МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

02.12.2025 г.

протокол № 3

Зав. кафедрой Назаров Д.М.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

16 декабря 2025 г.

протокол № 4

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Защита информации в банковских информационных системах
Направление подготовки	10.03.01 Информационная безопасность
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2026

Разработана:
Ассистент
Кузнецов А.Н.

Профессор, д.э.н.
Назаров Д.М.

Екатеринбург
2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование у студентов компетенций, направленных на изучение теоретических основ и практическое освоение методики обеспечения защиты информации в банковских системах и в кредитно-финансовой сфере России.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточная аттестация	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Лабораторные		
Семестр 6						
Экзамен	180	64	32	32	89	5

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Шифр и наименование компетенции	Индикаторы достижения компетенций
эксплуатационный	

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-1.ПК-3 Знать: Архитектура подсистем защиты информации в операционных системах Принципы построения систем управления базами данных Основные средства и методы анализа программных реализаций Принципы построения антивирусного программного обеспечения Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению Уязвимости используемого программного обеспечения и методы их эксплуатации Виды и формы функционирования вредоносного программного обеспечения Характерные признаки наличия вредоносного программного обеспечения Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения Принципы функционирования программных средств криптографической защиты информации Порядок обеспечения безопасности информации при эксплуатации программного обеспечения Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации
	ИД-2.ПК-3 Уметь: Анализировать угрозы безопасности информации программного обеспечения Формулировать правила безопасной эксплуатации программного обеспечения Обосновывать правила безопасной эксплуатации программного обеспечения Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-3.ПК-3 Иметь практический опыт: Определение порядка установки программного обеспечения с целью соблюдения требований по защите информации Контроль над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение Формулирование требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения Выполнение работ по обнаружению вредоносного программного обеспечения Ликвидация обнаруженного вредоносного программного обеспечения и последствий его функционирования Формулирование требований к встроенным средствам защиты информации программного обеспечения

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 6		24					
Тема 1.	Требования к информационной безопасности банка	24	4	2		18	
Семестр 6		25					
Тема 2.	Общие принципы защиты информации в банковских информационных системах	25	4	2		19	
Семестр 6		12					
Тема 3.	Автоматизация банковских операций и их защита	12	6	6			
Семестр 6		14					
Тема 4.	Методы защиты информации в автоматизированных системах обработки данных. Криптографические технологии защиты информации. ЭЦП. Полиграфические и голографические методы защиты от фальсификации документов и ценных бумаг	14	6	8			
Семестр 6		30					
Тема 5.	Автоматизация валютных операций	30	6	2		22	
Семестр 6		12					
Тема 6.	Защита информации при выполнении электронных платежей	12	6	6			
Семестр 6		36					
Тема 7.	Реализация технологий цифровой подписи, цифрового конверта, цифрового сейфа	36		6		30	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Тема 3	Тест (Приложение 4)	Тест состоит из 10 вопросов с вариантами ответов	1-10 баллов
Тема 2	Тест (Приложение 4)	Тест состоит из 10 вопросов с вариантами ответов	1-10 баллов
Тема 1	Тест (Приложение 4)	Тест состоит из 10 вопросов с вариантами ответов	1-10 баллов
Промежуточная аттестация(Приложение 5)			
6 семестр (Эк)	Экзаменационный билет (приложение 5)	27 билетов. 2 теоретических вопроса и 1 практическое задание	1-100 баллов

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущего контроля и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущий контроль.Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущего контроля, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения профессиональных задач
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Требования к информационной безопасности банка Роли и обязанности должностных лиц по проведению политики безопасности. Аудит информационной безопасности. Нормы и стандарты информационной безопасности на предприятии
Тема 2. Общие принципы защиты информации в банковских информационных системах Защита банковской информации. Несанкционированный доступ. Федеральный закон о деятельности банков. Защита от физического доступа. Защита резервных копий. Защита от инсайдеров
Тема 3. Автоматизация банковских операций и их защита Автоматизация банковских операций и их защита. Необходимость защиты банковских систем: тенденции и факты. Угрозы безопасности автоматизированных банковских систем. Особенности защиты информации в электронных банковских системах
Тема 4. Методы защиты информации в автоматизированных системах обработки данных. Криптографические технологии защиты информации. ЭЦП. Полиграфические и голографические методы защиты от фальсификации документов и ценных бумаг ЭЦП. Криптография. Голография. Принцип голографии. Полиграфические средства защиты
Тема 5. Автоматизация валютных операций Нормативная база защиты информации в финансово-кредитной сфере. Принципы политики безопасности
Тема 6. Защита информации при выполнении электронных платежей Понятие электронной платежной системы. Безопасность в электронных платежных системах. Электронные пластиковые карты

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Общие принципы защиты информации в банковских информационных системах Объекты защиты коммерческого банка. Государственные акты и стандарты защиты информации. Функции системы имитационного моделирования по управлению предприятием в условиях рыночной экономики
Тема 3. Автоматизация банковских операций и их защита 1. Банковские операции и их защита 2. Объекты и назначение средств программной защиты

Тема 4. Методы защиты информации в автоматизированных системах обработки данных. Криптографические технологии защиты информации. ЭЦП. Полиграфические и голографические методы защиты от фальсификации документов и ценных бумаг

1. Подпись документов при помощи симметричных криптосистем
2. Хэш-функция
3. Хранение ключей
4. Распределение ключей
5. Стандарты криптографии
6. Требования пользователей
7. Атаки на цифровую подпись
8. Атаки на алгоритмы
9. Атаки на криптосистему
10. Атаки на реализацию
11. Атаки на пользователей
12. Электронные цифровые подписи
13. Алгоритмы электронной цифровой подписи
14. "КриптоБанк"
15. Юридические аспекты использования технологии для контроля подлинности документов

Тема 5. Автоматизация валютных операций

Нормативные акты Банка России

Тема 6. Защита информации при выполнении электронных платежей

1. Кодирование магнитной полосы пластиковой карты
2. Программирование микросхемы

Тема 7. Реализация технологий цифровой подписи, цифрового конверта, цифрового сейфа

1. Цифровая подпись "Нотариус".
2. Цифровой конверт "Веста".
3. Криптосейф

7.3. Содержание самостоятельной работы

Тема 2. Общие принципы защиты информации в банковских информационных системах
Изучение понятийного аппарата темы, методического материала, глав рекомендованных учебников и дополнительных источников

Тема 5. Автоматизация валютных операций
Изучение понятийного аппарата темы, методического материала, глав рекомендованных учебников и дополнительных источников

Тема 7. Реализация технологий цифровой подписи, цифрового конверта, цифрового сейфа
Изучение понятийного аппарата темы, методического материала, глав рекомендованных учебников и дополнительных источников

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
Не предусмотрено

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
Материалы не предусмотрены

7.6 Методические рекомендации по выполнению курсовой работы
Материалы не предусмотрены

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

2. Щеглов А. Ю., Щеглов К. А. Защита информации: основы теории [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2024. - 309 – Режим доступа: https://urait.ru/bcode/537000

3. Внуков А. А. Защита информации в банковских системах [Электронный ресурс]:учебное пособие для вузов. - Москва: Юрайт, 2024. - 246 – Режим доступа: https://urait.ru/bcode/537248

Дополнительная литература:

2. Верещагина Е.А., Золкин А.Л., Фролов А.В. Исследование проблем информационной безопасности в банковской сфере [Электронный ресурс]:Монография. - Москва: Русайнс, 2023. - 177 – Режим доступа: https://book.ru/book/950915

3. Полякова Т. А., Чубукова С. Г., Ниесов В. А., Стрельцов А. А. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2024. - 357 – Режим доступа: https://urait.ru/bcode/555950

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Astra Linux Common Edition. Договор №0417-ПО/2019 от 08.05.2019, Акт №Sk000343 от 24.05.2019 и Контракт № 35-У/2018 от 13.06.2018, Акт № УТ213 от 17.12.2018. Срок действия лицензии - без ограничения срока.

Libre Office. Лицензия GNU LGPL. Срок действия лицензии - без ограничения срока.

Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии -Без ограничения срока.

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии -Без ограничения срока.

Microsoft Visual Studio Community. Лицензия для образовательных учреждений. Срок действия лицензии - без ограничения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

Справочно-правовая система Консультант +. Договор № 143/223-У/2025 от 02.12.2025 Срок действия лицензии до 31.12.2026

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.

Приложение 1
к рабочей программе

7.3.1. Примерные вопросы для самостоятельной подготовки к экзамену

1. Банковская система Российской Федерации и банковские операции. Каковы основные отличия банков от других организаций, осуществляющих свою деятельность в экономике?
2. Организация и функционирование банковской системы России. Законы РФ, определяющие построение банковской системы и регламентирующие банковскую деятельность. Этапы эволюции информационных систем.
3. Иерархия банковской системы России. Центральный банк России (ЦБ РФ). Функции, выполняемые ЦБ РФ. История развития банковских информационных систем.
4. Кредитные организации. Банки и небанковские кредитные организации. Операции и сделки, осуществляемые коммерческими банками. Опишите основные мировые тенденции развития банковского дела. Какие из них привели к росту значения информационных технологий для банков?
5. Структура банка как коммерческого предприятия. Бухгалтерия банка. Специфика банковских информационных систем
6. Что представляет собой банковская информационная система? Перечислите свойства банковской информационной системы.
7. Приведите основные характеристики информационных систем «Клиент-банк» и «Телебанк». В чем преимущество архитектуры построения БИС «Клиент-сервер»?
8. Назовите основные цели и функции применения в банке электронного документооборота.
9. Перечислите основные виды электронных услуг банков. Охарактеризуйте электронные услуги с использованием банковских карт.
10. Состав и структура базы данных БИС. Первичные документы. Отчетные документы. Справочники. Лицевые счета.
11. Учетные регистры. Назначение и типы счетов. План счетов коммерческого банка. План счетов ЦБ РФ.
12. Реквизиты и кодовое обозначение лицевого счета. Порядок регистрации счетов аналитического учета.
13. Особенности синтетического учета в банках.
14. Расчеты платежными поручениями. Расчеты платежными требованиями. Расчеты чеками.
15. Общее понятие о безналичных расчетах. Основные принципы безналичных расчетов. Формы безналичных расчетов.
16. Раскройте понятие дистанционного банковского обслуживания. Опишите основные преимущества использования ДБО для клиента и банка.
17. Сравните два способа осуществления межбанковских расчетов: на валовой основе и клиринга; назовите основные преимущества и недостатки каждого способа.
18. В чем состоят особенности межбанковского взаимодействия? Приведите примеры и охарактеризуйте наиболее распространенные системы межбанковских расчетов (SWIFT, RTGS).
19. Сформулируйте понятие информационных потоков. Перечислите характеристики информационных потоков. Сформулируйте определение системы управления информационными потоками.
20. Перечислите этапы реализации проекта создания банковской информационной системы. Какие передовые информационные технологии используются в банковской деятельности?
21. Сформулируйте определение системы оперативного управления наличностью денежной массы.

22. Дайте определение OLTP-системы.
23. Дайте определение технологии информационных хранилищ Data Warehouse.
24. В чем состоит назначение приложений аналитической обработки OLAP?
25. Перечислите направления автоматизации банков.
26. Какие инструментальные программные средства используются для проектирования, управления и поддержания баз данных? Назовите наиболее распространенные в России СУБД. Чем объясняется лидирующее место СУБД Oracle?
27. Какие требования предъявляются к информационному обеспечению банковских систем?
28. Дайте определение базового программного обеспечения банковских систем.
29. Дайте определение прикладного программного обеспечения банковских систем.
30. Какие требования предъявляются к программному обеспечению банковских систем?
31. Перечислите зарубежные компании, разрабатывающие банковские платформы. Назовите основных российских разработчиков банковских автоматизированных систем.
32. На какие классы можно разделить программные средства, используемые в качестве инструментария при решении задач финансового и инвестиционного менеджмента?
33. Какими программными продуктами представлены на отечественном и мировом рынках программные средства для анализа инвестиционных проектов?
34. Какие программы статистического анализа получили наибольшее распространение на российском рынке?
35. Какие программы математического анализа получили наибольшее распространение на российском рынке?
36. Какие программы для решения задач линейного программирования наиболее популярны на отечественном рынке?
37. Перечислите технологии искусственного интеллекта, использующиеся в финансово-кредитной сфере.
38. В каких областях финансового и инвестиционного менеджмента получили широкое применение нейронные сети?
39. Назовите наиболее популярные продукты, реализующие алгоритмы генетической оптимизации.
40. Назовите наиболее известные программные продукты, реализующие методы нечеткой логики.
41. В каких областях банковской деятельности можно применять экспертные системы?
42. В каких направлениях развиваются системы банковских электронных расчетов в условиях новых информационных технологий?
43. Дайте понятие Интернет-банкинга.
44. Как банк может проверить, что лицо, звонящее в отдел обслуживания клиентов, действительно является законным держателем карты? Как выполняется идентификация вне банка при работе с устройствами самообслуживания?
45. Дайте определение авторизации и персонализации. Что такое «ПИН-код»?
46. Сравните магнитные и смарт-карты. Обоснуйте тезис повышенной защищенности смарт-карты. Проанализируйте схемы обработки магнитной и смарт-карты. В чем сходство и различие этих схем? Какая из схем, на ваш взгляд, является более предпочтительной и почему?
47. Какие виды карт используются в банковской деятельности? Дайте им сравнительную характеристику. Какой вид карт более перспективен в России?
48. Какие карты являются «ключом к счету», а какие «электронным кошельком»? Обоснуйте ответ. Какие варианты «электронных кошельков» существуют? Проанализируйте преимущества и недостатки каждой из схем с позиций банка и клиента.
49. Назовите три особенности, которыми кредит по банковской карте отличается от обычного потребительского кредита.
50. Перечислите основные способы мошенничества с банковскими картами.

51. Опишите процедуру оплаты покупки кредитной картой. Объясните суть, назначение и особенности выполнения каждого действия продавца.
52. Какие существуют преимущества и недостатки применения кредитных карт для каждой стороны, участвующей в расчетах? Поясните примерами. В каком случае применение кредитных карт будет наиболее выгодным для банка?
53. Какие банковские услуги может получить держатель банковской карты? Докажите, что с позиций банка это разные услуги.
54. Дайте определение платежной системы. Назовите платежные системы, функционирующие на основе сетевых (цифровых) денег. Назовите российские платежные системы, функционирующие на основе банковских карт.

Приложение 2
к рабочей программе

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к экзамену

Номер задания	Содержание вопроса
1.	Потенциальные угрозы, против которых направлены технические меры защиты информации a) Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей b) Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения c) Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками. d) Потери информации из-за не достаточной установки сигнализации в помещении. ***e)*** Процессы преобразования, при котором информация удаляется
2.	Из приведенного ниже списка выделите виды аудита информационной безопасности a) активный аудит (внутренний и внешний); b) экспертный аудит; c) аудит на соответствие стандартам информационной безопасности; d) финансовый аудит; e) аудит на соответствие стандартам менеджмента и качества.
3.	Государственную тайну составляют, сведения в области внешней политики и экономики: a) сведения о банках, в которых содержатся счета организации; b) о сотрудничестве с иностранными организациями; c) обобщенные показатели по внешней задолженности; d) о финансовой политике в отношении иностранных государств.
4.	Какой вариант в полном объеме характеризует понятие угрозы безопасности информации? a) понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и
	аппаратных средств. b) потенциально возможное событие, процесс или явление, которое может (воздействуя на что-либо) привести к нанесению ущерба чьим-либо интересам. c) возможность реализации воздействия на информацию, обрабатываемую в АИС, приводящего к нарушению конфиденциальности, целостности или доступности этой информации, а также возможность воздействия на компоненты АИС, приводящего к их утрате, уничтожению или сбою функционирования. d) потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию, ее носители и процессы обработки может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

5.	Какие пункты включает в себя план проведения аудита информационной безопасности a) цель аудита информационной безопасности; b) критерии аудита информационной безопасности и ссылочные документы; c) область аудита информационной безопасности; d) дату и продолжительность проведения аудита информационной безопасности на месте; e) роли членов аудиторской группы и сопровождающих лиц со стороны проверяемой организации; f) результаты анализа документов, предоставленных проверяемой организацией для проведения аудита информационной безопасности, и оценку свидетельств аудита информационной безопасности; g) описание деятельности и мероприятий по проведению аудита информационной безопасности на месте; h) методика оценивания рисков информационной системы; i) методы оценки угроз и уязвимостей информационной системы; j) роли руководящего состава организации; методика оценки угроз.
6.	Оценка рисков позволяет ответить на следующие вопросы: a) чем рискует организация, используя информационную систему? b) чем рискуют пользователи информационной системы? c) Чем рискуют системные администраторы?
7.	Целью проведения аудита информационной безопасности является a) оценка состояния информационной безопасности организации, ее информационной системы, и разработка рекомендаций по применению комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных и иных ресурсов b) оценка состояния информационной c) безопасности организации, ее информационной системы, и разработка рекомендаций по проектированию комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных и иных ресурсов.
8.	Из приведенного ниже списка выделите виды аудита информационной безопасности a) активный аудит (внутренний и внешний); b) экспертный аудит; c) аудит на соответствие стандартам информационной безопасности; d) финансовый аудит; e) аудит на соответствие стандартам менеджмента и качества.
9.	Разработка и внедрение новых информационно-вычислительных систем, в рамках которых решается весь комплекс проблем защиты информации это a) креативный подход; b) аддитивный подход; c) интеграционный подход
10.	Наиболее важным при реализации защитных мер политики безопасности является: a) Аудит, анализ затрат на проведение защитных мер b) Аудит, анализ безопасности c) Аудит, анализ уязвимостей, риск-ситуаций

11.	Для чего проводят технико-экономическое обоснование средств защиты? Для … (в родительном падеже) (Ответ: для анализа и оценки целесообразности реализации применяемых средств)
12.	Для усовершенствования собственных процессов и систем, их соответствия требованиям и определения пригодности процессов и систем одной организации для другой на договорной основе - необходим a) контроль и проверка процессов систем организации; b) контроль и проверка финансового состояния организации; c) контроль и проверка процессов систем пожарной сигнализации.
13.	Виды информационной безопасности: a) персональная, корпоративная, государственная; b) клиентская, серверная, сетевая; c) локальная, глобальная, смешанная
14.	Из приведенного ниже списка выделите задачи мониторинга a) прогнозирование; b) разработка приемов и способов приведения объекта мониторинга в оптимальное состояние; c) проектирование; d) аудит информационной безопасности; e) сбор фактического материала, результатом которого является получение определенной информации о данном объекте; f) оценивание; g) контроль.
15.	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству: a) снизить уровень классификации этой информации; b) улучшить контроль за безопасностью этой информации; c) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации.
16.	Задача оценки эффективности КСЗИ может разбиваться на следующие частные задачи: a) Оценки эффективности защиты от сбоев и отказов аппаратных и программных средств; b) Оценки эффективности защиты от НСДИ; c) Оценки эффективности защиты от ПЭМИН; d) Оценки способности персонала соблюдать политику информационной безопасности
17.	Какие свойства информации выполняет резервное копирование? a) конфиденциальность; b) целостность; c) доступность.
18.	Основы кредитно-банковской системы России
19.	Платежная система и межбанковские расчеты
20.	Традиционная и электронная коммерции. Виды электронной коммерции.
21.	Типы дематериализованных денег. Электронные кошельки
22.	Факторы, влияющие на безопасность в банковской сфере.
23.	Классификация угроз.
24.	Состав и структура системы безопасности банка.
25.	Понятие и модели политики безопасности.

26.	Механизмы защиты.
27.	Принципы организации и контроля функционирования автоматизированных сетей.
28.	Опасные события и их предупреждение.
29.	Устранение нарушений. Дополнительные меры контроля.
30.	Обмен электронными данными. Торговые расчеты. Межбанковские расчеты. Основные способы межбанковских платежей.
31.	Общие проблемы безопасности электронного обмена данных.
32.	Классификация типов мошенничества в электронной коммерции. 2.Протокол SSL.
33.	Система сообщества всемирных межбанковских финансовых телекоммуникаций
34.	(SWIFT).
35.	Клиринговая система CHAPS.