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

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.В.ДВ.03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КРЕДИТНО-ФИНАНСОВЫХ ОПЕРАЦИЙ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Организация и технологии защиты информации
Уровень высшего образования: бакалавриат
Форма обучения: очная, очно-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: Сухотерин А.И. Рабочая программа дисциплины: «Информационная безопасность кредитно-финансовых операций». – Королев МО: «Технологический университет», 2023.

Рецензент: **Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

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

Рабочая программа согласована:

Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

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

2

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

Цел изучения дисциплины является:

1. Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации при проведении кредитно-финансовых операций;
2. Повысить уровень ямиспециальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
3. Формирование у студентов специализированной базы знаний по основным понятиям в области банковских информационных систем и технологий кредитно- финансовых операций;
4. Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации в банковской сфере (обеспечение электронной коммерции и интернет – расчетов).

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Профессиональные компетенции:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности

ПК-2. Способность принимать участие в проведении экспериментальных исследований системы защиты информации.

Основными **задачами** дисциплины являются:

1. Теоретические основы подготовки студентов для самостоятельного решения поставленных задачи в области применения банковских информационных систем и технологий на основе действующего российского законодательства с помощью с помощью современных принципов, методов, сил и средств в различных организационных структурах;
2. Практические аспекты формирования подходов обучаемых к выполнению самостоятельных исследований в области защиты информации в кредитно-финансовых организациях по базовым направлениям защиты банковской тайны и конфиденциальной информации;
3. Формирование, у обучающихся системы знаний для применения основных методов и средств защиты информации кредитно-финансовых

операций инструментов и технологий функциональных и контролирующих подразделений кредитно-финансовой организации.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;

Необходимые умения:

- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);
- применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;

Трудовые действия:

- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);
- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность кредитно-финансовых операций» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

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

Таблица1

Виды занятий	Всего часов	Семестр 6	Семестр 7	Семестр …	Семестр …
Общая трудоемкость	108	108	108		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32	32			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	66	66			
Другие виды контактной работы	10	10			
Практическая подготовка	8	8			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2			
Вид итогового контроля	Экзамен	Экзамен			
ОЧНО - ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	28		28		
Лекции (Л)	12		12		
Практические занятия (ПЗ)	16		16		
Лабораторные работы (ЛР)	-		-		
Самостоятельная работа	78		78		
Другие виды контактной работы	10		10		
Практическая подготовка	8		8		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+		+		
Вид итогового контроля	Экзамен		Экзамен		

Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное/очно-заочное	Практические занятия, час Очное/очно-заочное	Занятия в интерактивной форме, час Очное/очно-заочное	Практическая подготовка,час	Код компетенций
Тема 1: Информационная безопасность технологий электронных расчетов	2/1	2/2	2/2	**1/1**	ПК-1
Тема 2: Информационная безопасность при применении средств электронной цифровой подписи в кредитно-финансовых организациях	2/1	2/2	2/2	**1/1**	ПК-1
Тема 3:Информационная безопасность при выполнении электронных транзакций	2/1	2/2	2/2	**1/1**	ПК-1
Тема 4: Правовые и организационные основы применения ЭЦП в кредитно-финансовых организациях и оказании региональных электронных услуг	2/1	2/2	2/2	**1/1**	ПК-2
Тема 5: Информационная безопасность автоматизации расчетной функции в кредитно-финансовой организации и принципы построения защищенной электронной платежной системы	4/4	4/4	2/1	**2/2**	ПК-2
Тема 6: Информационная	4/4	4/4	2/1	**2/2**	ПК-1,2

безопасность и правила обмена электронными документами кредитно-финансовой организации и ее клиентами при осуществлении расчетов через расчетную сеть					
Итого:	16/12	16/16	12/10	8/8	

4.2. Содержание тем дисциплины

Тема 1: Информационная безопасность технологий электронных расчетов

Традиционные технологии расчетов и их автоматизированные (электронные) формы. Классификация расчетов по субъектам и формам. Структурная схема взаимодействия традиционных и автоматизированных (электронных) форм расчетов. Информационные технологии внешних взаимодействий КБ.

Назначение и архитектура системы «Клиент – банк». Способы передачи информации до компьютерной сети банка. Системы телефонного банкинга. Система «Клиент – банк» на основе технологии «толстого клиента» Понятие и модели Интернет - банкинга. Организация Интернет – банкинга через портал посредника –аутсорсера. Направления удаленного банковского обслуживания.

Классификация пластиковых карт. Чековые расчеты – основа банковской информационной технологии электронных расчетов. Участники карточной платежной системы и схема их работы. Расчеты банковскими картами в Интернете.

Тема 2: Информационная безопасность при применении средств электронной цифровой подписи в кредитно-финансовых организациях

Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Основные подходы, применяющиеся к решению задачи использования средств ЭЦП в сети межбанковских расчетов.

Тема 3. Информационная безопасность электронных транзакций

Основные понятия. Схема защищенного информационного обмена при использовании симметричных методов. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами. Симметричные алгоритмы

шифрования. Схема алгоритма работы сети Фейсталя. Режим электронной кодовой книги. Режим сцепления блоков шифротекста. Режим обратной связи по шифротексту. Режим обратной связи по выходу. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.

Тема 4: Правовые и организационные основы применения ЭЦП в кредитно-финансовых организациях и оказании региональных электронных услуг

Общее правило создания ЭЦП. Общее правило верификации ЭЦП. Защита электронных транзакций протокол (SSL). Схема работы протокола SET. Управление ключами. Распространение ключей в случае использования только симметричных методов преобразования информации. Распространение ключей в случае использования сертификатов открытых ключей. Электронные платежи с помощью цифровых денег.

Тема 5: Информационная безопасность автоматизации расчетной функции в кредитно-финансовой организации и принципы построения защищенной электронной платежной системы

Расчетная функция банков и ее автоматизация. Схема обработки платежного документа клиентами. Ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.

Тема 6: Информационная безопасность и правила обмена электронными документами кредитно-финансовой организации и ее клиентами при осуществлении расчетов через расчетную сеть

Правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД). Составление и направление ЭД участником – отправителем. Порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников. Порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

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 «Информационная безопасность кредитно-финансовых операций» приведена в Приложении 1.

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

Основная литература:

1.Кибербезопасность в условиях электронного банкинга : практическое пособие / под ред. П. В. Ревенкова. - Москва : Прометей, 2020. - 522 с. - ISBN 978-5-907244-61-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1284190 (дата обращения: 28.11.2022). – Режим доступа: по подписке.

2.Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 28.11.2022). – Режим доступа: по подписке.

Дополнительная литература:

3.Тавасиев, А. М. Банковское кредитование : учебник / А.М. Тавасиев, Т.Ю. Мазурина, В.П. Бычков ; под ред. А.М. Тавасиева. — 2-е изд., перераб. — Москва : ИНФРА-М, 2020. — 366 с. — (Среднее профессиональное образование). - ISBN 978-5-16-014239-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1039295 (дата обращения: 28.11.2022). – Режим доступа: по подписке.

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. – Публикации, статьи**.**
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.window.edu.ru** - Единое окно доступа.
6. **http://grebennikov.ru/** - Издательский дом «Гребенников»
7. **www.rucont.ru** - ЭБС «Руконт»
8. **http://www.minfin.ru -** Официальный сайт Министерства финансов Российской Федерации
9. **http://www.gov.ru** -Официальный сервер органов государственной власти Российской Федерации.

10. **http://www.fsb.ru** - Официальный сайт Федеральной Службы Безопасности
11. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методичские указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) 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.Электронные ресурсы образовательной среды Университета..
2.Информационно-справочные системы (Консультант+; Гарант)

Ресурсы информационно-образовательной среды МГОТУ:
Рабочая программа и методическое обеспечение по курсу «Информационная безопасность кредитно-финансовых операций»

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

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов по темам.

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КРЕДИТНО-ФИНАНСОВЫХ ОПЕРАЦИЙ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

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

№ п/п	Индекс компе-тенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ПК-1	Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности	Тема:1-8	- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);	- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);	- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
2.	ПК-2	Способность принимать участие в проведении экспериментальных исследований системы защиты	Тема:1-8	- разрабатывать модели, проекты и предложения в ходе проведения экспериме	- применять действующую нормативную базу выбирать целесообразные потребные	- руководящие и методические документы принципы организации по проведению экспериментальной

		информации		нтов деятельности по совершенствованию системы ЗИ;	средства и определять структуру системы ЗИ в ходе проведения экспериментов;	деятельности в области ЗИ;

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

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ПК-1,2	***Доклад***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	***Например:*** ***Проводится в письменной и/или устной форме.*** ***Критерии оценки:*** ***1. Соответствие содержания доклада заявленной тематике (1 балл).*** ***2. Качество источников и их количество при подготовке работы (1 балл).*** ***3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).*** ***4. Качество самой представленной работы (1 балл).*** ***5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).*** ***Максимальная сумма баллов - 5 баллов.***
ПК-1,2	***Выполнение контрольной работы***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u>***	***При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида***

		уровне – 4 балла; • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	

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. Технологии управления КБ и иные технологии оказания КБ услуги роль информационной безопасности при их применении.
2. Состав и свойства информационных объектов СБ (системы бюджетирования). Функциональность и алгоритмы СБ и ее информационная безопасность.
3. Информационная безопасность при оказании услуги и выполнении операций в кредитном учреждении.
4. Органические структуры. Управленческие функции и их разделение в банке. Информационное взаимодействие управленческой и аналитической служб. Организационная структура КБ. Подсистема ядра БИС. Роль и место службы информационной безопасности
5. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.
6. Информационная безопасность подсистемы работы с банковскими картами.
7. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.
8. Информационная безопасность подсистемы операций с ценными бумагами.
9. Информационная безопасность подсистема инкассации и подсистемы межбанковского взаимодействия.
10. Информационная безопасность подсистемы управления ресурсами (дилинга).
11. Информационная безопасность в подсистеме обеспечения безопасности.

12. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.
13. Информационная безопасность подсистема удаленного банковского обслуживания.
14. Информационная безопасность подсистема обеспечения внутренней деятельности кредитно-финансовой операции как субъекта экономики.
15. Информационная безопасность системы электронного документооборота банка.
16. Информационная безопасность традиционных технологий расчетов.
17. Информационная безопасность и архитектура системы «Клиент – банк».
18. Информационная безопасность и способы передачи информации до компьютерной сети кредитно-финансовой организации.
19. Информационная безопасность системы телефонного банкинга.
20. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
21. Информационная безопасность модели Интернет - банкинга.
22. Информационная безопасность расчетов банковскими картами в Интернете.
23. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
24. ИБ защищенного информационного обмена при использовании симметричных методов защиты информации.
25. ИБ защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
26. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
27. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.
28. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
29. Информационная безопасность электронных платежей с помощью цифровых денег.
30. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.
31. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.
32. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД) в кредитно-финансовой организации.
33. Информационная безопасность при составлении и направлении ЭД участником – отправителем.

34. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.

35. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

Примерная тематика заданий на контрольную работу:

1. Понятия и концепция информационной безопасности банка. Банк как объект противоправных посягательств.
2. Система угроз информационной безопасности банка.
3. Банк как субъект борьбы с противоправными посягательствами (информационный аспект).
4. Система правового обеспечения информационной безопасности банка.
5. Правовые акты общего действия, обеспечивающие информационную безопасность банков методами охранительного содержания.
6. Внутренние нормативные акты. Содержание аудита по информационной безопасности технических средств обработки информации.
7. Организация системы информационной безопасности банка. Субъекты обеспечения информационной безопасности банка.
8. Средства и методы обеспечения информационной безопасности банка.
9. Организация внутреннего контроля банка ее информационная безопасность.
10. Организация службы безопасности банка.
11. Система технических средств безопасности банка.
12. Технические средства охраны.
13. Технические средства охраны банковских операций и продуктов.
14. Информационная безопасность при противодействии хищению денежных средств и совершении кредитных операций.
15. Информационная безопасность при противодействии хищению денежных средств с незаконным использованием пластиковых карт.
16. Информационная безопасность при противодействии хищении денежных средств с использованием аккредитивов.
17. Информационная безопасность при противодействии хищению денежных средств с использованием чеков.
18. Информационная безопасность при противодействии хищению денежных средств с использованием платежных поручений
19. Правовая характеристика векселя. Риски в сфере вексельного обращения. Роль информационной безопасности при этом.
20. Преступления против собственности, в которых вексель является предметом посягательств. Роль информационной безопасности при этом.
21. Преступления против собственности, в которых вексель является средством совершения преступления. Роль информационной безопасности при этом.

22. Меры предупреждения преступлений в сфере вексельного обращения. Роль информационной безопасности при этом.

23. Злоупотребления полномочиями. Коммерческий подкуп. Роль информационной безопасности при этом.

24. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну. Роль информационной безопасности при этом.

25. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка. Роль информационной безопасности при этом.

26. Противоправные посягательства на кадровое обеспечение банка. Противоправные посягательства на нематериальные активы банка. Роль информационной безопасности при этом.

27. Информационная безопасность при легализации (отмывания) доходов, полученных преступным путем.

28. Информационная безопасность и система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма

29. Информация, использующая в целях обеспечения безопасности (информационной безопасности) банка, и ее источники.

30. Бюро кредитных историй.

31. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность (информационную безопасность) банка.

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

Формой контроля знаний по дисциплине «Информационная безопасность кредитно-финансовых операций» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	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

Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-1,2	20-40 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-1,2	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком образовательного процесса	Экзамен	ПК-1,2	2 теоретических вопроса + практическое задание	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 35 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • 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; «**Неудовлетвор и-тельно**»: • 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.

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.

Вариант (Технологии межбанковских электронных расчетов)

1. Что такое система межбанковских расчетов?
2. Какой нормативный срок установлен для проведения расчетов в замках субъекта РФ? А в пределах всей территории РФ?
3. С помощью каких видов счетов могут осуществляться расчеты через КО (филиалы)?
4. В какой очередности осуществляется списание денежных средств при недостаточности средств на счете?
5. Что такое операционный день банка?

6. Как осуществляется обработка платежного документа клиента банка?

7. Какие Вы знаете способы обработки электронных документов банком?

8. Какие Вы знаете способы защиты предупреждения ошибок ввода информации.

9. Перечислите основные параметры функционирования платежных систем?

10. Перечислите ключевые принципы для системно значимых платежных систем.

11. Расскажите о рисках, возникающих в процессе функционирования платежной системы.

12. Каковы основные направления решения проблемы распределению ресурсов, выделенных по корреспондентским счетам, участвующим в системе межбанковских расчетов?

13. Какими двумя способами может происходить исполнение платежей в любой платежной системе?

14. Каково главное достоинство брутто-расчетов?

15. Как решается проблема недостаточности средств при брутто - расчетах?

16. По какой причине в Швейцарии большинство банков не является участниками расчетов в национальной платежной системе?

17. Каким положением Банка России регулируется механизм содержания ликвидности кредитной организации в период временного отсутствия денежных средств в РФ?

18. По какой причине не оправдано развитие филиальной сети в России после кризиса 1998 года?

19. Перечислите известные Вам варианты технологий организации расчетов между филиалами внутри одного банка.

20. Каким образом определяется дата перечисления платежа?

21. Какие договоренности должны быть достигнуты между банком - респондентом и банком-корреспондентом?

22. Каким образом производится учет незавершенных расчетов собственным и транзитным платежам банка?

23. Перечислите наиболее часто используемые подходы при выборе окончательного решения кредитной организации по структуре и характеристикам ее корреспондентской сети.

24. Каковы недостатки действующей в настоящее время платежной системы РФ?

25. Каким образом формируется уникальный идентификатор составителя документа электронного документа?

26. В чем различие и особенности электронного платежного документа сокращенного формата и полноформатного?

27. Какова функция РКЦ (ГРКЦ) при организации расчетов через расчетную сеть Банка России?

28. Какой механизм межрегиональных расчетов в расчетной Банка России?
29. Какие Вы знаете преимущества и недостатки технологии клиринга?
30. Перечислите технологии расчетов между филиалами внутри одного банка.
31. Дайте определение и приведите классификацию клиринга?
32. Перечислите основные цели деятельности клиринговых организаций?
33. Какие операции клиринговых учреждений, обеспечивающие выполнение клиринга или способствующие осуществлению клиринговых взаиморасчетов, Вы знаете?
34. Опишите особенности построения коммуникационной сети которые обеспечивает транспорт сообщений между коммерческими банками и расчетными центрами.
35. Каковы основные функции коммуникационного центра?
36. Опишите схему модулей информационной системы автоматизированного расчетного центра и взаимодействия с коммерческим банком на основе электронной почты.
37. Какими тремя способами может быть организована технология взаимодействия расчетных центров по переводу средств?
38. Какова история появления и развития S.W.I.F.T.?
39. В чем состоят преимущества и недостатки системы S.W.I.F.T.?
40. Когда S.W.I.F.T. появилась в России (СССР)?
41. Какие функции у Российской Национальной Ассоциации ROS-S.W.I.F.T.?
42. Какова схема прохождения платежного поручения клиента в системе S.W.I.F.T.?
43. Что включает в себя стандарт SWIFT-RUR? .
44. По какой причине потребовалось введение стандарта SWIFT-RUR? Укажите текущую версию стандарта.
45. Назовите основные категории сообщений S.W.I.F.T.?
46. Опишите структуру сети S.W.I.F.T.?
47. Какие новые сервисы появились с переходом к SWIFTNet?
48. Перечислите 4 схемы доступа к сети S.W.I.F.T.
49. Какие интерфейсы системы S.W.I.F.T. Вы знаете?

Форма тестов

1. Основные способы незаконного получения банковской тайны.

Тайным;
Открытым;
В виде обмана;
С применением насилия;
Во всех перечисленных случаях.

2. **Основные направления, по которым осуществляется защита кадрового состава банка.**

Ограждение банка от проникновения в его личный состав нежелательных лиц;

Соответствие кадров системе требований;

Во всех перечисленных случаях.

4.2. Типовые вопросы, выносимые на экзамен

1. Технологии управления КБ и иные технологии оказания КБ услуги роль информационной безопасности при их применении.
2. Состав и свойства информационных объектов СБ (системы бюджетирования). Функциональность и алгоритмы СБ и ее информационная безопасность.
3. Информационная безопасность при оказании услуги и выполнении операций в кредитном учреждении.
4. Органические структуры. Управленческие функции и их разделение в банке. Информационное взаимодействие управленческой и аналитической служб. Организационная структура КБ. Подсистема ядра БИС. Роль и место службы информационной безопасности
5. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.
6. Информационная безопасность подсистемы работы с банковскими картами.
7. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.
8. Информационная безопасность подсистемы операций с ценными бумагами.
9. Информационная безопасность подсистема инкассации и подсистемы межбанковского взаимодействия.
10. Информационная безопасность подсистемы управления ресурсами (дилинга).
11. Информационная безопасность в подсистеме обеспечения безопасности.
12. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.
13. Информационная безопасность подсистема удаленного банковского обслуживания.
14. Информационная безопасность подсистема обеспечения внутренней деятельности кредитно-финансовой операции как субъекта экономики.
15. Информационная безопасность системы электронного документооборота банка.
16. Информационная безопасность традиционных технологий расчетов.

17. Информационная безопасность и архитектура системы «Клиент – банк».
18. Информационная безопасность и способы передачи информации до компьютерной сети кредитно-финансовой организации.
19. Информационная безопасность системы телефонного банкинга.
20. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
21. Информационная безопасность модели Интернет - банкинга.
22. Информационная безопасность расчетов банковскими картами в Интернете.
23. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
24. ИБ защищенного информационного обмена при использовании симметричных методов защиты информации.
25. ИБ защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
26. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
27. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.
28. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
29. Информационная безопасность электронных платежей с помощью цифровых денег.
30. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.
31. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.
32. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД) в кредитно-финансовой организации.
33. Информационная безопасность при составлении и направлении ЭД участником – отправителем.
34. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
35. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

**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.*

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КРЕДИТНО-ФИНАНСОВЫХ ОПЕРАЦИЙ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Общие положения

Целью изучения дисциплины является:

1. Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации при проведении кредитно- финансовых операций;
2. Повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
3. Формирование у студентов специализированной базы знаний по основным понятиям в области банковских информационных систем и технологий кредитно- финансовых операций;
4. Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации в банковской сфере (обеспечение электронной коммерции и интернет – расчетов).

Задачи дисциплины:

- Теоретические основы подготовки студентов для самостоятельного решения поставленных задачи в области применения банковских информационных систем и технологий на основе действующего российского законодательства с помощью с помощью современных принципов, методов, сил и средств в различных организационных структурах;
- Практические аспекты формирования подходов обучаемых к выполнению самостоятельных исследований в области защиты информации в кредитно-финансовых организациях по базовым направлениям защиты банковской тайны и конфиденциальной информации;
- Формирование, у обучающихся системы знаний для применения основных методов и средств защиты информации кредитно-финансовых операций инструментов и технологий функциональных и контролирующих подразделений кредитно-финансовой организации.

2. Указания по проведению практических занятий

Тема 1: Информационная безопасность технологий электронных расчетов. Технологии защиты безналичных электронных расчетов на основе систем «Клиент – банк». Технологии защиты безналичных расчетов на основе банковских карт

Практическое занятие 1.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа технологий электронных расчетов.

Основные положения темы занятия:

1. технологии защиты безналичных электронных расчетов на основе систем «Клиент – банк».
2. технологии защиты безналичных электронных расчетов на основе банковских карт.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Информационная безопасность технологий расчетов и их автоматизированные (электронные) формы. Классификация расчетов по субъектам и формам. Структурная схема взаимодействия традиционных и автоматизированных (электронных) форм расчетов. Защита информационных технологий внешних взаимодействий КБ.
2. Назначение и архитектура системы «Клиент – банк». Информационная безопасность передачи информации до компьютерной сети банка. Системы телефонного банкинга. Система «Клиент – банк» на основе технологии «толстого клиента» Понятие и модели Интернет - банкинга. Организация Интернет – банкинга через портал посредника –аутсорсера. Направления удаленного банковского обслуживания и их защита.
3. Информационная безопасность пластиковых карт. Карточные фокусы. Чековые расчеты – основа банковской информационной технологии электронных расчетов. Информационная безопасность карточной платежной системы и схема их работы. Расчеты банковскими картами в Интернете и их информационная безопасность.

Продолжительность занятия – 2/2 ч.

Тема 2: Информационная безопасность при применении средств электронной цифровой подписи в кредитно-финансовых организациях

Практическое занятие 2.

Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:
Цель работы: Получить практические навыки анализа технологий применения ЭП в кредитно-финансовых организациях.

Основные положения темы занятия:

1. технологии защиты с применением ЭП согласно существующего законодательства.
2. технологии защиты с применением ЭП для организации защищенного электронного документооборота в банках.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Место ЭЦП в ряду криптографических механизмов.
2. История возникновения ЭЦП в России.
3. Информационная безопасность при использовании средств ЭЦП в сети межбанковских расчетов.

Продолжительность занятия – 2/2 ч.

Тема 3. Информационная безопасность электронных транзакций
Практическое занятие 3.

Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:
Цель работы: Получить практические навыки анализа электронных транзакций.

Основные положения темы занятия:

1. технологии защиты электронных транзакций в банковской деятельности.
2. криптографические методы защиты информации.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1.Информационная безопасность защищенного информационного обмена при использовании симметричных методов.

2.Информационная безопасность защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.

3.Симметричные алгоритмы шифрования. Схема алгоритма работы сети Фейсталя. Режим электронной кодовой книги.

4.Режим сцепления блоков шифротекста. Режим обратной связи по шифротексту. Режим обратной связи по выходу. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.

Продолжительность занятия – 2/2 ч.

Тема 4: Правовые и организационные основы применения ЭЦП в кредитно-финансовых организациях и оказании региональных электронных услуг

Практическое занятие 4.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа технологий применения ЭП в кредитно-финансовых организациях.

Основные положения темы занятия:

1. технологии защиты электронных транзакций в банковской деятельности.
2. криптографические методы защиты информации в банковской сфере.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
2. Защита электронных транзакций протокол (SSL).
3. Схема работы протокола SET. Управление ключами.
4. Распространение ключей в случае использования только симметричных методов преобразования информации.
5. Распространение ключей в случае использования сертификатов открытых ключей.
6. Информационная безопасность электронных платежей с помощью цифровых денег.

Продолжительность занятия – 2/2 ч.

Тема5: Информационная безопасность автоматизации расчетной функции в кредитно-финансовой организации и принципы построения защищенной электронной платежной системы

Практическое занятие 5.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки в формировании и построении защищенной электронной платежной системы.

Основные положения темы занятия:

1. технологии защиты электронных платежных систем.
2. принципы построения защищенной электронной платежной системыие методы защиты информации в банковской сфере.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1.Расчетная функция банков и ее автоматизация.

2.Схема обработки платежного документа клиентами.

3.Ключевые принципы для системно – значимых платежных систем.

4.Определение количества ресурсов, которые банк будет держать на своих корсчетах.

Продолжительность занятия – 4/2 ч.

Тема 6: Информационная безопасность и правила обмена электронными документами кредитно-финансовой организации и ее клиентами при осуществлении расчетов через расчетную сеть

Практическое занятие 6.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия*.**

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки в формировании и построении защищенной системы электронного документооборота в кредитно-финансовой организации.

Основные положения темы занятия:

1. ознакомиться с основными правилами работы с электронными документами.
2. принципы построения защищенной СОД.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
2. Составление и направление ЭД участником – отправителем. Порядок контроля ЭД, полученных от участников – отправителей.
3. Порядок оформления ЭД, подтверждающих исполнение ЭД участников. Порядок приема к исполнению ЭД участником – получателем.
4. Порядок хранения и уничтожения ЭД.

Продолжительность занятия – 4/2 ч.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Понятия и концепция информационной безопасности банка. Банк как объект противоправных посягательств.**	***Подготовка докладов по темам:*** 1. Информационная безопасность при противодействии хищению денежных средств с незаконным использованием пластиковых карт. 2. Информационная безопасность при противодействии хищении денежных средств с использованием аккредитивов. 3. Информационная безопасность при противодействии хищению денежных средств с использованием чеков. **4.** Информационная безопасность при противодействии хищению денежных средств с использованием платежных поручений
2.	**Внутренние нормативные акты. Содержание аудита по информационной безопасности технических средств обработки информации.**	***Подготовка докладов по темам:*** 1. Правовая характеристика векселя. Риски в сфере вексельного обращения. Роль информационной безопасности при этом. 2. Преступления против собственности, в которых вексель является предметом посягательств. Роль информационной безопасности при этом. 3. Преступления против собственности, в которых вексель является средством совершения преступления. Роль информационной безопасности при этом. 4. Меры предупреждения преступлений в сфере вексельного обращения. Роль информационной безопасности при этом.
3	**Организация внутреннего контроля банка ее информационная безопасность.**	***Подготовка докладов по темам:*** 1. Злоупотребления полномочиями. Коммерческий подкуп. Роль информационной безопасности при этом. 2. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну. Роль информационной безопасности при этом. 3. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка. Роль информационной безопасности при этом.

		4. Противоправные посягательства на кадровое обеспечение банка. Противоправные посягательства на нематериальные активы банка. Роль информационной безопасности при этом.
4	**Информационная безопасность при противодействии хищению денежных средств и совершении кредитных операций.**	***Подготовка докладов по темам:*** 1. Средства и методы обеспечения информационной безопасности банка. 2. Организация внутреннего контроля банка ее информационная безопасность. 3. Организация службы безопасности банка. 4. Система технических средств безопасности банка.

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 анализа заданной электрической цепи и должна содержать промежуточные и окончательные результаты расчетов, а также соответствующие временные или частотные диаграммы, поясняющие работу электрической цепи.

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).

5.4. Примерные тематика контрольных работ

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 подсистема 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 подсистема удаленного банковского обслуживания.
10. Информационная безопасность подсистема обеспечения внутренней деятельности кредитно-финансовой операции 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 кредитно-финансовой организации.
15. Информационная безопасность системы телефонного банкинга.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1.Кибербезопасность в условиях электронного банкинга : практическое пособие / под ред. П. В. Ревенкова. - Москва : Прометей, 2020. - 522 с. - ISBN 978-5-907244-61-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1284190 (дата обращения: 28.11.2022). – Режим доступа: по подписке.

2.Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 28.11.2022). – Режим доступа: по подписке.

Дополнительная литература:

3.Тавасиев, А. М. Банковское кредитование : учебник / А.М. Тавасиев, Т.Ю. Мазурина, В.П. Бычков ; под ред. А.М. Тавасиева. — 2-е изд., перераб. — Москва : ИНФРА-М, 2020. — 366 с. — (Среднее профессиональное

образование). - ISBN 978-5-16-014239-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1039295 (дата обращения: 28.11.2022). – Режим доступа: по подписке.

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.

1. **www.biblioclub.ru** - Универсальная библиотека онлайн.
2. **www.window.edu.ru** - Единое окно доступа.
3. **http://grebennikov.ru/** - Издательский дом «Гребенников»
4. **www.rucont.ru** - ЭБС «Руконт»
5. **http://www.minfin.ru -** Официальный сайт Министерства финансов Российской Федерации
6. **http://www.gov.ru** - Официальный сервер органов государственной власти Российской Федерации.
7. **http://www.fsb.ru** - Официальный сайт Федеральной Службы Безопасности
8. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета
2. Информационно-справочные системы (Консультант+; Гарант).
3. Рабочая программа и методическое обеспечение по курсу: «Информационная безопасность кредитно-финансовых операций»