические решения, необходимые для реализации требований к СКЗИ кредитно-финансовой сферы.

16. Основные аутсорсинговые услуги, предоставляемые банкам по ИБ.

17. Стандарт Банка России СТО БР ИББС-1.4-2018 «Обеспечение ИБ организаций банковской системы Российской Федерации. Управление рисками нарушения ИБ при аутсорсинге»

18. Стратегия развития ИБ финансовой сферы 2020-2022. Доклад Зампредседателя Банка России Дмитрия Скобелкина на XII Уральском форуме.

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	10/20	Изучение открытых источников
2.	Подготовка к практическим занятиям	20/26	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	-/-	Изучение открытых источников
4.	Тематика докладов	20/26	См. примерные темы докладов
5.	Выполнение практических заданий	10/20	Информационная безопасность ДБО

Примерные темы докладов

1. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.
2. Информационная безопасность подсистемы работы с банковскими картами.
3. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.
4. Информационная безопасность подсистемы операций с ценными бумагами.
5. Информационная безопасность подсистемы инкассации и подсистемы межбанковского взаимодействия.
6. Информационная безопасность подсистемы управления ресурсами (дилинга).
7. Информационная безопасность в подсистеме обеспечения безопасности.
8. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.
9. Информационная безопасность подсистемы удаленного банковского обслуживания.
10. Информационная безопасность подсистемы обеспечения внутренней деятельности банка как субъекта экономики.
11. Информационная безопасность системы электронного документооборота банка.
12. Информационная безопасность традиционных технологий расчетов.

13. Информационная безопасность и архитектура системы «Клиент – банк».

14. Информационная безопасность и способы передачи информации до компьютерной сети банка.

15. Информационная безопасность системы телефонного банкинга.

16. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»

17. Информационная безопасность модели Интернет - банкинга.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

3. В процессе изложения материала необходимо давать ссылки на используемую литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Гамза В. А. Безопасность банковской деятельности: учебник для вузов / В. А. Гамза, И. Б. Ткачук, И. М. Жилкин. — 5 изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 455 с. — (Высшее образование). ISBN 978-5-534-13582-4

2. Кибербезопасность в условиях электронного банкинга: Практическое пособие / Под ред. П.В. Ревенкова. — М.: Прометей, 2020. — 522 с.: ISBN 978-5-907244-61-0 https://znanium.com/catalog/document?id=374846

3. Ясенев В.Н. Информационные системы в экономике: учебное пособие / В.Н. Ясенев, О.В. Ясенев. — Москва: КНОРУС, 2021. — 428 с. — (Бакалавриат). ISBN 978-5-406-05416-1 https://www.knorus.ru/catalog/informatika/591769-informacionnye-sistemy-v-ekonomike-bakalavriat-uchebnoe-posobie/

Дополнительная литература:

1. 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

2. Национальная платежная система. Бизнес-энциклопедия / под ред. А.С. Воронин. - М. :ЦИПСиР, 2018. - 422 с. - ISBN 978-5-406-02526-0https://biblioclub.ru/index.php?page=book&id=235075

3. Воронин, А. С. Национальная платежная система. Бизнес-энциклопедия [Электронный ресурс] / Коллектив авторов; ред.-сост. А. С. Воронин. - М.:КНОРУС: ЦИПСиР, 2013 - 424 с. - ISBN 978-5-406-02526-0http://znanium.com/bookread2.php?book=522012

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал.
3. **www.wikIsec.ru**- Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru**- ЭБС «Руконт».
6. **http://www.academy.it.ru/–** академия АЙТИ.
7. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации**.**
9. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности
10. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения: *MSOffice.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ.
2. Рабочая программа и методическое обеспечение по дисциплине «Безопасность банковских и платежных информационных систем».