

Государственное бюджетное профессиональное образовательное учреждение  
«Южно-Уральский государственный колледж»

## РАССМОТРЕНО

Председатель ПЦК Финансовых дисциплин

Пылина И.В.

\_\_\_\_\_ / \_\_\_\_\_  
подпись председателя ПЭК

«08» июня 2023г

**Комплект контрольно-измерительных материалов**  
по учебной дисциплине ОП.12. Безопасность банковской деятельности  
Образовательной программы по специальности СПО  
38.02.07 Банковское дело  
Квалификация: специалист банковского дела

Челябинск, 2023

ГБПОУ «ЮУГК»

Разработчик:  
преподаватель

Степанова Ю.А.

Эксперты:

АО ОТП Банк

Управляющий  
Филиал  
Челябинский

Байгузина А.И.

## СОДЕРЖАНИЕ

1. Общие положения	4
2. Комплект КИМ для текущего контроля	9
3. Комплект КИМ для промежуточной аттестации	33
Приложение 1	36

# 1. Общие положения

## Комплект контрольно-измерительных материалов (КИМ) по дисциплине ОП.12 Безопасность банковской деятельности

образовательной программы по профессии (или специальности) СПО

### 38.02.07 Банковское дело

содержит КИМ для текущего контроля и КИМ для промежуточной аттестации, которые позволяют оценивать сформированность общих и профессиональных компетенций в соответствии с установленными показателями (спецификация).

**Спецификация сформированности общих компетенций**, освоение которых подтверждается действиями обучающегося при текущем контроле и на промежуточной аттестации:

Таблица 1

ОК	Дескрипторы (показатели сформированности)	Код	Умения	Код	Знания	Код
ОК.01	1.Распознавание задачи и проблемы	ОД.01-1	1. распознавать задачу и/или проблему в профессиональном и/или социальном контексте	ОУ.01-1	1. актуальный профессиональный и социальный контекст, в котором приходится работать и жить;	ОЗ.01-1
	2.Анализ задачи и проблемы, поиск необходимой информации	ОД.01-2	2. анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы	ОУ.01-2	2. основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте	ОЗ.01-2
	3.Составление плана действий, определение ресурсов	ОД.01-3	3. составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий	ОУ.01-3	3. алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности	ОЗ.01-3
ОК.02	1.Определение задачи для поиска информации	ОД.02-1	1. определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска	ОУ.02-1	1. номенклатура информационных источников применяемых в профессиональной деятельности	ОЗ.02-1
	2.Структурирование и оценивание информации	ОД.02-2	2. структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска	ОУ.02-2	2. приемы структурирования информации;	ОЗ.02-2
	3.Оформление результатов поиска	ОД.02-3	3. оформлять результаты поиска	ОУ.02-3	3. формат оформления результатов поиска информации	ОЗ.02-3
ОК.03	1.Определение актуальности	ОД.03-1	1. определять актуальность нормативно-	ОУ.03-1	1. содержание актуальной	ОЗ.03-1

	нормативно-правовой документации		правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию;		нормативно-правовой документации; современная научная и профессиональная терминология	
	2. Выстраивание траектории профессионального развития	ОД.03-2	2. определять и выстраивать траектории профессионального развития и самообразования	ОУ.03-2	2. возможные траектории профессионального развития и самообразования	ОЗ.03-2
ОК.04	1. Организовывание работы коллектива	ОД.04-1	1. организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	ОУ.04-1	1. психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности	ОЗ.04-1
ОК.05	1. Описание значимости своей специальности	ОД.05-1	1. описывать значимость своей специальности	ОУ.05-1	1. сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности	ОЗ.05-1
	2. Применение стандартов антикоррупционного поведения	ОД.05-2	2. применять стандарты антикоррупционного поведения	ОУ.05-2	2. стандарты антикоррупционного поведения и последствия его нарушения	ОЗ.05-2
ОК.09	1. Применение средств информационных технологий	ОД.09-1	1. применять средства информационных технологий для решения профессиональных задач	ОУ.09-1	1. современные средства и устройства информатизации	ОЗ.09-1
	2. Использование современного программного обеспечения	ОД.09-2	2. использовать современное программное обеспечение	ОУ.09-2	2. порядок их применения и программное обеспечение в профессиональной деятельности	ОЗ.09-2
ОК.10	1. Понимание общего смысла высказываний о себе	ОД.10-1	1. понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы	ОУ.10-1	1. правила построения простых и сложных предложений на профессиональные темы;	ОЗ.10-1
	2. Участие в диалогах	ОД.10-2	2. участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связанные сообщения на знакомые или интересующие профессиональные темы	ОУ.10-2	2. основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности	ОЗ.10-2
ОК.11	1. Выявление достоинств и	ОД.11-1	1. выявлять достоинства и недостатки коммерческой	ОУ.11-1	1. основы предпринимательской	ОЗ.11-1

	недостатков коммерческой идеи, оформление бизнес-плана		идеи; презентовать идеи открытия собственного дела в профессиональной деятельности; оформлять бизнес-план; рассчитывать размеры выплат по процентным ставкам кредитования		деятельности; основы финансовой грамотности	
	2.Выявление инвестиционной привлекательности коммерческой идеи	ОД.11-2	2. инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; презентовать бизнес-идею; определять источники финансирования	ОУ.11-2	2. правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты	ОЗ.11-2

**Спецификация профессиональных компетенций, освоение которых подтверждается действиями обучающегося при текущем контроле и на промежуточной аттестации:**

Таблица 2

Формируемые компетенции	Действия	Код	Умения	Код	Знания	Код
ПК.1.1.	1.Оформление, заполнение документов	ПД1.1-1	1. -оформлять договоры банковского счета с клиентами; -проверять правильность и полноту оформления расчетных документов; -открывать и закрывать лицевые счета в валюте Российской Федерации и иностранной валюте; -выявлять возможность оплаты расчетных документов исходя из состояния расчетного счета клиента, вести картотеку неоплаченных расчетных документов; оформлять выписки из лицевых счетов клиентов; -рассчитывать и взыскивать суммы вознаграждения за расчетное обслуживание; -рассчитывать прогноз кассовых оборотов; -составлять	ПУ1.1-1	1. содержание и порядок формирования юридических дел клиентов; -порядок открытия и закрытия лицевых счетов клиентов в валюте Российской Федерации и иностранной валюте; -правила совершения операций по расчетным счетам, очередность списания денежных средств; -порядок оформления, представления, отзыва и возврата расчетных документов; -порядок планирования операций с наличностью; -порядок лимитирования остатков денежной наличности в кассах клиентов; -типичные нарушения при совершении расчетных операций по счетам клиентов	ПЗ1.1-1

			<p>календарь выдачи наличных денег;  -рассчитывать минимальный остаток денежной наличности в кассе;  составлять отчет о наличном денежном обороте;  -устанавливать лимит остатков денежной наличности в кассах клиентов;  -отражать в учете операции по расчетным счетам клиентов;  -исполнять и оформлять операции по возврату сумм, неправильно зачисленных на счета клиентов;  -использовать специализированное программное обеспечение для расчетного обслуживания клиентов</p>			
ПК.1.6.	1. Оформление платёжных карт; оформление документов на получение платёжных карт	ПД1.6-1	<p>1. -консультировать клиентов по вопросам открытия банковских счетов, расчетным операциям, с использованием различных видов платежных карт;  -оформлять выдачу клиентам платежных карт;  -оформлять и отражать в учете расчетные и налично-денежные операции при использовании платежных карт в валюте Российской Федерации и иностранной валюте;  использовать специализированное программное обеспечение совершения операций с платежными картами</p>	ПУ1.6-1	<p>1. виды платежных карт и операции, проводимые с их использованием; условия и порядок выдачи платежных карт;  технологии и порядок учета расчетов с использованием платежных карт, документальное оформление операций с платежными картами;  типичные нарушения при совершении операций с платежными картами</p>	ПЗ1.6-1

**Перечень учебных изданий,  
дополнительной литературы, Интернет-ресурсов**

Основные источники:

1. Партыка Л.П. Информационная безопасность. – СПб.: Питер, 2020.
2. Ярочкин В.И. Безопасность банковских систем. – М.: Ось-89, 2020.
3. Ярочкин В.И. Теория безопасности. – М.: Академический проект, 2020.

Дополнительные источники:

4. Ваксян А. Анатомия мошенничества. – М.: 2020.
5. Зежвда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2020.

Интернет источники:

1. Консультант +



## **2. Комплект КИМ для текущего контроля**

Текущий контроль освоения студентами материала дисциплины (или междисциплинарного курса) состоит из следующих видов: *оперативный и рубежный контроль*.

При проведении текущего контроля используются следующие формы:

### **1) Практическое задание**

*(перечисление применяемых форм контроля (например, аудиторная контрольная работа; письменное тестирование; фронтальный опрос; терминологический диктант; практическое задание; реферативное задание – выполнение и защита реферата; проектное или исследовательское задание; создание и защита электронной презентации; далее необходимо описать, как будут применены перечисленные формы контроля, каким документом студенту нужно руководствоваться при выполнении определенной работы, включая время на ее выполнение)*

**КИМ №1**  
**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ практического задания**

Раздел 1		Характеристика угроз безопасности банка	
Тема 1.2.		Наиболее характерные преступления, совершаемые в банковской сфере	
Раздел 2		Защита конфиденциальной банковской информации	
Тема 2.1.		Правовые основы защиты конфиденциальности банковской информации	
Раздел 3		Защита банковской информации в автоматизированных системах обработки	
Тема 3.1.		Классификация угроз утечки информации при автоматизированной обработке	
Тема 3.2.		Виды и источники утечки банковской информации по техническим каналам	
Форма контроля		Выполнение практического задания	
Вид контроля			
Спецификация ПК (Указываются коды профессиональных компетенций и коды их структурных элементов (действий, умений, знаний), которые проверяются данным КИМом)	ПК 1.1	ПД1.1-1, ПУ1.1-1, ПЗ1.1-1	
	ПК 1.6	ПД1.6-1, ПУ1.1-1, ПЗ1.1-1	
Спецификация ОК (Указываются коды общих компетенций и коды их структурных элементов (дескрипторов, умений, знаний), которые проверяются данным КИМом)	ОК01	ОД.01-1, ОД.01-2, ОД.01-3, ОУ.01-1, ОУ.01-2, ОУ.01-3, ОЗ.01-1, ОЗ.01-2, ОЗ.01-3	
	ОК02	ОД.02-1, ОД.02-2, ОД.02-3, ОУ.02-1, ОУ.02-2, ОУ.02-3, ОЗ.02-1, ОЗ.02-2, ОЗ.02-3	
	ОК03	ОД.03-1, ОД.03-2, ОУ.03-1, ОУ.03-2, ОЗ.03-1, ОЗ.03-2	
	ОК04	ОД.04-1, ОУ.04-1, ОЗ.04-1	
	ОК05	ОД.05-1, ОД.05-2, ОУ.05-1, ОУ.05-2, ОЗ.05-1, ОЗ.05-2	
	ОК09	ОД.09-1, ОД.09-2, ОУ.09-1, ОУ.09-2, ОЗ.09-1, ОЗ.09-2	
	ОК10	ОД.10-1, ОД.10-2, ОУ.10-1, ОУ.10-2, ОЗ.10-1, ОЗ.10-2	
	ОК11	ОД.11-1, ОД.11-2, ОУ.11-1, ОУ.11-2, ОЗ.11-1, ОЗ.11-2	
Условия выполнения задания		Практическое задание выполняется в аудитории, время проведения работы 90 минут	
Инструкция для студентов		Для выполнения практического задания необходимо использовать Практикум по дисциплине «Безопасность банковской деятельности», а также материалы лекции, Интернета	
Оборудование и оснащение		Для проведения работы применяется следующее оснащение: – оборудование: компьютер	
Источники		<u>Основные источники:</u> 1.Партыка Л.П. Информационная безопасность. – СПб.: Питер, 2020. 2.Ярочкин В.И. Безопасность банковских систем. – М.: Ось-89, 2020. 3.Ярочкин В.И. Теория безопасности. – М.: Академический проект, 2020. <u>Дополнительные источники:</u> 4.Ваксян А. Анатомия мошенничества. – М.: 2020. 5.Зежвда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2020. <u>Интернет источники:</u> 1.Консультант +	

<p><b>Вариант № 1</b> Наиболее характерные преступления, совершаемые в банковской сфере</p>	<p><b>Задание 1.1:</b> Ответьте на вопросы:</p> <ol style="list-style-type: none"> <li>1.Что такое преступление?</li> <li>2.Назовите 4 вида экономических преступлений.</li> <li>3.Дайте определение мошенничества.</li> <li>4.При каких операциях совершаются мошеннические действия на финансовом рынке России? (перечислите 5).</li> <li>5. Назовите факторы мошенничества</li> <li>6.Что такое лжепредпринимательство?</li> <li>7. С чем связано злоупотребление депозитным капиталом?</li> <li>8.Перечислите другие преступления совершаемые в банковской сфере.</li> <li>9.Внутренние злоумышленники – это?</li> <li>10.На какие классы могут быть разделены злоумышленники по степени подготовки и оснащенности?</li> </ol> <p><b>Задание 2.1:</b> Ответьте на тестовые вопросы:</p> <p><b>1.Одно из преступлений против собственности, одна из ненасильственных форм хищения, представляет собой завладение чужим имуществом путем обмана либо злоупотребления доверием – это?</b></p> <ol style="list-style-type: none"> <li>A) Мошенничество</li> <li>B) Кража</li> <li>C) Разбой</li> <li>D) Нападение</li> </ol> <p><b>2.Преступник (или группа), находящийся вне объекта охраны, целью которого является проникновение на объект для хищения ценностей или информации – это?</b></p> <ol style="list-style-type: none"> <li>A) Внутренний злоумышленник</li> <li>B) Внешний злоумышленник</li> <li>C) Хулиган</li> <li>D) Убийца</li> </ol> <p><b>3.Служащий банка или сотрудник охраны, имеющий доступ на объект, располагающий определенной информацией о режиме работы банка и, может быть, системе охраны – это?</b></p> <ol style="list-style-type: none"> <li>A) Преступник</li> <li>B) Хулиган</li> <li>C) Внешний злоумышленник</li> <li>D) Внутренний злоумышленник</li> </ol> <p><b>4.Неосведомленный злоумышленник, как правило, невооруженный и без специального оснащения человек, пытающийся проникнуть в помещение банка без определенного плана действий.</b></p> <ol style="list-style-type: none"> <li>A) Случайный</li> <li>B) Одиночный</li> <li>C) Высококвалифицированный</li> <li>D) Опытный</li> </ol> <p><b>5.... - это общественно опасное деяние (действие или бездействие), посягающее на личность, общество и государство, а также на иные охраняемые законом объекты.</b></p> <ol style="list-style-type: none"> <li>A) Угроза</li> <li>B) Насилие</li> <li>C) Преступление</li> <li>D) Разбой</li> </ol> <p><b>Задание 2.2:</b> Соотнесите термины с их определениями:</p>	
	<p><b>1.Мошенничество</b></p>	<p>A)преступник (или группа), находящийся вне объекта охраны, целью которого является проникновение на объект для хищения ценностей</p>

			или информации.	
		<b>2.Внешний злоумышленник</b>	Б)общественно опасное деяние (действие или бездействие), посягающее на личность, общество и государство, а также на иные охраняемые законом объекты.	
		<b>3.Внутренний злоумышленник</b>	В)одно из преступлений против собственности, одна из ненасильственных форм хищения, представляет собой завладение чужим имуществом путем обмана либо злоупотребления доверием.	
		<b>4.Преступление</b>	Г)служащий банка или сотрудник охраны, имеющий доступ на объект, располагающий определенной информацией о режиме работы банка и, может быть, системе охраны.	
		<b>5.Лжепредпринимательство</b>	Д)создание коммерческой организации без намерения осуществлять предпринимательскую или банковскую деятельность, имеющее целью получение кредитов, освобождение от налогов, извлечение иной имущественной выгоды или прикрытие запрещенной деятельности, причинившее крупный ущерб.	
<b>Вариант №2</b> Правовые основы защиты конфиденциальности банковской информации		<b>Задание 3.1:</b> Согласно Федеральному Закону «О банках и банковской деятельности», №395-1, от 2.12.1990 года (с изменениями и дополнениями), ответьте на вопросы: <ol style="list-style-type: none"> <li>1. Банк – это...</li> <li>2. Иностранный банк – это...</li> <li>3. Банковской группой признается...</li> <li>4. К банковским операциям относятся:</li> <li>5. Кредитная организация обязана раскрывать по <a href="#">формам</a>, в порядке и <a href="#">сроки</a>, которые устанавливаются Банком России, следующую информацию о своей деятельности...</li> <li>6. Устав кредитной организации должен содержать...</li> <li>7. Уставный капитал кредитной организации составляется из...</li> <li>8. Минимальный размер уставного капитала на день подачи ходатайства о государственной регистрации и выдаче лицензии на осуществление банковских операций устанавливается в сумме...</li> <li>9. Минимальный размер собственных средств (капитала) с 1 января 2018 года устанавливается в сумме...</li> <li>10. Размер собственных средств (капитала) небанковской кредитной организации, ходатайствующей о получении статуса должен составлять...</li> <li>11. Минимальный размер собственных средств (капитала) устанавливается для небанковской кредитной организации - центрального контрагента в размере...</li> </ol>		

	<p>12. Кредитные организации подлежат государственной регистрации в соответствии с каким Федеральным <a href="#">законом</a>?</p> <p>13. В целях настоящего Федерального закона под квотой понимается...</p> <p>14. При достижении квоты Банк России осуществляет следующие меры в отношении иностранных инвестиций...</p> <p>15. Филиалом кредитной организации является...</p> <p>16. Представительством кредитной организации является...</p> <p>17. Ликвидатором кредитной организации, имевшей лицензию Банка России на привлечение во вклады денежных средств физических лиц, является...</p> <p>18. Контроль за соблюдением кредитными организациями антимонопольного законодательства Российской Федерации на рынке банковских услуг осуществляют...</p> <p>19. Вклад – это...</p> <p>20. Банки имеют право создавать фонды добровольного страхования вкладов для...</p> <p><b>Задание 3.2:</b> Согласно ФЗ №86-ФЗ от 10.07.2002г. (с изм. и доп.) «О ЦЕНТРАЛЬНОМ БАНКЕ РОССИЙСКОЙ ФЕДЕРАЦИИ (БАНКЕ РОССИИ)», ответьте на вопросы:</p> <p>1. Целями деятельности Банка России являются...</p> <p>2. Банк России подотчетен какому органу?</p> <p>3. Банк России имеет уставный капитал в размере ...</p> <p>4. Национальный финансовый совет – это...</p> <p>5. Численность Национального финансового совета составляет сколько человек?</p> <p>6. Председатель Банка России назначается на должность Государственной Думой сроком на сколько лет?</p> <p>7. Кандидатуру для назначения на должность Председателя Банка России представляет кто?</p> <p>8. Отчетный период (отчетный год) Банка России устанавливается с... по...?</p> <p>9. Годовой отчет Банка России включает...</p> <p>10. Основными инструментами и методами денежно-кредитной политики Банка России являются...</p> <p>11. Под операциями Банка России на открытом рынке понимаются...</p> <p>12. Под рефинансированием понимается...</p> <p>13. Под прямыми количественными ограничениями Банка России понимается...</p> <p>14. Обеспечением кредитов Банка России могут выступать...</p> <p>15. Банк России устанавливает для небанковских кредитных организаций - центральных контрагентов следующие обязательные нормативы...</p> <p>16. В рамках осуществления своей деятельности уполномоченный представитель Банка России вправе...</p>
--	--

	<p>17. Некредитными финансовыми организациями в соответствии с настоящим Федеральным законом признаются лица, осуществляющие следующие виды деятельности...</p> <p><b>Задание 4.1:</b> Согласно Федеральному Закону "О коммерческой тайне" от 29.07.2004 № 98-ФЗ (с изм.и дополнениями), ответьте на следующие вопросы:</p> <ol style="list-style-type: none"> <li>1. коммерческая тайна – это...</li> <li>2. информация, составляющая коммерческую тайну – это...</li> <li>3. обладатель информации, составляющей коммерческую тайну – это...</li> <li>4. доступ к информации, составляющей коммерческую тайну – это...</li> <li>5. передача информации, составляющей коммерческую тайну – это...</li> <li>6. контрагент – это...</li> <li>7. предоставление информации, составляющей коммерческую тайну – это...</li> <li>8. разглашение информации, составляющей коммерческую тайну – это...</li> <li>9. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя...</li> <li>10. Меры по охране конфиденциальности информации признаются разумно достаточными, если...</li> <li>11. В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель обязан...</li> <li>12. Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет какую ответственность?</li> <li>13. Органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну какую ответственность?</li> </ol> <p><b>Задание 4.2:</b> Перепишите в тетрадь для практических занятий</p> <p style="text-align: center;"><i>Соотношение банковской и коммерческой тайны</i></p> <p>Некоторые исследователи считают, что банковская тайна представляет собой особую разновидность коммерческой тайны. С такой позицией сложно согласиться, так как банковская тайна существенно отличается от коммерческой.</p> <ol style="list-style-type: none"> <li>1. Банковская тайна возникает в силу закона вне зависимости от волеизъявления субъектов отношений по поводу ее охраны. Напротив, информация приобретает статус коммерческой тайны после одностороннего объявления её коммерческой тайной. В отношении банковской тайны закон устанавливает ее содержание, субъектов, порядок предоставления. В то же время в соответствии с Федеральным законом от</li> </ol>
--	--

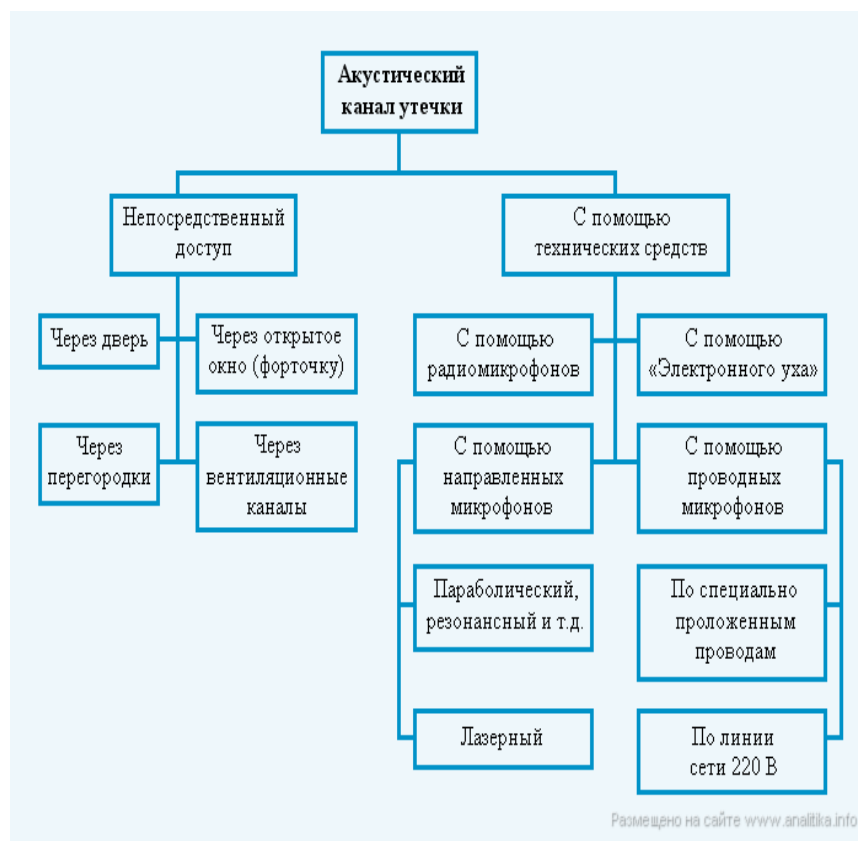
	<p>29.07.2004 № 98-ФЗ «О коммерческой тайне», объем информации, относящейся к коммерческой тайне, устанавливается организацией самостоятельно, также как и круг лиц, обладающих доступом к охраняемым сведениям.</p> <p>2. Одним из основных признаков банковской тайны является то, что конфиденциальная информация предоставляется клиентом банку в целях обеспечения надлежащего оказания банком соответствующих услуг по договору с клиентом. Таким образом, передача сведений носит вспомогательный (акцессорный) характер по отношению к заключенному между банком и клиентом договору. Обязанность хранить банковскую тайну неотделима от других обязательств банка по такому договору. Коммерческая тайна, в отличие от банковской, не имеет признаков акцессорности – создание коммерческой тайны является самоцелью действий субъекта по установлению соответствующего режима.</p> <p>3. Обязанность по охране банковской тайны является относительной: одному управомоченному лицу (клиенту) противостоит одно обязанное (банк). Напротив, отношения по охране коммерческой тайны являются абсолютными: одному управомоченному лицу (обладателю информации) противостоит неопределенный круг лиц, обязанных воздерживаться от посягательства на эту информацию.</p> <p>4. Одним из обязательных признаков коммерческой тайны является принятие ее обладателем мер к охране ее конфиденциальности. Для режима банковской тайны характерно закрепление обязанности по охране конфиденциальности сведений только за владельцами и пользователями информации в интересах обладателя, но не за самим обладателем информации.</p> <p>5. Коммерческая тайна может являться предметом сделок (например, такую информацию можно передать другому лицу, получив за это деньги), а банковская тайна не может передаваться лицом, осуществляющим ее охрану, по сделкам с третьими лицами.</p> <p>6. К числу обязательных признаков коммерческой тайны относится наличие у информации действительной или потенциальной коммерческой ценности в силу ее неизвестности третьим лицам. Для лица, осуществляющего охрану тайны, существует позитивный экономический стимул. Банковская же тайна предполагает охрану не только информации, связанной с предпринимательской деятельностью, а любой информации, которая связана с соответствующими банковскими операциями, в том числе и не имеющей коммерческого характера.</p>
<p><b>Вариант</b> №3 Классификация угроз утечки информации при автоматизированной</p>	<p><b>Задание 5.1:</b> заполните таблицу:</p>

обработке	Виды угроз:		
	№	Виды угроз	Характеристика
	1	Естественные угрозы	
	2	Искусственные угрозы	
	3	Угрозы, источником которых является природная среда	
	4	Угрозы, источником которых является человек	
	5	Угрозы, источником которых являются санкционированные программно-аппаратные средства	
	6	Угрозы, источником которых являются несанкционированные программно-аппаратные средства	
	7	Угрозы, источник которых расположен вне контролируемой зоны	
	8	Угрозы, источник которых расположен в пределах контролируемой зоны	
	9	Угрозы, использующие стандартный доступ	
	10	Угрозы, использующие нестандартный путь доступа	
	11	Угрозы нарушения конфиденциальности информации	
	12	Угрозы нарушения целостности информации	
	13	Угрозы нарушения доступности информации	
	14	Активные угрозы	
	15	Пассивные угрозы	
<b>Задание 6.1:</b> Опишите схему:			
<pre> graph TD     A[Технические каналы утечки информации] --&gt; B[По физической природе носителя]     A --&gt; C[По информативности]     A --&gt; D[По времени функционирования]     A --&gt; E[По структуре]     B --&gt; B1[оптические]     B --&gt; B2[акустические]     B --&gt; B3[радиозлектронные]     B --&gt; B4[материально-вещественные]     C --&gt; C1[информативные]     C --&gt; C2[малоинформативные]     D --&gt; D1[постоянные]     D --&gt; D2[эпизодические]     D --&gt; D3[случайные]     E --&gt; E1[одноканальные]     E --&gt; E2[составные] </pre> <p>Технические каналы утечки информации</p> <ul style="list-style-type: none"> <li>По физической природе носителя <ul style="list-style-type: none"> <li>- оптические</li> <li>- акустические</li> <li>- радиозлектронные</li> <li>- материально-вещественные</li> </ul> </li> <li>По информативности <ul style="list-style-type: none"> <li>- информативные</li> <li>- малоинформативные</li> </ul> </li> <li>По времени функционирования <ul style="list-style-type: none"> <li>- постоянные</li> <li>- эпизодические</li> <li>- случайные</li> </ul> </li> <li>По структуре <ul style="list-style-type: none"> <li>- одноканальные</li> <li>- составные</li> </ul> </li> </ul>			
<b>Задание 6.2:</b> Опишите схему:			





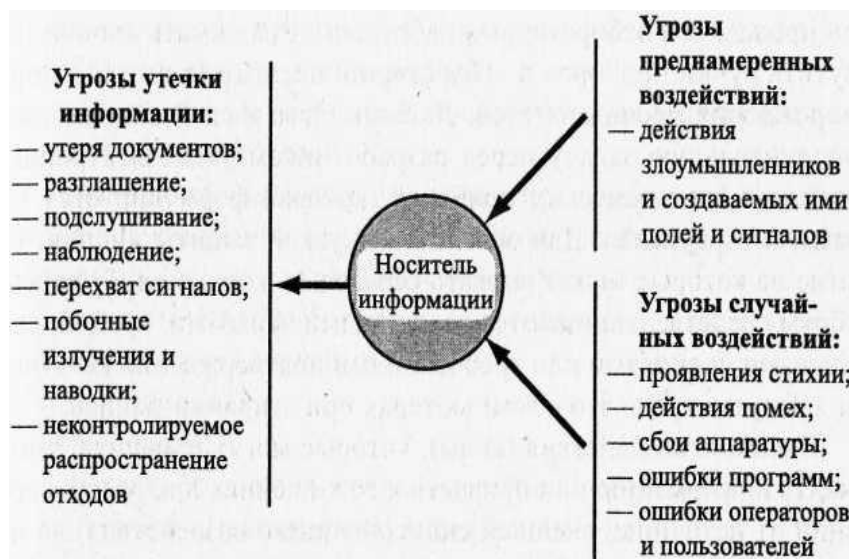
**Задание 6.3:** Опишите схему:



**Задание 7.1:** Охарактеризуйте схему:



**Задание 7.2:** Охарактеризуйте схему:



**Вариант №4** Виды и источники утечки банковской информации по техническим каналам

**Задание 8.1:** Ответьте на тестовые задания:

**1.Гарантированная конституционными, законодательными и практическими мерами защищенность и обеспеченность жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз – это...**

- А) Угроза
- Б) Безопасность
- В) Опасность
- Г) Ущерб

**2.Предполагает разработку системы безопасности на основе федерального законодательства и других нормативных актов – это принцип организации**

	<p><b>и функционирования системы безопасности?</b></p> <p>А) Экономичность</p> <p>Б) Совершенствование</p> <p>В) Законность</p> <p>Г) Специализация</p> <p><b>3. Состояние защищенности интересов владельцев, руководства и клиентов банка, материальных ценностей и информационных ресурсов от внутренних и внешних угроз – это...</b></p> <p>А) Безопасность банка</p> <p>Б) Основная цель безопасности банка</p> <p>В) Угроза</p> <p>Г) Опасность</p> <p><b>4. Предполагает самостоятельное функционирование системы безопасности по единым правовым, организационным, функциональным и методологическим принципам – это принцип организации и функционирования системы безопасности?</b></p> <p>А) Своевременность</p> <p>Б) Комплексность</p> <p>В) Активность</p> <p>Г) Централизация управления</p> <p><b>5. Что является объектом безопасности?</b></p> <p>А) Государство</p> <p>Б) Персонал</p> <p>В) Клиент</p> <p>Г) Служба безопасности</p> <p><b>6. Одно из преступлений против собственности, одна из ненасильственных форм хищения, представляет собой завладение чужим имуществом путем обмана либо злоупотребления доверием.</b></p> <p>А) Мошенничество</p> <p>Б) Кража</p> <p>В) Разбой</p> <p>Г) Нападение</p> <p><b>7. Преступник (или группа), находящийся вне объекта охраны, целью которого является проникновение на объект для хищения ценностей или информации.</b></p> <p>А) Внутренний злоумышленник</p> <p>Б) Внешний злоумышленник</p> <p>В) Хулиган</p> <p>Г) Убийца</p> <p><b>8. Служащий банка или сотрудник охраны, имеющий доступ на объект, располагающий определенной информацией о режиме работы банка и,</b></p>
--	--

	<p><b>может быть, системе охраны.</b></p> <p>А)Преступник  Б)Хулиган  В)Внешний злоумышленник  Г)Внутренний злоумышленник</p> <p><b>9.Неосведомленный злоумышленник, как правило, невооруженный и без специального оснащения человек, пытающийся проникнуть в помещение банка без определенного плана действий.</b></p> <p>А)Случайный  Б)Одиночный  В)Высококвалифицированный  Г)Опытный</p> <p><b>10.... - это общественно опасное деяние (действие или бездействие), посягающее на личность, общество и государство, а также на иные охраняемые законом объекты.</b></p> <p>А)Угроза  Б)Насилие  В)Преступление  Г)Разбой</p> <p><b>11.Какая защита нужна банку от недобросовестных деловых партнеров и необоснованных обвинений правоохранительных органов?</b></p> <p>А)Обычная охрана;  Б)Юридическая защита;  В)Защита службы банковской безопасности;  Г)Защита частных охранно-детективных структур.</p> <p><b>12.Что относится к внешним правовым, законодательным и нормативным актам обеспечения безопасности банка?</b></p> <p>А)Конституция, законы, кодексы, постановления, указы;  Б)Устав и положения банка;  В)Руководство, инструкции, устав, положения;  Г)Перечень сведений, относящихся к банковской тайне.</p> <p><b>13.К внутренним правовым, законодательным и нормативным актам обеспечения безопасности банка относятся:</b></p> <p>А)Конституция, законы, кодексы;  Б)Нормы, постановления, указы;  В)Устав, положение, руководство, инструкции;  Г)Конституция, законы, кодексы, положение о системе безопасности.</p> <p><b>14.Как называется статья 182 Уголовного Кодекса Российской Федерации?</b></p> <p>А)«Заведомо ложная реклама»;  Б)«Неприкосновенность жилища, охрана личной жизни и тайна переписки»;  В)«Применение звукозаписи при допросе»;</p>
--	---

	<p>Г) «Разглашение данных предварительного расследования».</p> <p><b>15. Как называется статья 151 Гражданского Кодекса Российской Федерации?</b></p> <p>А) «Защита чести, достоинства и деловой репутации»;</p> <p>Б) «Коммерческое представительство»;</p> <p>В) «Компенсация морального вреда»;</p> <p>Г) «Обязанности должника возместить убытки».</p> <p><b>16. Как называется информация, доступ к которой ограничивается в соответствии с законодательством РФ?</b></p> <p>А) Секретная;</p> <p>Б) Конфиденциальная;</p> <p>В) Служебная;</p> <p>Г) Профессиональная</p> <p><b>17. Какое название у федерального закона, который напрямую относит к категории конфиденциальной информации?</b></p> <p>А) «О банках и банковской деятельности в РСФСР»;</p> <p>Б) «О связи»;</p> <p>В) «О коммерческой деятельности»;</p> <p>Г) «Об информации, информатизации и защите информации»</p> <p><b>18. Что такое информация?</b></p> <p>А) это сведения о предметах, объектах, явлениях и процессах, отображаемые в сознании человека, для последующего их восприятия человеком;</p> <p>Б) информационные носители в виде самых разнообразных изданий: книги, статьи, доклады, тезисы и т.д.;</p> <p>В) сведения, составляющие тайну следствия и судопроизводства;</p> <p>Г) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников.</p> <p><b>19. Личная информация – это ...</b></p> <p>А) Служебные сведения, доступ к которым ограничен органами государственной власти;</p> <p>Б) Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен законами;</p> <p>В) Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его персональные данные, за исключением сведений, подлежащих распространению в СМИ в установленном порядке;</p> <p>Г) Сведения связанные с профессиональной деятельностью, доступ к которым ограничен законами.</p> <p><b>20. Что из перечисленного не относится к техническим носителям информации?</b></p> <p>А) Бумажные носители;</p> <p>Б) Видеофильмы;</p> <p>В) Информация на экранах ЭВМ;</p>
--	---

	<p>Г) Рекламные проспекты</p> <p><b>21.К способам воровства конфиденциальной информации не относится:</b></p> <p>А)физический доступ к местам ее хранения и обработки;</p> <p>Б)использование резервных копий;</p> <p>В)несанкционированный доступ сотрудниками банка;</p> <p>Г)сбой операционных систем.</p> <p><b>22.Группа людей в банке, обладающих в локальной сети повышенными привилегиями:</b></p> <p>А)руководители;</p> <p>Б)системные администраторы;</p> <p>В)мошенники;</p> <p>Г)клиенты.</p> <p><b>23.При использовании этого принципа криптографической защиты данные в основном хранилище всегда находятся только в закодированном виде:</b></p> <p>А)принцип прозрачного шифрования;</p> <p>Б)винчестеров;</p> <p>В)принцип технических особенностей;</p> <p>Г)принцип системы серверной защиты.</p> <p><b>24.Надежно защитить резервные копии от несанкционированного использования можно только с помощью:</b></p> <p>А)шифрования;</p> <p>Б)криптографии;</p> <p>В)смарт-карт;</p> <p>Г)закрытого диска.</p> <p><b>25.Управлять шифрованием информации должен:</b></p> <p>А)офицер безопасности;</p> <p>Б)технический сотрудник;</p> <p>В)системный администратор;</p> <p>Г)руководитель организации.</p> <p><b>26.Для совершения злоупотреблений в кредитных и вексельных отделах банковские служащие чаще всего подделывают на векселях...</b></p> <p>А)Печать</p> <p>Б)Подписи клиентов</p> <p>В)Данные</p> <p>Г)Номер векселя</p> <p><b>27.Недобросовестные сотрудники присваивают банковские деньги в свои карманы путем...</b></p> <p>А)Занижения дохода</p> <p>Б)Выдачи фиктивных займов</p> <p>В)Завышения дохода</p>
--	---

	<p>Г)Нет верного ответа</p> <p><b>28.Для сокрытия растраты служащие иногда...</b></p> <p>А)занижают проводки по кредиту и завышают проводки по дебету</p> <p>Б)занижают проводки по дебету и завышают проводки по кредиту</p> <p>В)занижают доход</p> <p>Г)занижают расходы</p> <p><b>29.Одно из нарушений проявляющееся в конфиденциальности</b></p> <p>А)Разглашение</p> <p>Б)Мошенничество</p> <p>В)Потери</p> <p>Г)Нарушение связи</p> <p><b>30.Одно из нарушений проявляющееся в доверенности</b></p> <p>А)Фальсификация</p> <p>Б)НСД</p> <p>В)Ошибки</p> <p>Г)Нарушение связи</p> <p><b>31.Объект, осуществляющий выбор из всей совокупности информационных сообщений одного сообщения, подлежащего передаче по каналу связи адресату – это ...</b></p> <p>А)источник информации;</p> <p>Б)сообщение;</p> <p>В)отправитель сообщения;</p> <p>Г)канал распространения.</p> <p><b>32.Набор знаков (текст документа), с помощью которых сведения могут быть переданы другому объекту и восприняты им – это ...</b></p> <p>А)источник информации;</p> <p>Б)сообщение;</p> <p>В)отправитель сообщения;</p> <p>Г)канал распространения.</p> <p><b>33.Объект, осуществляющий непосредственную передачу документа, содержащего конфиденциальную информацию – это ...</b></p> <p>А)источник информации;</p> <p>Б)сообщение;</p> <p>В)отправитель сообщения;</p> <p>Г)канал распространения.</p> <p><b>34.Среда, используемая для передачи сообщения –это ...</b></p> <p>А)источник информации;</p> <p>Б)сообщение;</p> <p>В)отправитель сообщения;</p> <p>Г)канал распространения.</p> <p><b>35.Источником конфиденциальной информации не является:</b></p>
--	--

	<p>А)персонал предприятия;</p> <p>Б)технические средства;</p> <p>В)средства коммуникации;</p> <p>Г)канал распространения.</p> <p><b>36.Цель защиты информации?</b></p> <p>А)установление особого режима конфиденциальности</p> <p>Б)ограничение доступа к конфиденциальной информации</p> <p>В)осуществление контроля за соблюдением установленного режима конфиденциальности</p> <p>Г)предотвращение утечки, хищения, искажения, подделки информации</p> <p><b>37.Особый режим конфиденциальности подразумевает?</b></p> <p>А)установление особого режима конфиденциальности</p> <p>Б)ограничение доступа к конфиденциальной информации</p> <p>В)установление порядка пользования носителями конфиденциальной информации</p> <p>Г)осуществление контроля за соблюдением установленного режима конфиденциальности</p> <p><b>38.Цель защиты информации?</b></p> <p>А)меры по обеспечению ее конфиденциальности принимает собственник информации.</p> <p>Б)передача сведений о деятельности предприятия и данных о его сотрудниках в территориальные инспекторские и надзорные органы</p> <p>В)сохранение государственной тайны, конфиденциальности документированной информации.</p> <p>Г)свободного доступа на законном основании</p> <p><b>39.Мероприятие по ее защите коммерческой информации?</b></p> <p>А)ограничение доступа к конфиденциальной информации</p> <p>Б)предотвращение несанкционированных действий по уничтожению, искажению, блокированию информации</p> <p>В)предотвращение утечки, хищения, искажения, подделки информации;</p> <p>Г)сохранение государственной тайны, конфиденциальности документированной информации</p> <p><b>40.Особый режим конфиденциальности подразумевает?</b></p> <p>А)предотвращение утечки, хищения, искажения, подделки информации</p> <p>Б)предотвращение несанкционированных действий по уничтожению информации</p> <p>В)закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность</p> <p>Г)сохранение государственной тайны, конфиденциальности документированной информации</p> <p><b>41. Проявление фактов угроз со стороны отдельных лиц или групп – это?</b></p>
--	--



	<p>А)Кризисная обстановка  Б)Кризисная ситуация  В)Опасная ситуация  Г)Опасная обстановка</p> <p><b>42.Какие задачи не решает кризисная группа?</b></p> <p>А)оценка обстановки  Б)принятие неотложных мер по безопасности  В)обеспечение оперативного взаимодействия с органами правопорядка  Г)выявление возможных преступных групп</p> <p><b>43.Какие режимы функционирования системы безопасности предлагают специалисты?</b></p> <p>А)Повседневной деятельности, повышенной готовности, чрезвычайного положения  Б)Чрезвычайного положения, рабочий, усиленной готовности  В)Усиленной готовности, повышенной готовности, умеренной готовности  Г)Усиленной готовности, повышенной готовности, повседневный</p> <p><b>44. Главная цель создания кризисной группы – это:</b></p> <p>А)Защита банка от внутренних угроз  Б)Восстановление банка после кризиса  В)Противодействие внешним угрозам безопасности банка  Г)Все ответы верны</p> <p><b>45.На кого возложено руководство в кризисной группе?</b></p> <p>А)На главу банка  Б)На отдел безопасности  В)На ЦБ  Г)На правоохранительные органы</p> <p><b>Задание 9.1:</b> Согласно Закону «Об электронной подписи» № 63-ФЗ от 6.04.2011, (с изм. и доп.) ответьте на следующие вопросы:</p> <ol style="list-style-type: none"> <li>1. Электронная подпись – это...</li> <li>2. Сертификат ключа проверки электронной подписи – это...</li> <li>3. Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) – это...</li> <li>4. Владелец сертификата ключа проверки электронной подписи – это...</li> <li>5. Ключ электронной подписи – это...</li> <li>6. Ключ проверки электронной подписи – это...</li> <li>7. Удостоверяющий центр – это...</li> <li>8. Аккредитация удостоверяющего центра – это...</li> <li>9. Средства электронной подписи – это...</li> <li>10. Средства удостоверяющего центра – это...</li> <li>11. Участники электронного взаимодействия – это...</li> <li>12. Корпоративная информационная система – это...</li> </ol>
--	--

	<p>13. Информационная система общего пользования – это...</p> <p>14. Вручение сертификата ключа проверки электронной подписи – это...</p> <p>15. Подтверждение владения ключом электронной подписи – это...</p> <p>16. Виды электронных подписей, используемых органами исполнительной власти и органами местного самоуправления, порядок их использования, а также требования об обеспечении совместимости средств электронных подписей при организации электронного взаимодействия указанных органов между собой устанавливает какой орган?</p> <p>17. Простая электронная подпись – это...</p> <p>18. Неквалифицированной электронной подписью является электронная подпись, которая...</p> <p>19. Квалифицированная электронная подпись – это...</p> <p>20. Электронный документ считается подписанным простой электронной подписью при выполнении, в том числе одного из следующих условий:</p> <p>21. При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:</p> <p>22. Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые...</p> <p>23. При создании электронной подписи средства электронной подписи должны...</p> <p>24. Сертификат ключа проверки электронной подписи должен содержать следующую информацию...</p> <p>25. Сертификат ключа проверки электронной подписи прекращает свое действие:</p> <p>26. Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи в следующих случаях...</p> <p><b>Задание 10.1:</b> Согласно Закону «О кредитных историях» № 218-ФЗ от 30.12.2004, (с изм. и доп.) ответьте на следующие вопросы:</p> <ol style="list-style-type: none"> <li>1. Кредитная история – это...</li> <li>2. Запись кредитной истории – это...</li> <li>3. Кредитный отчет – это...</li> <li>4. Бюро кредитных историй – это...</li> <li>5. Пользователь кредитной истории – это...</li> <li>6. Центральный каталог кредитных историй – это...</li> <li>7. Государственный реестр бюро кредитных историй – это...</li> <li>8. Код субъекта кредитной истории – это...</li> <li>9. Кредитная история субъекта кредитной истории - физического лица состоит из...</li> <li>10. Кредитная история субъекта кредитной истории - юридического лица состоит из...</li> </ol>
--	---

	<p>11. Бюро кредитных историй предоставляет кредитный отчет кому, каким органам?</p> <p>12. Бюро кредитных историй вправе...</p> <p>13. Центральный каталог кредитных историй создается каким банком?</p> <p><b>Задание 11.1:</b> Согласно Федеральному Закону от 27 июля 2010 года, № 224-ФЗ (с изменениями и дополнениями) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», ответьте на вопросы:</p> <ol style="list-style-type: none"> <li>1. Инсайдерская информация – это...</li> <li>2. Предоставление информации – это...</li> <li>3. К инсайдерской информации не относятся...</li> <li>4. К инсайдерам относятся следующие лица...</li> <li>5. Запрещается использование инсайдерской информации...</li> </ol> <p><b>Задание 11.2:</b> Согласно Закону РФ «О персональных данных» от 27.07.2006 (с изм.и доп), ответьте на вопросы:</p> <ol style="list-style-type: none"> <li>1. Персональные данные – это...</li> <li>2. Оператор – это...</li> <li>3. Обработка персональных данных – это...</li> <li>4. Автоматизированная обработка персональных данных – это...</li> <li>5. Распространение персональных данных – это...</li> <li>6. Предоставление персональных данных – это...</li> <li>7. Блокирование персональных данных – это...</li> <li>8. Уничтожение персональных данных – это...</li> <li>9. Обезличивание персональных данных – это...</li> <li>10. Информационная система персональных данных – это...</li> <li>11. Трансграничная передача персональных данных – это...</li> <li>12. В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его...</li> <li>13. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности...</li> <li>14. Уведомление должно содержать следующие сведения...</li> <li>15. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано...</li> </ol> <p><b>Задание 11.3:</b> Согласно Закону РФ «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ» от 7 июля 2006 года №149-ФЗ (с изм. и доп), ответьте на вопросы:</p> <ol style="list-style-type: none"> <li>1. Информация – это...</li> <li>2. Информационные технологии – это...</li> <li>3. Информационная система – это...</li> </ol>
--	--

	4. Информационно-телекоммуникационная сеть – это... 5. Владелец информации – это... 6. Доступ к информации – это... 7. Конфиденциальность информации – это... 8. Предоставление информации – это... 9. Распространение информации – это... 10. Электронное сообщение – это... 11. Документированная информация – это... 12. Электронный документ – это... 13. Оператор информационной системы – это... 14. Сайт в сети "Интернет" – это... 15. Страница сайта в сети "Интернет" – это... 16. Доменное имя – это... 17. Сетевой адрес – это... 18. Владелец сайта в сети "Интернет" – это... 19. Провайдер хостинга – это... 20. Единая система идентификации и аутентификации – это... 21. Поисковая система – это... 22. Информация в зависимости от порядка ее предоставления или распространения подразделяется на... 23. Владелец информации, если иное не предусмотрено федеральными законами, вправе... 24. Владелец информации при осуществлении своих прав обязан... 25. Государственное регулирование в сфере применения информационных технологий предусматривает... 26. Информационные системы включают в себя... 27. В реестр нарушителей включаются...	
Пакет преподавателя	<hr/> <hr/> <i>ответы (ключи к выполнению работы, или алгоритм решения задания)</i>	
Критерии оценки	Отлично	теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко
	Хорошо	теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками
	Удовлетворительно	теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном

		сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки
	Неудовлетворительно	теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки

**КИМ №2**  
**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ устного опроса**

<b>Раздел 1</b>		<b>Характеристика угроз безопасности банка</b>
Тема 1.2.		Наиболее характерные преступления, совершаемые в банковской сфере
<b>Раздел 2</b>		<b>Защита конфиденциальной банковской информации</b>
Тема 2.1.		Правовые основы защиты конфиденциальности банковской информации
<b>Раздел 3</b>		<b>Защита банковской информации в автоматизированных системах обработки</b>
Тема 3.1.		Классификация угроз утечки информации при автоматизированной обработке
Тема 3.2.		Виды и источники утечки банковской информации по техническим каналам
<b>Форма контроля</b>		
<b>Вид контроля</b>		
<b>Спецификация ПК</b> (Указываются коды профессиональных компетенций и коды их структурных элементов (действий, умений, знаний), которые проверяются данным КИМом)	ПК 1.1	ПД1.1-1, ПУ1.1-1, ПЗ1.1-1
	ПК 1.6	ПД1.6-1, ПУ1.1-1, ПЗ1.1-1
<b>Спецификация ОК</b> (Указываются коды общих компетенций и коды их структурных элементов (дескрипторов, умений, знаний), которые проверяются данным КИМом)	ОК01	ОД.01-1, ОД.01-2,ОД.01-3,ОУ.01-1,ОУ.01-2,ОУ.01-3, ОЗ.01-1,ОЗ.01-2,ОЗ.01-3
	ОК02	ОД.02-1,ОД.02-2,ОД.02-3,ОУ.02-1,ОУ.02-2,ОУ.02-3,ОЗ.02-1,ОЗ.02-2,ОЗ.02-3
	ОК03	ОД.03-1,ОД.03-2,ОУ.03-1,ОУ.03-2,ОЗ.03-1,ОЗ.03-2
	ОК04	ОД.04-1,ОУ.04-1,ОЗ.04-1
	ОК05	ОД.05-1,ОД.05-2,ОУ.05-1,ОУ.05-2,ОЗ.05-1,ОЗ.05-2
	ОК09	ОД.09-1,ОД.09-2,ОУ.09-1,ОУ.09-2,ОЗ.09-1,ОЗ.09-2
	ОК10	ОД.10-1,ОД.10-2,ОУ.10-1,ОУ.10-2,ОЗ.10-1,ОЗ.10-2
	ОК11	ОД.11-1,ОД.11-2,ОУ.11-1,ОУ.11-2,ОЗ.11-1,ОЗ.11-2
<b>Условия выполнения задания</b>		Устный опрос выполняется в аудитории, время проведения работы 30 минут
<b>Инструкция для студентов</b>		Для устного опроса необходимо использовать материалы лекции, Интернета
<b>Оборудование и оснащение</b>		–
<b>Источники</b>		<u>Основные источники:</u> 1.Партыка Л.П. Информационная безопасность. – СПб.: Питер, 2020. 2.Ярочкин В.И. Безопасность банковских систем. – М.: Ось-89, 2020. 3.Ярочкин В.И. Теория безопасности. – М.: Академический проект, 2020. <u>Дополнительные источники:</u> 4.Ваксян А. Анатомия мошенничества. – М.: 2020. 5.Зежвда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2020. <u>Интернет источники:</u> 1.Консультант +

Тема 1.1 Организационные основы банковской безопасности. Цель и задачи обеспечения безопасности банка. Внешние и внутренние угрозы безопасности банка	<b>Вопросы для устного опроса:</b> <ol style="list-style-type: none"> <li>1. Понятие безопасности банка.</li> <li>2. Понятие риска.</li> <li>3. Понятие угрозы.</li> <li>4. Основная цель безопасности банка.</li> <li>5. Задачи безопасности банка.</li> <li>6. Виды угроз по признаку целевой направленности.</li> <li>7. Виды угроз по признаку источника угрозы..</li> <li>8. Виды угроз по экономическому характеру.</li> </ol>
Тема 1.2. Наиболее характерные преступления, совершаемые в банковской сфере	<b>Вопросы для устного опроса:</b> <ol style="list-style-type: none"> <li>1. Характеристика «беловоротничковых» преступлений.</li> <li>2. Понятие насильственной преступности.</li> <li>3. Характеристика лиц, совершающих насильственные преступления и хулиганство.</li> <li>4. Нравственно-психологические свойства личности насильственных преступников.</li> <li>5. Характеристика мошенничества.</li> <li>6. Характеристика лжепредпринимательства.</li> <li>7. Преступления, совершаемые с использованием методов бухгалтерского учёта.</li> <li>8. Преступления, совершаемые другими категориями банковских служащих.</li> <li>9. Злоупотребления в транзитных отделах банка.</li> </ol>
Тема 2.1. Правовые основы защиты конфиденциальности банковской информации	<b>Вопросы для устного опроса:</b> <ol style="list-style-type: none"> <li>1. Понятие конфиденциальности.</li> <li>2. Понятие банковской тайны.</li> <li>3. Основные объекты банковской тайны.</li> <li>4. Владельцы и пользователи банковской тайны.</li> <li>5. Понятие профессиональной тайны.</li> <li>6. Признаки профессиональной тайны.</li> </ol>
Тема 2.2. Понятие и состав конфиденциальной банковской информации	<b>Вопросы для устного опроса:</b> <ol style="list-style-type: none"> <li>1. Понятие конфиденциальности информации.</li> <li>2. Режим коммерческой тайны.</li> <li>3. Понятие коммерческой тайны.</li> <li>4. Виды ответственности за разглашение коммерческой тайны.</li> <li>5. Основные отличия коммерческой и банковской тайны.</li> <li>6. Разглашение информации, составляющей коммерческую тайну.</li> </ol>
Тема 2.3. Источники утечки банковской информации	<b>Вопросы для устного опроса:</b> <ol style="list-style-type: none"> <li>1. Прямой ущерб от утечек данных.</li> <li>2. Косвенный ущерб от утечек данных.</li> <li>3. Случайные угрозы утечки информации.</li> <li>4. Преднамеренные утечки информации.</li> <li>5. Характеристика DLP-системы.</li> <li>6. Причины утечки банковской информации.</li> <li>7. Методы защиты банковской информации.</li> </ol>
Тема 3.1. Классификация угроз утечки информации при автоматизированной обработке	<b>Вопросы для устного опроса:</b> <ol style="list-style-type: none"> <li>1. Умышленные угрозы.</li> <li>2. Случайные.</li> <li>3. Активные.</li> <li>4. Пассивные.</li> </ol>

	<p>5. Угроза доступа к информации на внешних запоминающих устройствах (ЗУ), например, копирование данных с жесткого диска.</p> <p>6. Угроза доступа к информации в оперативной памяти (несанкционированное обращение к памяти).</p> <p>7. Угроза доступа к информации, циркулирующей в линиях связи (путем незаконного подключения).</p> <p>8. Угрозы, проявляющиеся независимо от активности КС (хищение носителей информации).</p> <p>9. Угрозы, проявляющиеся только в процессе обработки данных (распространение вирусов).</p> <p>10. Активные и пассивные угрозы утечки.</p>	
Тема 3.2. Виды и источники утечки банковской информации по техническим каналам	<p><b>Вопросы для устного опроса:</b></p> <p>1. Угрозы утечки акустической (речевой) информации</p> <p>2. Угрозы утечки видовой информации</p> <p>3. Угрозы утечки информации по каналам ПЭМИН</p> <p>4. Вспомогательные технические средства</p>	
<b>Критерии оценки</b>		
	Отлично	теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко
	Хорошо	теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками
	Удовлетворительно	теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки
	Неудовлетворительно	теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки



### **3. Комплект КИМ для промежуточной аттестации**

Промежуточная аттестация проводится в форме: **дифференцированного зачёта**

*В произвольной форме описывается организация промежуточной аттестации при изучении учебной дисциплины.*

*Промежуточная аттестация в форме дифференцированного зачёта проводится во время урока по текущим оценкам и по ответам на поставленные вопросы. Обучающемуся необходимо ответить на вопросы, которые предлагаются для зачёта.*

*Перечень теоретических вопросов выдается студентам не позднее, чем за месяц до начала сессии.*

**КИМ № 3**  
**ПЕРЕЧЕНЬ ВОПРОСОВ для дифференцированного зачёта**

<b>Форма контроля</b>		Дифференцированный зачёт
<b>Вид контроля</b>		промежуточная аттестация
<b>Объекты оценки:</b>		
<b>Спецификация ПК</b> (Указываются коды профессиональных компетенций и коды их структурных элементов (действий, умений, знаний), которые проверяются данным КИМом)	ПК 1.1	ПД1.1-1, ПУ1.1-1, ПЗ1.1-1
	ПК 1.6	ПД1.6-1, ПУ1.1-1, ПЗ1.1-1
<b>Спецификация ОК</b> (Указываются коды общих компетенций и коды их структурных элементов (дескрипторов, умений, знаний), которые проверяются данным КИМом)	ОК01	ОД.01-1, ОД.01-2, ОД.01-3, ОУ.01-1, ОУ.01-2, ОУ.01-3, ОЗ.01-1, ОЗ.01-2, ОЗ.01-3
	ОК02	ОД.02-1, ОД.02-2, ОД.02-3, ОУ.02-1, ОУ.02-2, ОУ.02-3, ОЗ.02-1, ОЗ.02-2, ОЗ.02-3
	ОК03	ОД.03-1, ОД.03-2, ОУ.03-1, ОУ.03-2, ОЗ.03-1, ОЗ.03-2
	ОК04	ОД.04-1, ОУ.04-1, ОЗ.04-1
	ОК05	ОД.05-1, ОД.05-2, ОУ.05-1, ОУ.05-2, ОЗ.05-1, ОЗ.05-2
	ОК09	ОД.09-1, ОД.09-2, ОУ.09-1, ОУ.09-2, ОЗ.09-1, ОЗ.09-2
	ОК10	ОД.10-1, ОД.10-2, ОУ.10-1, ОУ.10-2, ОЗ.10-1, ОЗ.10-2
	ОК11	ОД.11-1, ОД.11-2, ОУ.11-1, ОУ.11-2, ОЗ.11-1, ОЗ.11-2
<b>Условия проведения</b>		Аудитория.
<b>Инструкция для студентов</b>		1. Ответить на два теоретических вопроса, если по текущим оценкам не выходит итоговая оценка.
<b>Оборудование и оснащение</b>		Учебная аудитория, стол
<b>Источники</b>		<u>Основные источники:</u> 1.Партыка Л.П. Информационная безопасность. – СПб.: Питер, 2020. 2.Ярочкин В.И. Безопасность банковских систем. – М.: Ось-89, 2020. 3.Ярочкин В.И. Теория безопасности. – М.: Академический проект, 2020. <u>Дополнительные источники:</u> 4.Ваксян А. Анатомия мошенничества. – М.: 2020. 5.Зежвда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2020. <u>Интернет источники:</u> <b>1.Консультант +</b>
<b>Перечень вопросов для зачёта</b>		1. Понятие безопасности банка. 2. Классификация угроз. 3. Насильственные преступления. 4. Финансовые преступления. 5. Правовая охрана банковской тайны. Право конфиденциальности. 6. Банковская тайна. 7. Профессиональная тайна. 8. Конфиденциальная банковская информация 9. Понятие коммерческой тайны. 10. Основные отличия коммерческой и банковской тайны. 11. Утечка банковской информации.. 12. Причины утечки.

	13. Виды угроз утечки информации. 14. Случайные угрозы. 15. Угрозы утечки через каналы доступа. 16. Активный и пассивный перехват информации. 17. Основные технические каналы утечки банковской информации. 18. Основные и вспомогательные технические средства.	
<b>Критерии оценки</b>	Отлично	ставится обучающемуся,, проявившему всесторонние и глубокие знания учебного материала, освоившему основную и дополнительную литературу, обнаружившему творческие способности в понимании, изложении и практическом использовании усвоенных знаний. Оценка «отлично» соответствует высокому уровню освоения дисциплины
	Хорошо	ставится обучающемуся, проявившему полное знание учебного материала, освоившему основную рекомендованную литературу, обнаружившему стабильный характер знаний и умений и способному к их самостоятельному применению, и обновлению в ходе последующего обучения и практической деятельности. Оценка «хорошо» соответствует достаточному уровню освоения дисциплины
	Удовлетворительно	ставится обучающемуся,, проявившему знания основного учебного материала в объеме, необходимом для последующего обучения и предстоящей практической деятельности, знакомому с основной рекомендованной литературой, допустившему неточности при ответе, но в основном обладающему необходимыми знаниями и умениями для их устранения при корректировке со стороны преподавателя. Оценка «удовлетворительно» соответствует достаточному уровню освоения дисциплины
	Неудовлетворительно	ставится обучающемуся, обнаружившему существенные пробелы в знании основного учебного материала, допустившему принципиальные ошибки при применении теоретических знаний, которые не позволяют ему продолжить обучение или приступить к практической деятельности без дополнительной подготовки по данной дисциплине (или МДК). Оценка «неудовлетворительно» соответствует низкому уровню освоения дисциплины

Государственное бюджетное профессиональное образовательное учреждение  
«Южно-Уральский государственный колледж»

Рассмотрено на заседании предметно-цикловой  
комиссии

УТВЕРЖДАЮ:  
Зам. директора по учебной работе

\_\_\_\_\_  
Председатель ПЦК  
\_\_\_\_\_/\_\_\_\_\_  
Протокол № \_\_\_\_ от \_\_\_\_ 20 \_\_\_\_  
г.

\_\_\_\_\_  
« \_\_\_\_ » \_\_\_\_ 20 \_\_\_\_ г.

**Вопросы для дифференцированного зачёта**

По учебной дисциплине «Безопасность банковской деятельности»

Специальность 38.02.07 Банковское дело

2020-2021 учебный год

Преподаватель: Степанова Юлия Александровна

## **Перечень вопросов и практических задач**

*(прикладывается перечень вопросов и практических задач в сквозном порядке)*

1. Понятие безопасности банка.
2. Классификация угроз.
3. Насильственные преступления.
4. Финансовые преступления.
5. Правовая охрана банковской тайны. Право конфиденциальности.
6. Банковская тайна.
7. Профессиональная тайна.
8. Конфиденциальная банковская информация
9. Понятие коммерческой тайны.
10. Основные отличия коммерческой и банковской тайны.
11. Утечка банковской информации..
12. Причины утечки.
13. Виды угроз утечки информации.
14. Случайные угрозы.
15. Угрозы утечки через каналы доступа.
16. Активный и пассивный перехват информации.
17. Основные технические каналы утечки банковской информации.
18. Основные и вспомогательные технические средства.