ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Стерлитамакский филиал

Колледж

Рабочая программа дисциплины

дисциплина ***ОП.16 Безопасность банковской деятельности***

Общепрофессиональный цикл, обязательная часть
цикл дисциплины и его часть (обязательная, вариативная)

специальность
38.02.07 ***Банковское дело***
код наименование специальности

квалификация
специалист банковского дела

Год начала подготовки
2021

Разработчик (составитель)
преподаватель первой категории
Пименова С.С.
ученая степень, ученое звание,
категория, Ф.И.О.

Стерлитамак 2023

ОГЛАВЛЕНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы

Рабочая программа дисциплины «Безопасность банковской деятельности» является частью основной образовательной программы в соответствии с ФГОС для специальности: 38.02.07 Банковское дело (укрупнённая группа специальностей 38.02.00 Экономика и управление), для обучающихся очной формы обучения.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Безопасность банковской деятельности» относится к профессиональному циклу, общепрофессиональным дисциплинам, входящей в вариативную часть ППССЗ.

1.3. Цель и планируемые результаты освоения дисциплины:

Код ОК, ПК	Умения	Знания
ОК. 02 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	составлять системное описание банковских угроз для конкретной кредитной организации;	потенциально уязвимые места банка со стороны криминальных угроз;
ОК.3 Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	принимать эффективные решения, используя систему методов управления	особенности организации управления в банковских учреждениях;
ОК. 04 Осуществлять поиск и использование информации, необходимой для эффективности выполнения профессиональных задач, профессионального и личностного развития	рассчитывать по принятой методологии основные технико-экономические показатели деятельности организации;	организацию производственного и технологического процессов;
ОК. 07 Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	принимать эффективные решения, используя систему методов управления	особенности организации управления в банковских учреждениях;

ОК. 08 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	применять в профессиональной деятельности приемы и методы эффективного делового общения;	сущность и основные виды коммуникаций;
ОК. 10 Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий	использовать правовые нормы в целях защиты интересов банка;	роль и место правовых актов органов государственной власти, Банка России и внутренних нормативных актов банка в обеспечении безопасности банковской деятельности;
ОК. 11 Знать правила техники безопасности, нести ответственность за организацию мероприятий по обеспечению безопасности труда	выявлять типичные признаки преступных посягательств;	способы совершения хищений в процессе кредитных операций и т.п.;
ПК 1.1 Осуществлять расчетно-кассовое обслуживание клиентов	выполнять задачи по организации деятельности структурных подразделения системы безопасности;	структуру системы безопасности кредитных организаций, порядок формирования, цели и задачи системы безопасности банка;
ПК 1.2 Осуществлять безналичные платежи с использованием различных форм расчетов в национальной и иностранной валютах.	делать выбор конкретных устройств, предназначенных для охраны банка и защиты банковских операций и продуктов;	виды технических средств обеспечения безопасности банка и их назначение;
ПК 1.3 Осуществлять расчетное обслуживание счетов бюджетов различных уровней.	оформлять документацию в соответствии с нормативной базой, используя информационные технологии и средства оргтехники;	основные понятия документационного обеспечения управления;
ПК 1.4 Осуществлять межбанковские расчеты.	выявлять типичные признаки преступных посягательств;	способы совершения хищений в процессе кредитных операций и т.п.;
ПК 1.5 Осуществлять	выявлять типичные признаки	виды рисков в сфере вексельного

международные расчеты по экспортно-импортным операциям.	преступных посягательств;	обращения, типичные неправомерного завладения векселями;
ПК 2.1 Оценивать кредитоспособность клиентов.	составлять системное описание банковских угроз для конкретной кредитной организации;	потенциально уязвимые места банка со стороны криминальных угроз;
ПК 2.4 Проводить операции на рынке межбанковских кредитов.	использовать правовые нормы в целях защиты интересов банка;	роль и место правовых актов органов государственной власти, Банка России и внутренних нормативных актов банка в обеспечении безопасности банковской деятельности;

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Объем дисциплины и виды работы

Вид работы	*Объем часов*
Максимальная учебная нагрузка (всего)	**26**
Обязательная аудиторная учебная нагрузка (всего)	***26***
в том числе:	
лекции (уроки)	*20*
практические занятия	*6*
Самостоятельная работа обучающегося (всего)	
Промежуточная аттестация в форме контрольной работы в VI семестре	

2.2. Тематический план и содержание дисциплины

Очная форма обучения

Наименование разделов и тем	**Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся**	**Объе**	**Осваиваемые элементы компетенций**
1	2	3	4
Раздел 1. Концепция безопасности банка		**10**	
Тема 1.1. Основные положения концепции безопасности банка. Объект и субъект банковской безопасности.	**Содержание учебного материала**		ОК 1, ОК 2-11, ПК 1.1-ПК 1.5, ПК 2.1, ПК 2.4.
	Основные положения концепции безопасности банка Объект и субъект банковской безопасности.	2	
Тема 1.2. Правовые и организационные основы безопасности. Политика безопасности банка	**Содержание учебного материала**		ОК 1, ОК 2-11, ПК 1.1-ПК 1.5, ПК 2.1, ПК 2.4.
	Правовые и организационные основы безопасности Политика безопасности банка	2	
Тема 1.3. Классификация угроз. Матрица угроз	**Содержание учебного материала**		ОК 1, ОК 2-11, ПК 1.1-ПК 1.5, ПК 2.1, ПК 2.4.
	Классификация угроз. Матрица угроз	2	
Тема 1.4. Мошенничество. Виды мошенничества.	**Содержание учебного материала**	**2**	ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.3, ПК 4.4.
	Мошенничество. Виды мошенничества.		

Тематическое тестирование по разделу 1		**2**	
Раздел 2. Особенности обеспечения банковской безопасности		**16**	
Тема 2.1. Особенности обеспечения информационной безопасности в различных автоматизированных банковских системах	**Содержание учебного материала**		
	Информационная безопасность Автоматизированные банковские системы	2	ОК 1, ОК 2-11, ПК 1.1-ПК 1.5, ПК 2.1, ПК 2.4.
Тема 2.2. Охранная деятельность банка	**Содержание учебного материала**		ОК 1, ОК 2-11, ПК 1.1-ПК 1.5, ПК 2.1, ПК 2.4.
	Охранная деятельность банка Нормативная документация	2	
Тема 2.3. Информация, использующаяся в целях обеспечения безопасности банка, и ее источники	**Содержание учебного материала**		ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.3, ПК3.1 ПК 4.4.
	Информация, использующаяся в банке, и ее источники Конфиденциальная информация Банковская тайна	2	
Тема 2.4. Бюро кредитных историй	**Содержание учебного материала**		ОК 1, ОК 2-11, ПК 1.1-ПК 1.5, ПК 2.1, ПК 2.4.
	Бюро кредитных историй Пользователи информации	2	
Тема 2.5. Хищения денежных средств при	**Содержание учебного материала**		ОК 1, ОК 2-11, ПК 1.1-

совершении кредитных операций	Хищения денежных средств при совершении кредитных операций. Особенности.	2	ПК 1.5, ПК 2.1, ПК 2.4.
Тема 2.6. Хищения денежных средств банка в сфере расчетно-кассового обслуживания	**Содержание учебного материала**		ОК 1, ОК 2-11, ПК 1.1-ПК 1.5, ПК 2.1, ПК 2.4.
	Хищения денежных средств банка в сфере расчетно-кассового обслуживания. Особенности.	2	
Тема 2.7. Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем	**Содержание учебного материала**		ОК 1, ОК 2-11, ПК 1.1-ПК 1.5, ПК 2.1, ПК 2.4.
	Понятие легализации (отмывания) доходов, полученных преступным путем. ФЗ-115 Обязанности банков по ФЗ-115	2	
Итоговая контрольная работа		**2**	
	ИТОГО:	**26**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ, ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Фонд оценочных средств (далее – ФОС) - комплект методических и контрольных материалов, используемых при проведении текущего контроля освоения результатов обучения и промежуточной аттестации. ФОС предназначен для контроля и управления процессом приобретения обучающимися необходимых знаний, умений, практического опыта и компетенций, определенных во ФГОС (Приложение № 2).

4. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета дисциплин права.

Оборудование учебного кабинета: учебная мебель, доска.

4.2. Учебно-методическое и информационное обеспечение дисциплины (модуля)

4.2.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная учебная литература:

1. Банковское дело в 2 ч. Часть 1 : учебник для СПО / Н. Н. Мартыненко, О. М. Маркова, О. С. Рудакова, Н. В. Сергеева ; под ред. Н. Н. Мартыненко. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2022. — 217 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-09422-0. – Режим доступа: https://biblio-online.ru/book/bankovskoe-delo-v-2-ch-chast-1-437007
2. Банковское дело в 2 ч. Часть 2 : учебник для СПО / Н. Н. Мартыненко, О. М. Маркова, О. С. Рудакова, Н. В. Сергеева. — 2-е изд., испр. и доп. — М.: Издательство Юрайт, 2018. — 368 с. — (Серия: Профессиональное образование). — ISBN 978-5-534-08471-9. – Режим доступа: https://biblio-online.ru/book/bankovskoe-delo-v-2-ch-chast-1-437007
3. Информационные технологии в экономике : учебное пособие для СПО / О. Ю. Нетёсова. — 3-е изд., испр. и доп. — М.: Издательство Юрайт, 2022. — 178 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-09107-6. – Режим доступа:

Дополнительная учебная литература:

1. Гамза, В. А. Безопасность банковской деятельности : учебник для академического бакалавриата / В. А. Гамза, И. Б. Ткачук, И. М. Жилкин. — 4-е изд., пер. и доп. — М. : Издательство Юрайт, 2022. — 432 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-08166-4.

4.2.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), необходимых для освоения дисциплины (модуля)

Перечень договоров ЭБС и БД			
Учебный год		**Наименование документа с указанием реквизитов**	**Срок действия документа**
2023/2024	1	Договор на доступ к ЭБС ZNANIUM.COM между УУНиТ в лице директора СФ УУНиТ и ООО «Знаниум»№ 1151-эбс от 11.07.2023	С 12.07.2023 по 11.07.2024
	2	Договор на доступ к ЭБС ZNANIUM.COM между УУНиТ в лице директора СФ УУНиТ и ООО «Знаниум»№ 223/801 от 23.08.2023 (предоставление доступа к коллекции ЭФУ «Федеральный перечень учебников издательства «Провещение»	С 28.08.2023 по 31.12.2024
	3	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между УУНиТ в лице директора СФ УУНиТ и ООО «Электронное издательство ЮРАЙТ» № 1/23-эбс от 03.03.2023	С 04.03.2023 по 02.03.2024
	4	Договор на доступ к ЭБС «Университетская библиотека онлайн» между БашГУ и «Нексмедиа» № 223-950 от 05.09.2022	С 01.10.2022 по 30.09.2023
	5	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-948 от 05.09.2022	С 01.10.2022 по 30.09.2023
	6	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-949 от 05.09.2022	С 01.10.2022 по 30.09.2023
	7	Соглашение о сотрудничестве между БашГу и издательством «Лань» № 5 от 05.09.2022	С 01.10.2022 по 30.09.2023
	8	ЭБС «ЭБ БашГУ», бессрочный договор между БашГУ и ООО «Открытые библиотечные системы» № 095 от 01.09.2014 г.	бессрочный
	9	Договор на доступ к электронным изданиям в составе базы данных «НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU» между УУНиТ и ООО НЭБ № SU- 20179 /2023 от 28.03.2023	С 28.03 2023 по 31.12.2023
	10	Договор на БД диссертаций между УУНиТ и РГБ № 223-997 от 11.07.2023	С 11.08.2023 по 10.08.2024
	11	Договор о подключении к НЭБ и о предоставлении доступа к объектам НЭБ между БашГУ в лице директора СФ БашГУ с ФГБУ «РГБ» № 101/НЭБ/1438-П от 11.06.2019	С 11.06.2019 по 10.06.2024

4.2.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Наименование программного обеспечения
Office Standard 2007 Russian OpenLicensePack NoLevel Acdmc
КонсультантПлюс
Microsoft Windows 7 Professional

5. ИНЫЕ СВЕДЕНИЯ И (ИЛИ) МАТЕРИАЛЫ

5.1. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине

Активные и интерактивные формы проведения занятий

Активные и интерактивные формы проведения занятий реализуются при подготовке по программам среднего профессионального образования и предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и студенты) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуации в атмосфере делового сотрудничества, оптимальной для выработки навыков и качеств будущего профессионала.

Основные преимущества активных и интерактивных форм проведения занятий:

- активизация познавательной и мыслительной деятельности студентов;
- усвоение студентами учебного материала в качестве активных участников;
- развитие навыков рефлексии, анализа и критического мышления;
- усиление мотивации к изучению дисциплины и обучению в целом;
- создание благоприятной атмосферы на занятии;
- развитие коммуникативных компетенций у студентов;
- развитие навыков владения современными техническими средствами и технологиями обработки информации;
- формирование и развитие способности самостоятельно находить информацию и определять уровень ее достоверности;
- использование электронных форм, обеспечивающих четкое управление учебным процессом, повышение объективности оценки результатов обучения студентов;
- приближение учебного процесса к условиям будущей профессиональной деятельности.

Активные и интерактивные формы учебных занятий могут быть использованы при проведении лекций, практических и лабораторных занятий, выполнении курсовых проектов (работ), при прохождении практики и других видах учебных занятий.

Использование активных и интерактивных форм учебных занятий позволяет осуществлять оценку усвоенных знаний, сформированности умений и навыков, компетенций в рамках процедуры текущего контроля по дисциплине (междисциплинарному курсу, профессиональному модулю), практике.

Активные и интерактивные формы учебных занятий реализуются преподавателем согласно рабочей программе учебной дисциплины (профессионального модуля) или программе практики.

Дискуссия – это публичное обсуждение или свободный вербальный обмен знаниями, суждениями, идеями или мнениями по поводу какого-либо спорного вопроса, проблемы. Ее существенными чертами являются сочетание взаимодополняющего диалога и обсуждения-спора, столкновение различных точек зрения, позиций.

Возможности метода групповой дискуссии:

- участники дискуссии с разных сторон могут увидеть проблему, сопоставляя противоположные позиции;
- уточняются взаимные позиции, что, уменьшает сопротивление восприятию новой информации;
- в процессе открытых высказываний устраняется эмоциональная предвзятость в оценке позиции партнеров и тем самым нивелируются скрытые конфликты;
- вырабатывается групповое решение со статусом групповой нормы;

- можно использовать механизмы возложения и принятия ответственности, увеличивая включенность участников дискуссии в последующую реализацию групповых решений;

- удовлетворяется потребность участников дискуссии в признании и уважении, если они проявили свою компетентность, и тем самым повышается эффективность их отдачи и заинтересованность в решении групповой задачи.

Основные функции преподавателя при проведении дискуссии:

- формулирует проблему и тему дискуссии, дает их рабочие определения;

- создает необходимую мотивацию, показывает значимость проблемы для участников дискуссии, выделяет в ней нерешенные и противоречивые моменты, определяет ожидаемый результат;

- создает доброжелательную атмосферу;

- формулирует вместе с участниками правила ведения дискуссии;

- добивается однозначного семантического понимания терминов и понятий;

- способствует поддержанию высокого уровня активности всех участников, следит за соблюдением регламента и темы дискуссии;

- фиксирует предложенные идеи на плакате или на доске, чтобы исключить повторение и стимулировать дополнительные вопросы;

- участвует в анализе высказанных идей, мнений, позиций; подводит промежуточные итоги, чтобы избежать движения дискуссии по кругу.

- обобщает предложения, высказанные группой, и подытоживает все достигнутые выводы и заключения;

- сравнивает достигнутый результат с исходной целью.

При проведении дискуссии могут использоваться различные организационные формы занятий.

Разбор конкретных ситуаций (кейс-метод). Метод кейсов представляет собой изучение, анализ и принятие решений по ситуации, которая возникла в результате происшедших событий, реальных ситуаций или может возникнуть при определенных обстоятельствах в конкретной организации в тот или иной момент времени.

Цели использования кейс-метода:

- развитие навыков анализа и критического мышления;

- соединение теории и практики;

- представление примеров принимаемых решений и их последствий;

- демонстрация различных позиций и точек зрения;

- формирование навыков оценки альтернативных вариантов в условиях неопределенности.

Метод разбора конкретных ситуаций может быть представлен такими своими разновидностями как решение ситуационных задач, выполнение ситуационных упражнений, кейс-стадии, метод «инцидента» и проч.

При разработке содержания кейсов (конкретных ситуаций) следует соблюдать следующие требования к учебному кейсу:

- Кейс должен опираться на знания основных разделов дисциплины, а не каких-то частностей.

- Кейс должен содержать текстовый материал (описание) и другие виды подачи информации (таблицы, графики, диаграммы, иллюстрации и т. п.).

- Кейс не должен содержать прямой формулировки проблемы.

- Кейс должен быть написан профессиональным языком, но в интересной для чтения форме.

- Кейс должен быть основан на реальных материалах, но названия компаний, товаров, географических мест и т. п. сведения могут быть изменены. Об этом должно быть сказано в сноске к описанию кейса. 3.6.5. Рекомендуется следующая структура кейса:

1. Описание ситуации.

2. Дополнительная информация в виде форм отчетности, статистических и аналитических таблиц, графиков, диаграмм, исторических справок о компании, списка источников и любой другой информации, которая нужна для анализа ситуации.

3. Методическая записка (1–2 стр.), содержащая как рекомендации для студента, анализирующего кейс, так и для преподавателя, который организует обсуждение кейса.

4. Перечень вопросов, которые должны помочь студентам понять его основное содержание, сформулировать проблему и соотнести проблему с соответствующими разделами учебной дисциплины.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Стерлитамакский филиал

Колледж

Календарно-тематический план

по дисциплине ***ОП.16 Безопасность банковской деятельности***

специальность

38.02.07 ***Банковкое дело***

код наименование специальности

квалификация

специалист банковского дела

Разработчик (составитель)
преподаватель 1 категории
Пименова С.С.
ученая степень, ученое звание,
категория, Ф.И.О.

Стерлитамак 2023

6 семестр					
№ п/п	**Наименование разделов и тем**	**Кол-во часов**	**Календарные сроки изучения (план)**	**Вид занятия**	**Домашнее задание**
Раздел 1. Концепция безопасности банка					
1.	Основные положения концепции безопасности банка. Объект и субъект банковской безопасности.	2/2	Сентябрь	лекция	Повторить пройденное
2.	Правовые и организационные основы безопасности. Политика безопасности банка	2/4	Сентябрь	лекция	Повторить пройденное
3.	Классификация угроз. Матрица угроз.	2/6	Ноябрь	лекция	Составить тест
4.	Мошенничество. Виды мошенничества.	2/8	Декабрь	лекция	Составить схему виды мошенничества
5.	Тематическое тестирование по разделу 1	2/10	Декабрь	практическое занятие	Повторить пройденное
Раздел 2. Особенности обеспечения банковской безопасности					
6.	Особенности обеспечения информационной безопасности в различных автоматизированных банковских системах	2/12	Январь	практическое занятие	Повторить пройденное, составить схемы
7.	Охранная деятельность банка	2/14	Февраль	лекция	Изучение нормативных документов
8.	Информация, использующаяся в целях обеспечения безопасности банка, и ее источники	2/16	март	лекция	Повторить пройденное
9.	Бюро кредитных историй	2/18	март	лекция	Работа с сайтом
10.	Хищения денежных средств при	2/20	март	лекция	Повторить пройденное

	совершении кредитных операций				
11.	Хищения денежных средств банка в сфере расчетно-кассового обслуживания	2/22	март	лекция	Составить таблицы-схемы
12.	Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем	2/24	март	практическое занятие	Изучение Фз-115
13.	**Итоговая контрольная работа**	2/26	апрель		
Всего часов		26			

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Стерлитамакский филиал

Колледж

Фонд оценочных средств

по дисциплине ***ОП.16 Безопасность банковской деятельности***

Общепрофессиональный цикл, обязательная часть

цикл дисциплины и его часть (обязательная, вариативная)

специальность

38.02.07 ***Банковское дело***

код наименование специальности

квалификация

специалист банковского дела

Разработчик (составитель)
преподаватель первой категории
Пименова С.С.
ученая степень, ученое звание,
категория, Ф.И.О.

Стерлитамак 2023

1. Паспорт фондов оценочных средств

1. Область применения

Фонд оценочных средств (ФОС) предназначен для проверки результатов освоения дисциплины «безопасность банковской деятельности», входящей в состав программы подготовки специалистов среднего звена по специальности 38.02.07 Банковское дело. Объем часов на аудиторную нагрузку по дисциплине 84, на самостоятельную работу 34, на консультации 12 часов.

2. Объекты оценивания – результаты освоения дисциплины

ФОС позволяет оценить следующие результаты освоения дисциплины в соответствии с ФГОС специальности право и организация социального обеспечения и рабочей программой дисциплины семейное право:

умения:

составлять системное описание банковских угроз для конкретной кредитной организации;

рассчитывать по принятой методологии основные технико-экономические показатели деятельности организации;

принимать эффективные решения, используя систему методов управления

применять в профессиональной деятельности приемы и методы эффективного делового общения;

использовать правовые нормы в целях защиты интересов банка;

выявлять типичные признаки преступных посягательств;

выполнять задачи по организации деятельности структурных подразделения системы безопасности;

делать выбор конкретных устройств, предназначенных для охраны банка и защиты банковских операций и продуктов;

оформлять документацию в соответствии с нормативной базой, используя информационные технологии и средства оргтехники;

выявлять типичные признаки преступных посягательств;

выявлять типичные признаки преступных посягательств;

составлять системное описание банковских угроз для конкретной кредитной организации;

использовать правовые нормы в целях защиты интересов банка.

знания:

потенциально уязвимые места банка со стороны криминальных угроз;

организацию производственного и технологического процессов;

особенности организации управления в банковских учреждениях;

сущность и основные виды коммуникаций;

роль и место правовых актов органов государственной власти, Банка России и внутренних нормативных актов банка в обеспечении безопасности банковской деятельности;

способы совершения хищений в процессе кредитных операций и т.п.;

структуру системы безопасности кредитных организаций, порядок формирования, цели и задачи системы безопасности банка;

виды технических средств обеспечения безопасности банка и их назначение;

основные понятия документационного обеспечения управления;

способы совершения хищений в процессе кредитных операций и т.п.;

виды рисков в сфере вексельного обращения, типичные неправомерного завладения векселями;

потенциально уязвимые места банка со стороны криминальных угроз;

роль и место правовых актов органов государственной власти, Банка России и внутренних нормативных актов банка в обеспечении безопасности банковской деятельности;

Вышеперечисленные умения, знания направлены на формирование у обучающихся следующих **общих и профессиональных компетенций**:

ОК. 02 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес

ОК.3 Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность

ОК. 04 Осуществлять поиск и использование информации, необходимой для эффективности выполнения профессиональных задач, профессионального и личностного развития

ОК. 07 Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК. 08

Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации

ОК. 10 Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий

ОК. 11 Знать правила техники безопасности, нести ответственность за организацию мероприятий по обеспечению безопасности труда

ПК 1.1 Осуществлять расчетно-кассовое обслуживание клиентов

ПК 1.2 Осуществлять безналичные платежи с использованием различных форм расчетов в национальной и иностранной валютах.

ПК 1.3 Осуществлять расчетное обслуживание счетов бюджетов различных уровней.

ПК 1.4 Осуществлять межбанковские расчеты.

ПК 1.5 Осуществлять международные расчеты по экспортно-импортным операциям.

ПК 2.1 Оценивать кредитоспособность клиентов.

ПК 2.4 Проводить операции на рынке межбанковских кредитов.

3. Формы контроля и оценки результатов освоения дисциплины

Контроль и оценка результатов освоения – это выявление, измерение и оценивание знаний, умений и формирующихся общих и профессиональных компетенций в рамках освоения дисциплины.

В соответствии с учебным планом специальности право и организация социального обеспечения, рабочей программой дисциплины семейное право предусматривается текущий и промежуточный контроль результатов освоения.

3.1 Формы текущего контроля

Текущий контроль успеваемости представляет собой проверку усвоения учебного материала, регулярно осуществляемую на протяжении курса обучения.

Текущий контроль результатов освоения дисциплины в соответствии с рабочей программой и календарно-тематическим планом происходит при использовании следующих обязательных форм контроля:

– выполнение и защита и практических работ,

- проверка выполнения самостоятельной работы студентов,

- проверка выполнения контрольных работ,

Во время проведения учебных занятий дополнительно используются следующие формы текущего контроля – устный опрос, решение задач, тестирование по темам отдельных занятий.

Выполнение и защита практических работ. Практические работы проводятся с целью усвоения и закрепления практических умений и знаний, овладения компетенциями. В ходе практической работы студенты приобретают умения, предусмотренные рабочей

программой дисциплины, учатся анализировать полученные результаты и делать выводы, опираясь на теоретические знания.

Список практических работ:

II семестр

Практическая работа № 1

Задание: Проанализировать причины совершения и дать характеристику наиболее характерным преступлениям в банковской сфере России

Алгоритм решения задания:

1 Составить кластер «Классификация преступлений в банковской сфере России»

2 Составить таблицу «Насильственные преступления в отношении персонала и имущества банков»

3 Составить таблицу «Финансовые преступления в сфере банковской деятельности»

4 По материалам периодических изданий и сайтов Интернет подготовить доклад о совершенном преступлении в банковской сфере

Практическая работа № 2

Задание: Провести анализ защищенности конфиденциальной банковской информации

Алгоритм решения задания

1 Составить таблицу «Меры по защите конфиденциальной информации, предпринимаемые в банке»

2 По материалам периодических изданий и сайтов Интернет подготовить доклад о последствиях утечки конфиденциальной банковской информации

Практическая работа № 3

Задание: Провести анализ проблем безопасности электронных платежей и банковских платежных карт

Алгоритм решения задания

1 Составить таблицу Способы мошенничества с пластиковыми картами

2 По материалам периодических изданий и сайтов Интернет подготовить доклад о проблемах безопасности электронных платежей и банковских платежных карт

Практическая работа № 4

Задание: Провести анализ механизма взаимодействия с органами МВД в обеспечении безопасности банка

Алгоритм решения задания

1 С помощью системы КонсультантПлюс изучить как Уголовный Кодекс РФ регулирует отношения по поводу обеспечения безопасности банка путем установления уголовно-правовой охраны от преступлений

2 С помощью системы КонсультантПлюс изучить Соглашение между МВД России и Ассоциацией российских банков о взаимодействии в области обеспечения банковской безопасности и рассмотреть основные направления такого взаимодействия

Практическая работа № 5

Задание: Провести анализ действия службы безопасности и сотрудников банка в кризисных ситуациях

Алгоритм решения задания

1 Составить перечень возможных кризисных ситуаций в банковской деятельности

2 По материалам периодических изданий и сайтов Интернет подготовить доклад о действиях службы безопасности и сотрудников банка в кризисных ситуациях

Практическая работа № 6

Задание: Изучить инженерно-технические средства охраны, средства самозащиты, специальный транспорт

Алгоритм решения задания

1 составить кластер «Классификация технических средств защиты банковской тайны»
2 По материалам периодических изданий и сайтов Интернет подготовить доклад о современных технических средствах защиты банковской тайны

Практическая работа № 7

Задание №1. Сотрудник отдела безопасности банка принимает решение о возможности выдачи кредита физическому лицу. Частный клиент предоставил справку с места работы о среднемесячном доходе в размере 178 000 рублей. Как проверить работнику отдела безопасности финансово-кредитной организации достоверность информации, содержащейся в справке клиента?

Задание №2. Мошенник желает осуществить операцию покупки, расплатившись в торгово-сервисном предприятии картой, подделанной путём перекодирования информации, содержащейся на магнитном носителе (внешние реквизиты и данные магнитного носителя не совпадают). Каким образом кассовой сотрудник торгово-сервисной точки может узнать, что карта поддельная?

Практическая работа № 8

Задание №1. Клиент проводит операцию по оплате налоговых платежей, которую он совершает наличными деньгами на общую сумму 56 000 рублей. При введении сотрудником кредитной организации идентификационных данных клиента в программу банка по проведению платежей, машина высветила информацию, что данный клиент находится в списках экстремистов и террористов. Какие должны последовать за этим действия операционнокассового сотрудника банка?

Задание №2. С каким кодом(ами) обязательного контроля подлежит отправки в Федеральную службу по финансовому мониторингу следующая операция: Физическое лицо открывает обезличенный металлический счёт в золоте, при этом в кассу банка он вносит не слитки, а 780 000 рублей.

Практическая работа № 9

Задание №1. У сотрудника банка по работе с клиентами возникли сомнения относительно подлинности платёжного поручения на списание денежных средств со счёта юридического лица, предоставленного в банк. Какие дальнейшие действия должны последовать со стороны операционно-кассового сотрудника?

Практическая работа № 10

Проблема Мошенники изобрели массу способов изъятия денег с чужой банковской карты. Как в современных условиях максимально обезопасить свои средства?

Задание Составьте десять правил пластиковой безопасности.

Практическая работа № 11

1. Бюро кредитных историй и их роль в обеспечении безопасности банка.
2. Понятие финансовой безопасности коммерческого банка и ее составляющие.
3. Организация противодействия (легализации) отмыванию доходов, полученных преступным путем и финансированию терроризма.
4. Вольфсбергские принципы финансовой безопасности банка.

Проверка выполнения самостоятельной работы. Самостоятельная работа направлена на самостоятельное освоение и закрепление обучающимися практических умений и знаний, овладение профессиональными компетенциями.

Самостоятельная подготовка обучающихся по дисциплине предполагает следующие виды и формы работы:

- *Систематическая проработка конспектов занятий, учебной и специальной литературы.*
- *Самостоятельное изучение материала и конспектирование лекций по учебной и специальной литературе.*

Проверка выполнения контрольных работ. Контрольная работа проводится с целью контроля усвоенных умений и знаний и последующего анализа типичных ошибок и затруднений обучающихся в конце изучения темы или раздела. Согласно календарно-тематическому плану дисциплины предусмотрено проведение следующих контрольных работ:

Контрольная работа № 1

1. Безопасность – это:
   а) Специфическая совокупность внешних и внутренних условий деятельности, позволяющих субъекту контролировать процесс собственного существования и достигать намеченных целей указанной деятельности;
   б) Источник потенциального ущерба имуществу или инфраструктуре банка, причинение которого может воспрепятствовать достижению банка установленных целей;
   в) Мера допустимо опасных условий деятельности банка, неблагоприятные последствия которых реализуются в связи с ошибочными действиями или бездействием персонала банка.
2. По экономическому характеру угрозы делятся на:
   а) Потенциальные, реализуемые угрозы;
   б) Угрозы со стороны конкурентов, со стороны персонала банка;
   в) Угрозы имущественного и неимущественного характера.
3. К важной для банка информации относится:
   а) Незаменимая информация, утечка или разрушение которой ставят под угрозу само функционирование кредитной организации;
   б) Информация, утечка или разрушение которой наносит материальный ущерб кредитной организации, однако она может эффективно функционировать и после этого;
   в) Информация, процесс ликвидации последствий утечки или разрушения которой сложен или связан с большими затратами.
4. Для банков ориентированных на обслуживание высокорентабельных предприятий (отраслей), наиболее целесообразным вариантом стратегии обеспечение собственной безопасности является:
   а) Стратегия «упреждающего противодействия»;
   б) Стратегия «адекватного противодействия»;
   в) Стратегия «пассивной защиты».
5. Деятельность отдела собственной безопасности в составе службы безопасности банка направлен на контроль:
   а) высших руководителей банка;
   б) сотрудников самой службы безопасности;
   в) эффективности управления безопасностью банка в целом.
6. В обучении новых сотрудников банка правилам обеспечения его безопасности должны принимать участие:
   а) Сотрудники службы безопасности;
   б) Сотрудники службы персонала;
   в) Руководители их структурных подразделений;
   г) Все перечисленные выше специалисты банка.
7. При нападении на банк персоналу необходимо:
   а) Не выполнять все требования нападавших, так как они влекут за собой впоследствии банкротство банка;
   б) Выполнять абсолютно все требования нападавших, даже если они влекут за собой впоследствии банкротство банка;
   в) Действовать на своё усмотрение.

8. Задачи обеспечения безопасности БИС в локальных или глобальных вычислительных сетях:
   а) Обеспечение сохранности информации, как в памяти ЭВМ, так и на отдельных носителях;
   б) Защита информации от несанкционированного доступа;
   в) Обеспечение достоверности, идентификации и сохранности информации при ее передаче по каналам связи;

9. Коммерческая тайна – это:
   а) Информация по счетам или вкладам своих клиентов и корреспондентов;
   б) Любая информация, обеспечивающая достижение преимуществ над конкурентами и извлечение прибыли;
   в) Информация об объемах и структуре предоставленных и полученных кредитов и депозитов.
10. Механизм электронной цифровой подписи реализует функции:
   а) Шифрование, сертификация;
   б) Аутентификация, шифрование;
   в) Сертификация, аутентификация.
11. Промышленный шпионаж – это:
   а) получение обманным путем конфиденциальной информации, используемой в различных противоправных целях;
   б) уголовно наказуемое и иное противоправное деяние, посягающее на имущественные и приравненные к ним права и интересы банка либо на порядок его функционирования;
   в) присвоение кредитов по фиктивным банковским гарантиям подставными фирмами.
12. Внутренняя безопасность включает:
   а) Регламентацию доступа пользователей и обслуживающего персонала к информации системы;
   б) Защиту от несанкционированного доступа к информации;
   в) Защиту от случайных внешних воздействий;
13. Криптография – это:
   а) Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности;
   б) Реквизит электронного документа, предназначенный для защиты данного документа от модификации;
   в) Наука о методах обеспечения конфиденциальности и аутентичности информации.
14. Какая концепция предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз:
   а) Стратегия адекватного ответа;
   б) Стратегия пассивной защиты;
   в) Упреждающего противодействия.
15. Финансовые махинации относятся к … преступлениям в банковской сфере:
   б) насильственным;
   в) «беловоротничковым»;

г) Экономическим.

II вариант

1. Внешняя безопасность включает:
   а) Регламентацию доступа пользователей и обслуживающего персонала к информации системы;
   б) Защиту от несанкционированного доступа к информации;
   в) Регламентацию доступа пользователей и обслуживающего персонала к ресурсам системы.
2. По признаку целевой направленности угрозы делятся на:
   а) Угроза разглашения конфиденциальной информации, угроза имуществу банка;
   б) Угрозы со стороны конкурентов и со стороны криминальных структур;
   в) Угрозы имущественного характера и неимущественного характера.
3. Что относится к организационно-управленческой информации, которая входит в состав коммерческой тайны:
   а) Источники и объёмы финансирования и кредитования;
   б) Базы данных по клиентам;
   в) Базы данных о ведущих специалистов банка.
4. Главным элементом криптосистемы считаются:
   а) Алгоритмы шифрования;
   б) Методы распространения ключей к этим шифрам;
   в) Обе группы указанных элементов в равной степени.
5. К насильственным преступлениям в банковской сфере относятся:
   а) Грабежи;
   б) Финансовые хищения;
   в) Махинации
6. К «беловоротничковым» преступлениям в банковской сфере относятся:
   а) Грабежи;
   б) Финансовые хищения;
   в) Налёты на обменные пункты.
7. Налёты на обменные пункты относятся к … преступлениям в банковской сфере:
   а) насильственным;
   б) «беловоротничковым»;
   в) Экономическим.
8. Аутентификация – это:
   а) Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности;
   б) Реквизит электронного документа, предназначенный для защиты данного документа от модификации;
   в) Наука о методах обеспечения конфиденциальности и аутентичности информации.
9. К полезной банковской информации относится:
   а) Незаменимая информация, утечка или разрушение которой ставят под угрозу само функционирование кредитной организации;
   б) Информация, утечка или разрушение которой наносит материальный ущерб кредитной организации, однако она может эффективно функционировать и после этого;
   в) Информация, процесс ликвидации последствий утечки или разрушения которой сложен или связан с большими затратами.
10. Данные составляющие банковскую тайну:
   а) Объёмы инвестиций, планы маркетинга;
   б) Базы данных об акционерах и специалистах;

в) Информация банковского вклада, операций по счёту и сведений о клиенте.

11. Какая концепция предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз:

а) Стратегия адекватного ответа;
б) Стратегия пассивной защиты;
в) Упреждающего противодействия.

12 . Задача проведения анализа уязвимости информационной банковской системы:

а) Рассмотрение всех возможных угроз и оценка размеров возможного ущерба;
б) Определение всех возможных слабых мест информационной банковской системы;
в) Регламентация деятельности кредитной организации.

13. При реализации, какой концепции допускаются банковский шпионаж, не всегда легитимные методы контроля:

а) Стратегия адекватного ответа;
б) Стратегия пассивной защиты;
в) Упреждающего противодействия.

14. Задачи обеспечения безопасности БИС в локальных или глобальных вычислительных сетях:

а) Обеспечение сохранности информации, как в памяти ЭВМ, так и на отдельных носителях;
б) Обеспечение достоверности, идентификации и сохранности информации при ее передаче по каналам связи;
в) Защита информации от несанкционированного доступа;

15. По вероятности практической реализации угрозы делятся на:

а) Имущественного и неимущественного характера;
б) Угрозы со стороны нелояльных сотрудников и конкурентов;
в) Потенциальные и реализованные угрозы.

Контрольная работа № 2

I вариант

1. Что включает в себя безопасность банковской деятельности?
   1) привлечение потенциальных опасностей
   2) отсутствие опасностей
   3) поступление информации от потребителей
   4) нет верного ответа
2. Угрозы финансовых ресурсов проявляются в виде:
   1) не возврата кредитных сумм, хищения финансовых средств из банкомата и инкассаторских машин
   2) нападения, вторжения, захвата
   3) вымогательства значительных сумм денежных средств, льгот перед лицом террористической угрозы
   4) обстрела из огнестрельного оружия
3. По характеру воздействия угрозы классифицируют на:
   1) вероятные, весьма вероятные, маловероятные
   2) стихийные, преднамеренные
   3) предельные, значительные, незначительные
   4) активные, пассивные
4. Субъектами правоотношений при решении проблемы безопасности являются:
   1) государство

2) юридические и физические лица
3) службы безопасности банков и частные охранные структуры
4) верны все ответы

5. Что НЕ относится к экономическому преступлению?
1) хищение финансовых и материальных средств
2) изготовление поддельных денег
3) обман потребителей
4) рекламирование своей продукции
6. Что НЕ относится к основной деятельности по обеспечению безопасности банка?
1) безопасность персонала
2) безопасность информационных ресурсов
3) сохранность и физическая защита материальных и финансовых средств и объектов
4) подбор и расстановка кадров
7. Что НЕ относится к преступлению в сфере экономики?
1) преступление против собственности
2) преступление против чести, свободы и достоинства
3) заведомо ложная реклама
4) незаконное предпринимательство
8. Безопасность - это...
1) наука, которую надо изучать
2) наука, которую надо развивать
3) искусство, которое надо постигать
4) наука, которую надо изучать и развивать, искусство, которое надо постигать, культура, которую надо воспитывать у предпринимателей
9. К видам негативных воздействий злоумышленников относятся:

1) экономическое подавление
2) физическое подавление
3) экономическое, физическое, финансовое, информационное, психи-ческое подавление
4) нет верного ответа
10. Ущерб от угроз бывает:
1) материальный и моральный
2) физический
3) психологический
4) интеллектуальный
11. Финансовые средства, материальные ценности и новейшие технологии - это…
1) субъекты безопасности
2) объекты безопасности
3) органы безопасности
4) задачи безопасности
12. Безопасность на рынке финансов - это...
1) основа бизнеса
2) состояние защищенности
3) обеспечение устойчивости финансирования
4) охрана руководителей
13. Преступные посягательства (угрозы) совершают в целях…
1) собственной выгоды
2) получения материального и морального удовлетворения
3) нанесения ущерба

4) создания служб безопасности для сокращения безработицы

14. Мошенничество - это...

1) форма хищения по средствам насилия или убийства с целью завладения заведомо чужим имуществом

2) одно из преступлений против личности, наносящее вред здоровью личности

3) одно из преступлений против собственности, одна из форм хищения, представляющая собой завладение чужим имуществом путём обмана или злоупотреблением доверием

4) нет верного ответа

15. Способами мошенничества являются:

1) злоупотребление доверием, разбой

2) нападение, разбой

3) обман, нападение

4) обман, злоупотребление доверием

II вариант

1. Источниками мошенничества являются:

1) форс-мажорные обстоятельства

2) законопослушные граждане

3) хакеры

4) нет верного ответа

2. К внутренним условиям мошенничества можно отнести:

1) недоверчивость

2) некомпетентность, безответственность

3) несовершенство личности

4) все ответы верны

3. К каким источникам опасности относят следующие объекты: подкуп персонала, перехват сообщений, съём информации со специальной аппаратуры?

1) к персоналу

2) к конкурентам

3) к недобросовестным контрагентам

4) к техногенным катастрофам

4. Что относится к психологическому давлению злоумышленников?

1) угрозы и шантаж

2) сокращение производства

3) мошенничество

4) устранение сотрудников и руководства

5. К какому виду преступлений относится данная характеристика: операционные системы, системы управления базами данных, пароли?

1) подмена

2) кража

3) перехват информации

4) уничтожение

6. Действия злоумышленников могут быть:

1) параллельные

2) вертикальные, горизонтальные

3) международные

4) внешние и внутренние

7. Политика безопасности банка представляет собой:

1) непрерывность

2) экономность

3) систему взглядов (мер, решений)

4) нет верного ответа

8. К финансовым преступлениям в сфере банковской деятельности относят:
    1) лжекредитование
    2) залог
    3) страховку
    4) консалтинг
9. К основным приёмам деятельности преступных группировок относят:
    1) террор
    2) саботаж
    3) сращивание экономической и уголовной преступности
    4) нет верного ответа
10. В классификации источников внутренних угроз банка выделяют:
    1) финансовые преступления
    2) организованную преступность
    3) шпионаж
    4) нет верного ответа
11. Обеспечение экономической безопасности банка является прерогативой…
    1) Министерства Внутренних Дел
    2) Федеральной службы безопасности
    3) Министерства финансов
    4) администрации банка
12. Правовое регулирование коммерческой безопасности распространяется на:
    1) банки
    2) торговые точки
    3) спецфонды
    4) благотворительные организации
13. Обеспечение личной безопасности банковских служащих является задачей:
    1) прокуратуры
    2) милиции
    3) самих банковских служащих
    4) нет верного ответа
14. К видам безопасности относят:
    1) залог
    2) гарантию
    3) страховку
    4) геобиофизическую, техническую, общественную безопасность
15. К угрозам банковской безопасности по объекту посягательства относятся:
    1) политические угрозы
    2) криминальные угрозы
    3) информационные угрозы
    4) нет верного ответа

Контрольная работа № 3

I вариант

1. Какие реквизиты должны содержать защищенные документы?
    1) регистрационный номер, товарный знак
    2) название фирмы
    3) дату создания документа
    4) основные реквизиты
2. К числу преступлений в компьютерной сфере относят:
    1) аппаратные сбои
    2) перегрузку

3) перехват информации
4) вирусы

3. К защите банковской информации в автоматизированной системе обработки относят:
1) моральную, политическую, производственную ответственность граждан
2) технологические приобретения, установку и использование защит-ных средств от различного рода воздействий технических средств обработки информации
3) персонал
4) новейшие технологии

4. К видам угроз утечки информации при автоматизированной обработке относят:
1) банковскую тайну
2) профессиональную тайну
3) отказы и сбои в работе аппаратуры
4) нет верного ответа

5. К основным техническим каналам утечки банковской информации относят:
1) разговорный
2) телефонный
3) электромагнитный
4) нет верного ответа

6. Обеспечение информационной безопасности банковских систем достигается путём:
1) факса
2) электронных платежей
3) телефона
4) ксерокса

7. Какой разновидности пластиковых карт нет?
1) интеллектуальных
2) кредитных
3) дебетовых
4) клиринговых

8. Уязвимые места защиты в системах обмена электронными данными (ОЭД):
1) пересылка платёжных и других сообщений между банками или между банком и клиентом
2) обработка информации внутри организаций отправителя и получателя
3) доступ клиента к средствам, аккумулированным на счёте
4) все ответы верны

9. Что НЕ относится к угрозам безопасности по принципу воздействия на автоматизированную систему обработки информации банка?
1) использование доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т.д.)
2) использование закрытых каналов связи
3) использование открытых каналов связи
4) воздействие на систему разрешений (в т.ч. захват привилегий)

10. Укажите угрозы безопасности автоматизированной системы обработки информации банка по способу воздействия на объект атаки:
1) непосредственное воздействие на объект атаки
2) воздействие на систему разрешений (в том числе захват привилегий)
3) опосредованное воздействие (через других пользователей)
4) все ответы верны

11. Какие типы PIN- кодов существуют?
1) назначаемые выведенные
2) назначаемые случайные
3) выбираемые пользователем
4) все ответы верны

12. Идентификация клиента с использованием PIN-кодов работает в случаях:
    1) отсутствия перехвата карточки
    2) воровства банковских карточек
    3) невозможности доступа к системе другим пользователем
    4) все ответы верны
13. Что произойдет при вводе неверного PIN-кода?
    1) "самоблокировка" карточки
    2) включение сигнализации
    3) автоматическое уничтожение карточки
    4) нет верного ответа
14. Недостаток интеллектуальной карточки:
    1) низкая стоимость производства карточки
    2) уменьшенная по сравнению со стандартом толщина карточки и объём информации
    3) высокий процент за обслуживание
    4) увеличенная по сравнению со стандартом толщина карточки и высокая стоимость производства карточки
15. Что НЕ относится к защите пластиковой карточки?
    1) торговое имя продукта
    2) вокруг панели расположена кайма печатных кодов идентификации банка
    3) поле fine-line в области идентификации продукции
    4) трехмерная голограмма голубя

II вариант

1. Задачи автоматического кассового аппарата:
    1) идентификация и аутентификация клиента
    2) выдача наличных денег
    3) оповещение о состоянии счета клиента
    4) все ответы верны
2. К эмитенту карточки предъявляются требования:
    1) карточка должна восприниматься вручную
    2) карточка не должна обладать технологией проверки собственных обменных PIN-кодов
    3) карточка не должна соответствовать правильности PIN-кодов
    4) карточка должна восприниматься автоматически и обладать техно-логией проверки собственных обменных PIN-кодов
3. Виды защиты информации:
    1) средства физической защиты
    2) программные средства
    3) административные меры защиты
    4) все ответы верны
4. Что относится к угрозам конфиденциальной информации в нарушении конфиденциальности?
    1) разглашение
    2) утечка
    3) НСД (несанкционированный доступ)
    4) все ответы верны
5. Что относится к угрозам конфиденциальной информации в нарушении доступности?
    1) изменение информации
    2) закрытый доступ получения информации
    3) нарушение связи, запрет получения информации
    4) нет верного ответа
6. Разглашение конфиденциальной информации проявляется в виде:

1) сообщения (передачи, предоставления)
2) пересылки
3) опубликования
4) все ответы верны

7. К факторам и обстоятельствам, способствующим утечке конфиденциальной информации относится:

1) недостаточное знание сотрудником правил защиты конфиденциальной информации и непонимание необходимости их тщательного соблюдения
2) использование неаттестованных технических средств обработки конфиденциальной информации
3) слабый контроль за соблюдением правил защиты информации право-выми, организационными и инженерно-техническими мерами
4) все ответы верны

8. Источники угроз несанкционированного доступа:

1) конкуренты
2) преступники
3) административные органы
4) верны все ответы

9. Утечка конфиденциальной информации - это…

1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним
3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений
4) нет верного ответа

10. Разглашение - это…

1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним
3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений
4) нет верного ответа

11. Несанкционированный доступ - это…

1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним
3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений
4) нет верного ответа

12. В какой форме оформляется обязательство о неразглашении конфиденциальной информации при переводе сотрудника на другую работу, связанную с конфиденциальной информацией, а так же при увольнении сотрудника?

1) в письменном
2) в устном
3) по усмотрению службы безопасности
4) нет правильного ответа

13. К угрозам информационных ресурсов относится:
1) разглашение конфиденциальной информации
2) подслушивание конфиденциальных переговоров в служебных помеще-ниях
3) подлог платёжных документов и пластиковых карт
4) информационно-психологическое воздействие
14. Правовой основой банковского бизнеса служит:
1) страхование
2) залог
3) закон "О банках и банковской деятельности"
4) нет верного ответа
15. Правовая основа защиты конфиденциальной банковской информации базируется на:
1) депозитах
2) кредитах
3) банковской тайне (профессиональной тайне)
4) нет верного ответа

Контрольная работа № 4

1. По характеру защитных мероприятий инженерно-технические средства защиты классифицируются:
1) организационные, системные, банковские
2) организационные, технические, организационно-технические
3) технические, банковские, внебанковские
4) организационные, инженерные
2. Какие виды защиты информации используются в линиях связи?
1) магнитные преобразования информации
2) незащищенные волоконно-оптические линии связи
3) жучки
4) криптографические преобразования информации и защищенные волоконно-оптические линии связи
3. Инкассаторская автомашина НЕ отвечает требованиям:
1) бронированная защита кузова
2) улучшенные ходовые характеристики
3) двери кабины водителя и кузова имеют специальные внутренние запорные устройства
4) звукоизоляция кузова
4. На какие группы подразделяются технические средства защиты?
1) средства труда, оборотные средства
2) средства оповещения, средства первой медицинской помощи
3) средства охраны, средства защиты информации
4) нет верного ответа
5. Какие из перечисленных средств относятся к информационной безопасности компьютерных сетей?
1) управляющая электроника и программное обеспечение
2) средства учёта и контроля автотранспорта
3) антикражная система
4) биометрические средства защиты информации
6. К инженерно-техническим средствам защиты относятся:
1) сейфы и оборудование банковских хранилищ, банкоматы и др.
2) транкинговые системы
3) средства производственной и пожарной информатики

4) информационные системы

7. Какие технологии средства НЕ относятся к системам связи и оповещения?

1) транкинговые системы

2) профессиональные, носимые, мобильные и базовые радиостанции

3) учрежденческие АТС, системы конференц-связи

4) аварийно-спасательная техника

8. Какие технологические средства относятся к системам связи и оповещения?

1) сейфы и специальные шкафы

2) оборудование банковских хранилищ

3) системы тревожного оповещения

4) пожарная техника

9. Услуги, средства поддержки и обслуживания систем безопасности…

1) системы бесперебойного питания и автономные энергоустановки

2) суда, катера и другие плавсредства

3) транкинковые системы

4) специальная одежда, обувь и обмундирование

10. Вход для клиентов оборудуется следующими техническими средствами:

1) учрежденческими АТС

2) специальными сетями связи и информационными системами

3) кнопкой тревожной сигнализации, устройствами дистанционного управления, входными и выходными дверями

4) монтажным оборудованием и инструментом

11. Входной тамбур и место дежурства сотрудника охраны должны быть оборудовано следующими техническими средствами:

1) телефонным аппаратом прямой связи с центральным пунктом охраны, кнопкой тревожной сигнализации, датчиком открывания дверей

2) аварийно-спасательным инструментом

3) оборудованием для специальных автомобилей, судами, катерами и другими плавсредствами

4) контрольно- измерительной аппаратурой

12. Зона кассиров должна иметь следующие технические средства:

1) автомобили для перевозки денежных средств и ценностей

2) кнопку тревожной сигнализации (ручную или ножную) телекамеру, датчики открытия, закрытия дверей

3) оборудование для специальных автомобилей

4) обнаружители наркотических средств, металлодетекторы

13. Защита от перехвата побочных, электромагнитных измерений и наводок самого различного характера обеспечивается…

1) экранированием помещений средств канальных коммуникаций, использованием автономных телефонных систем, локальных систем ЭВМ, не имеющих выхода за пределы охраняемой территории и др.

2) аварийно-спасательной техникой, оборудованием для специальных автомобилей

3) системой вентиляции и кондиционированием воздуха, контрольно-измерительной аппаратурой

4) страхованием и детективной деятельностью, физической охраной объектов

14. К антитеррористическому и досмотровому оборудованию относятся:

1) стенографические средства защиты и передачи информации

2) металлодетекторы, рентгеновское оборудование, системы радиационного мониторинга, обнаружители наркотических веществ

3) автоматизированные системы управления интеллектуальным зданием, комплекс систем информации

4) автоматизированные средства защиты

15. Кризисная ситуация - это…

1) проявление факторов угроз со стороны отдельных лиц или групп
2) слабость в средствах защиты, вызванная ошибками или слабостями в процедурах, проекте, реализации, внутреннем контроле системы, которая может быть использована для проникновения в систему
3) проявление факторов угроз со стороны массовых групп
4) нет верного ответа

II вариант

1. Что НЕ относится к принципам организации и функционирования системы безопасности?

1) непрерывность
2) своевременность
3) бесконечность
4) нет верного ответа

2. Комплексный принцип организации и функционирования системы безопас-ности подразумевает:

1) защиту интересов банка с достаточной степенью настойчивости, широко используемую силу, средства обеспечения безопасности и нестандартные методы защиты
2) обеспечение безопасности персонала, материальных, финансовых ресурсов от возможных угроз всеми доступными законными средствами, мерами и мероприятиями
3) совершенствование мер и средств защиты на основе собственного опыта, появление новых технических средств с учетом изменения методов и средств разведки и промышленного шпионажа
4) привлечение к разработке и внедрению средств защиты специализиро-ванных органов

3. Главные цели системы безопасности:

1) обеспечение устойчивого функционирования банка и предотвращение угроз по безопасности
2) защита законных интересов от противоправных посягательств, охраны жизни и здоровья персонала и недопущение хищения финансовых и материально-технических средств

3) обеспечение неустойчивости функционирования банка
4) нет верного ответа

4. На какой правовой нормативный акт необходимо опираться при практичес-ком решении задач обеспечения безопасности банка?

1) на устав банка
2) на приказ руководителя банка
3) на заявление физического лица
4) на положение о государственной системе защиты информации от инженерно-технических работ и от утечки

5. К основным задачам службы безопасности относится:

1) выявление и локализация возможных каналов утечки конфиден-циальной информации, обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания
2) информация о порядке работы с иностранными представителями
3) безопасность информационных ресурсов
4 безопасность персонала

6. Кто возглавляет службу безопасности в банке?

1) начальник в должности заместителя руководителя банка по безопасности
2) руководитель банка
3) начальник отдела безопасности
4) нет верного ответа

7. В службу безопасности НЕ входит следующая структурная служба:

1) подразделение обновления системы
2) подразделение режима и охраны
3) подразделение инженерно-технической защиты
4) подразделение информационно-аналитической деятельности

8. Что НЕ относится к действиям частных детективов?

1) защита жизни и здоровья граждан
2) наведение справок
3) внешний осмотр строений, помещений
4) слежка за объектами

9. Для чего предназначена охранная система?

1) для ограничения круга лиц, имеющих доступ к документам, обеспечения оптимального режима пользования теми лицами, кому они доверены
2) для ограничения круга лиц, имеющих доступ к документам
3) для обеспечения оптимального режима к информации
4) для охраны жизни и здоровья членов семей работников банка

10. К основным кризисным ситуациям в работе банков относят:

1) взятие заложников
2) забастовку
3) демонстрацию
4) нет верного ответа

11. При каких условиях органам предварительного следствия предоставляется информация, составляющая банковскую тайну?

1) с согласия руководителя банка
2) с согласия прокурора и клиента банка
3) с согласия клиента банка
4) по возбуждённым уголовным делам и с согласия прокурора

12. Кому выдаются справки по счетам и вкладам физических лиц банком?

1) клиенту
2) суду

3) органам предварительного следствия по делам, находящимся в их производстве, с согласия прокурора

4) все ответы верны

13. Система безопасности - это…

1) организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих, защиту жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз

2) финансовые мероприятия по защите информации с целью минимизации рисков утраты или изменения информации и уменьшения страхового возмещения

3) финансовые мероприятия по защите населения

4) нет верного ответа

14. Основными элементам системы безопасности банка являются:

1) ответственный руководитель системы и клиенты банка

2) совет безопасности и клиенты банка

3) ответственный руководитель системы и совет безопасности банка

4) нет верного ответа

15. На основе каких организационно-правовых документов действует система безопасности?

1) устава банка

2) положения о системе безопасности

3) руководства по защите конфиденциальной информации

4) верны все ответы

Сводная таблица по применяемым формам и методам текущего контроля и оценки результатов обучения

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Освоенные умения:	
- оказывать правовую помощь с целью восстановления нарушенных прав;	устный опрос; мониторинг роста творческой активности и самостоятельности
- анализировать и решать юридические проблемы в сфере правовых отношений.	практические задания; экспертная оценка выполнения практической работы
Усвоенные знания:	
- основные понятия и источники частного права;	устный опрос тестирование
- содержание основных институтов частного права.	Устный опрос практические задания;

3.2 Форма промежуточной аттестации

Промежуточная аттестация по дисциплине «Безопасность банковской деятельности» в форме итоговой контрольной работы в V и VI семестре.

ЗАДАНИЯ К ИТОГОВОЙ КОНТРОЛЬНОЙ РАБОТЕ ПО ДИСЦИПЛИНЕ «РИМСКОЕ ПРАВО» ЗА V СЕМЕСТР

I вариант

1. Что включает в себя безопасность банковской деятельности?

1) привлечение потенциальных опасностей
2) отсутствие опасностей
3) поступление информации от потребителей
4) нет верного ответа

2. Угрозы финансовых ресурсов проявляются в виде:
1) не возврата кредитных сумм, хищения финансовых средств из банкомата и инкассаторских машин
2) нападения, вторжения, захвата
3) вымогательства значительных сумм денежных средств, льгот перед лицом террористической угрозы
4) обстрела из огнестрельного оружия

3. По характеру воздействия угрозы классифицируют на:
1) вероятные, весьма вероятные, маловероятные
2) стихийные, преднамеренные
3) предельные, значительные, незначительные
4) активные, пассивные

4. Субъектами правоотношений при решении проблемы безопасности являются:
1) государство
2) юридические и физические лица
3) службы безопасности банков и частные охранные структуры
4) верны все ответы

5. Что НЕ относится к экономическому преступлению?
1) хищение финансовых и материальных средств
2) изготовление поддельных денег
3) обман потребителей
4) рекламирование своей продукции

6. Что НЕ относится к основной деятельности по обеспечению безопасности банка?
1) безопасность персонала
2) безопасность информационных ресурсов
3) сохранность и физическая защита материальных и финансовых средств и объектов
4) подбор и расстановка кадров

7. Что НЕ относится к угрозам безопасности по принципу воздействия на автоматизированную систему обработки информации банка?
1) использование доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т.д.)
2) использование закрытых каналов связи
3) использование открытых каналов связи
4) воздействие на систему разрешений (в т.ч. захват привилегий)

8. Укажите угрозы безопасности автоматизированной системы обработки информации банка по способу воздействия на объект атаки:
1) непосредственное воздействие на объект атаки

2) воздействие на систему разрешений (в том числе захват привилегий)
3) опосредованное воздействие (через других пользователей)
4) все ответы верны

9. Какие типы PIN- кодов существуют?
1) назначаемые выведенные
2) назначаемые случайные
3) выбираемые пользователем
4) все ответы верны

10. Идентификация клиента с использованием PIN-кодов работает в случаях:
1) отсутствия перехвата карточки
2) воровства банковских карточек
3) невозможности доступа к системе другим пользователем
4) все ответы верны

11. Что НЕ относится к преступлению в сфере экономики?
1) преступление против собственности
2) преступление против чести, свободы и достоинства
3) заведомо ложная реклама
4) незаконное предпринимательство

12. Безопасность - это...
1) наука, которую надо изучать
2) наука, которую надо развивать
3) искусство, которое надо постигать
4) наука, которую надо изучать и развивать, искусство, которое надо постигать, культура, которую надо воспитывать у предпринимателей

13. К видам негативных воздействий злоумышленников относятся:
1) экономическое подавление
2) физическое подавление
3) экономическое, физическое, финансовое, информационное, психическое подавление
4) нет верного ответа

14. Ущерб от угроз бывает:
1) материальный и моральный
2) физический
3) психологический
4) интеллектуальный

15. Финансовые средства, материальные ценности и новейшие технологии - это…
1) субъекты безопасности
2) объекты безопасности
3) органы безопасности
4) задачи безопасности

16. Безопасность на рынке финансов - это...
1) основа бизнеса
2) состояние защищенности

3) обеспечение устойчивости финансирования
4) охрана руководителей

17. Преступные посягательства (угрозы) совершают в целях…
1) собственной выгоды
2) получения материального и морального удовлетворения
3) нанесения ущерба
4) создания служб безопасности для сокращения безработицы

18. Мошенничество - это...
1) форма хищения по средствам насилия или убийства с целью завладения заведомо чужим имуществом
2) одно из преступлений против личности, наносящее вред здоровью личности
3) одно из преступлений против собственности, одна из форм хищения, представляющая собой завладение чужим имуществом путём обмана или злоупотреблением доверием
4) нет верного ответа

19. Способами мошенничества являются:
1) злоупотребление доверием, разбой
2) нападение, разбой
3) обман, нападение
4) обман, злоупотребление доверием

20. Источниками мошенничества являются:
1) форс-мажорные обстоятельства
2) законопослушные граждане
3) хакеры
4) нет верного ответа

21. Принципы коммерческой тайны:
1) соответствующая информация не известна третьим лицам
2) нет свободного доступа к информации на законном основании
3) собственник информации принимает меры обеспечения конфиденциаль-ности
4) все ответы верны

22. Что относится к угрозам конфиденциальной информации в нарушении достоверности?
1) фальсификация
2) подделка
3) мошенничество
4) все ответы верны

23. Что НЕ относится к угрозам конфиденциальной информации в нарушении целостности?
1) искажение
2) ошибки
3) потери
4) мошенничество

24. Что относится к угрозам конфиденциальной информации в нарушении конфиденциальности?

1) разглашение
2) утечка
3) НСД (несанкционированный доступ)
4) все ответы верны

25. Что относится к угрозам конфиденциальной информации в нарушении доступности?

1) изменение информации
2) закрытый доступ получения информации
3) нарушение связи, запрет получения информации
4) нет верного ответа

26. К внутренним условиям мошенничества можно отнести:

1) недоверчивость
2) некомпетентность, безответственность
3) несовершенство личности
4) все ответы верны

27. К каким источникам опасности относят следующие объекты: подкуп персонала, перехват сообщений, съём информации со специальной аппаратуры?

1) к персоналу
2) к конкурентам
3) к недобросовестным контрагентам
4) к техногенным катастрофам

28. Что относится к психологическому давлению злоумышленников?

1) угрозы и шантаж
2) сокращение производства
3) мошенничество
4) устранение сотрудников и руководства

29. К какому виду преступлений относится данная характеристика: операционные системы, системы управления базами данных, пароли?

1) подмена
2) кража
3) перехват информации
4) уничтожение

30. Действия злоумышленников могут быть:

1) параллельные
2) вертикальные, горизонтальные
3) международные
4) внешние и внутренние

II вариант

1. Политика безопасности банка представляет собой:

1) непрерывность

2) экономность
3) систему взглядов (мер, решений)
4) нет верного ответа

2. К финансовым преступлениям в сфере банковской деятельности относят:
1) лжекредитование
2) залог
3) страховку
4) консалтинг

3. К основным приёмам деятельности преступных группировок относят:
1) террор
2) саботаж
3) сращивание экономической и уголовной преступности
4) нет верного ответа

4. В классификации источников внутренних угроз банка выделяют:
1) финансовые преступления
2) организованную преступность
3) шпионаж
4) нет верного ответа

5. Обеспечение экономической безопасности банка является прерогативой…
1) Министерства Внутренних Дел
2) Федеральной службы безопасности
3) Министерства финансов
4) администрации банка

6. Правовое регулирование коммерческой безопасности распространяется на:
1) банки
2) торговые точки
3) спецфонды
4) благотворительные организации

7. Обеспечение личной безопасности банковских служащих является задачей:
1) прокуратуры
2) милиции
3) самих банковских служащих
4) нет верного ответа

8. К видам безопасности относят:
1) залог
2) гарантию
3) страховку
4) геобиофизическую, техническую, общественную безопасность

9. К угрозам банковской безопасности по объекту посягательства относятся:
1) политические угрозы
2) криминальные угрозы
3) информационные угрозы
4) нет верного ответа

10. Какое наказание предусмотрено за мошенничество?

1) лишение свободы на срок до 3 лет
2) лишение свободы на срок до 5 лет
3) лишение свободы на срок до 10 лет
4) нет верного ответа

11. Принципы коммерческой тайны:
1) соответствующая информация не известна третьим лицам
2) нет свободного доступа к информации на законном основании
3) собственник информации принимает меры обеспечения конфиденциаль-ности
4) все ответы верны

12. Что относится к угрозам конфиденциальной информации в нарушении достоверности?
1) фальсификация
2) подделка
3) мошенничество
4) все ответы верны

13. Что НЕ относится к угрозам конфиденциальной информации в нарушении целостности?
1) искажение
2) ошибки
3) потери
4) мошенничество

14. Что относится к угрозам конфиденциальной информации в нарушении конфиденциальности?
1) разглашение
2) утечка
3) НСД (несанкционированный доступ)
4) все ответы верны

15. Что относится к угрозам конфиденциальной информации в нарушении доступности?
1) изменение информации
2) закрытый доступ получения информации
3) нарушение связи, запрет получения информации
4) нет верного ответа

16. Разглашение конфиденциальной информации проявляется в виде:
1) сообщения (передачи, предоставления)
2) пересылки
3) опубликования
4) все ответы верны

17. К факторам и обстоятельствам, способствующим утечке конфиденциальной информации относится:
1) недостаточное знание сотрудником правил защиты конфиденциальной информации и непонимание необходимости их тщательного соблюдения

2) использование неаттестованных технических средств обработки конфи-денциальной информации

3) слабый контроль за соблюдением правил защиты информации право-выми, организационными и инженерно-техническими мерами

4) все ответы верны

18. Источники угроз несанкционированного доступа:

1) конкуренты

2) преступники

3) административные органы

4) верны все ответы

19. Утечка конфиденциальной информации - это…

1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена

2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним

3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений

4) нет верного ответа

20. Разглашение - это…

1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена

2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним

3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений

4) нет верного ответа

21. Несанкционированный доступ - это…

1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена

2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним

3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений

4) нет верного ответа

22. В какой форме оформляется обязательство о неразглашении конфиденциальной информации при переводе сотрудника на другую работу, связанную с конфиденциальной информацией, а так же при увольнении сотрудника?

1) в письменном
2) в устном
3) по усмотрению службы безопасности
4) нет правильного ответа

23. К угрозам информационных ресурсов относится:
1) разглашение конфиденциальной информации
2) подслушивание конфиденциальных переговоров в служебных помеще-ниях
3) подлог платёжных документов и пластиковых карт
4) информационно-психологическое воздействие

24. Правовой основой банковского бизнеса служит:
1) страхование
2) залог
3) закон "О банках и банковской деятельности"
4) нет верного ответа

25. Правовая основа защиты конфиденциальной банковской информации базируется на:
1) депозитах
2) кредитах
3) банковской тайне (профессиональной тайне)
4) нет верного ответа

26. Понятие и состав конфиденциальной тайны включает:
1) понятие банковской тайны
2) хищение кредитов
3) лжекредиты
4) нет верного ответа

27. Источниками утечки банковской информации является:
1) закон
2) указ
3) отсутствие персональной ответственности
4) нет верного ответа

28. Содержание банковской тайны:
1) банковский счёт
2) банковский вклад
3) операции по счетам и вкладам
4) все варианты

29. Какие реквизиты должны содержать защищенные документы?
1) регистрационный номер, товарный знак
2) название фирмы
3) дату создания документа
4) основные реквизиты

30. К числу преступлений в компьютерной сфере относят:
1) аппаратные сбои
2) перегрузку

3) перехват информации
4) вирусы

ЗАДАНИЯ К ИТОГОВОЙ КОНТРОЛЬНОЙ РАБОТЕ ПО ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ» ЗА VI СЕМЕСТР

1. Что НЕ относится к принципам организации и функционирования системы безопасности?
   1) непрерывность
   2) своевременность
   3) бесконечность
   4) нет верного ответа
2. Комплексный принцип организации и функционирования системы безопас-ности подразумевает:
   1) защиту интересов банка с достаточной степенью настойчивости, широко используемую силу, средства обеспечения безопасности и нестандартные методы защиты
   2) обеспечение безопасности персонала, материальных, финансовых ресурсов от возможных угроз всеми доступными законными средствами, мерами и мероприятиями
   3) совершенствование мер и средств защиты на основе собственного опыта, появление новых технических средств с учетом изменения методов и средств разведки и промышленного шпионажа
   4) привлечение к разработке и внедрению средств защиты специализиро-ванных органов
3. Главные цели системы безопасности:
   1) обеспечение устойчивого функционирования банка и предотвращение угроз по безопасности
   2) защита законных интересов от противоправных посягательств, охраны жизни и здоровья персонала и недопущение хищения финансовых и материально-технических средств
   3) обеспечение неустойчивости функционирования банка
   4) нет верного ответа
4. На какой правовой нормативный акт необходимо опираться при практичес-ком решении задач обеспечения безопасности банка?
   1) на устав банка
   2) на приказ руководителя банка
   3) на заявление физического лица
   4) на положение о государственной системе защиты информации от инженерно-технических работ и от утечки
5. К основным задачам службы безопасности относится:
   1) выявление и локализация возможных каналов утечки конфиден-циальной информации, обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания
   2) информация о порядке работы с иностранными представителями
   3) безопасность информационных ресурсов
   4 безопасность персонала
6. Кто возглавляет службу безопасности в банке?
   1) начальник в должности заместителя руководителя банка по безопасности
   2) руководитель банка
   3) начальник отдела безопасности

4) нет верного ответа

7. В службу безопасности НЕ входит следующая структурная служба:
1) подразделение обновления системы
2) подразделение режима и охраны
3) подразделение инженерно-технической защиты
4) подразделение информационно-аналитической деятельности

8. Что НЕ относится к действиям частных детективов?
1) защита жизни и здоровья граждан
2) наведение справок
3) внешний осмотр строений, помещений
4) слежка за объектами

9. Для чего предназначена охранная система?
1) для ограничения круга лиц, имеющих доступ к документам, обеспечения оптимального режима пользования теми лицами, кому они доверены
2) для ограничения круга лиц, имеющих доступ к документам
3) для обеспечения оптимального режима к информации
4) для охраны жизни и здоровья членов семей работников банка

10. К основным кризисным ситуациям в работе банков относят:
1) взятие заложников
2) забастовку
3) демонстрацию
4) нет верного ответа

11. При каких условиях органам предварительного следствия предоставляется информация, составляющая банковскую тайну?
1) с согласия руководителя банка
2) с согласия прокурора и клиента банка
3) с согласия клиента банка
4) по возбуждённым уголовным делам и с согласия прокурора

12. Кому выдаются справки по счетам и вкладам физических лиц банком?
1) клиенту
2) суду
3) органам предварительного следствия по делам, находящимся в их производстве, с согласия прокурора
4) все ответы верны

13. Система безопасности - это…
1) организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих, защиту жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз
2) финансовые мероприятия по защите информации с целью минимизации рисков утраты или изменения информации и уменьшения страхового возмещения
3) финансовые мероприятия по защите населения
4) нет верного ответа

14. Основными элементам системы безопасности банка являются:
1) ответственный руководитель системы и клиенты банка
2) совет безопасности и клиенты банка
3) ответственный руководитель системы и совет безопасности банка
4) нет верного ответа

15. На основе каких организационно-правовых документов действует система безопасности?
1) устава банка
2) положения о системе безопасности
3) руководства по защите конфиденциальной информации

4) верны все ответы

16. Кризисная ситуация - это…
    1) проявление факторов угроз со стороны отдельных лиц или групп
    2) слабость в средствах защиты, вызванная ошибками или слабостями в процедурах, проекте, реализации, внутреннем контроле системы, которая может быть использована для проникновения в систему
    3) проявление факторов угроз со стороны массовых групп
    4) нет верного ответа
17. Задачи кризисной группы:
    1) оценка безопасности
    2) принятие неотложных мер по безопасности
    3) управление деятельностью в экстренных условиях
    4) все ответы верны
18. Общие функции службы безопасности:
    1) обеспечение пропускного режима
    2) защита банковской тайны
    3) контроль требований по защите банковской тайны
    4) все ответы верны
19. Причины взаимодействия службы безопасности с правоохранительными органами:
    1) недостаток сил и средств службы безопасности
    2) ограниченность источников информации о криминальной обстановке
    3) сложность охраны транспортных перевозок материальных ценностей и финансовых средств
    4) все ответы верны
20. Какие реквизиты должны содержать защищенные документы?

    1) регистрационный номер, товарный знак
    2) название фирмы
    3) дату создания документа
    4) основные реквизиты
21. К числу преступлений в компьютерной сфере относят:
    1) аппаратные сбои
    2) перегрузку
    3) перехват информации
    4) вирусы

22. К защите банковской информации в автоматизированной системе обработки относят:
    1) моральную, политическую, производственную ответственность граждан
    2) технологические приобретения, установку и использование защит-ных средств от различного рода воздействий технических средств обработки информации
    3) персонал
    4) новейшие технологии
23. К видам угроз утечки информации при автоматизированной обработке относят:
    1) банковскую тайну
    2) профессиональную тайну
    3) отказы и сбои в работе аппаратуры
    4) нет верного ответа
24. К основным техническим каналам утечки банковской информации относят:
    1) разговорный
    2) телефонный
    3) электромагнитный
    4) нет верного ответа

25. Обеспечение информационной безопасности банковских систем достигается путём:
1) факса
2) электронных платежей
3) телефона
4) ксерокса
26. Какой разновидности пластиковых карт нет?
1) интеллектуальных
2) кредитных
3) дебетовых
4) клиринговых
27. Уязвимые места защиты в системах обмена электронными данными (ОЭД):
1) пересылка платёжных и других сообщений между банками или между банком и клиентом
2) обработка информации внутри организаций отправителя и получателя
3) доступ клиента к средствам, аккумулированным на счёте
4) все ответы верны
28. Что НЕ относится к угрозам безопасности по принципу воздействия на автоматизированную систему обработки информации банка?
1) использование доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т.д.)
2) использование закрытых каналов связи
3) использование открытых каналов связи
4) воздействие на систему разрешений (в т.ч. захват привилегий)
29. Укажите угрозы безопасности автоматизированной системы обработки информации банка по способу воздействия на объект атаки:
1) непосредственное воздействие на объект атаки
2) воздействие на систему разрешений (в том числе захват привилегий)
3) опосредованное воздействие (через других пользователей)
4) все ответы верны
30. Какие типы PIN- кодов существуют?
1) назначаемые выведенные
2) назначаемые случайные
3) выбираемые пользователем
4) все ответы верны

II вариант

1. Идентификация клиента с использованием PIN-кодов работает в случаях:
1) отсутствия перехвата карточки
2) воровства банковских карточек
3) невозможности доступа к системе другим пользователем
4) все ответы верны
2. Что произойдет при вводе неверного PIN-кода?
1) "самоблокировка" карточки
2) включение сигнализации
3) автоматическое уничтожение карточки
4) нет верного ответа
3. Недостаток интеллектуальной карточки:
1) низкая стоимость производства карточки
2) уменьшенная по сравнению со стандартом толщина карточки и объём информации
3) высокий процент за обслуживание
4) увеличенная по сравнению со стандартом толщина карточки и высокая стоимость производства карточки

4. Что НЕ относится к защите пластиковой карточки?

1) торговое имя продукта
2) вокруг панели расположена кайма печатных кодов идентификации банка
3) поле fine-line в области идентификации продукции
4) трехмерная голограмма голубя

5. Задачи автоматического кассового аппарата:

1) идентификация и аутентификация клиента
2) выдача наличных денег
3) оповещение о состоянии счета клиента
4) все ответы верны

6. К эмитенту карточки предъявляются требования:

1) карточка должна восприниматься вручную
2) карточка не должна обладать технологией проверки собственных обменных PIN-кодов
3) карточка не должна соответствовать правильности PIN-кодов
4) карточка должна восприниматься автоматически и обладать техно-логией проверки собственных обменных PIN-кодов

7. Виды защиты информации:

1) средства физической защиты
2) программные средства
3) административные меры защиты
4) все ответы верны

8. По характеру защитных мероприятий инженерно-технические средства защиты классифицируются:

1) организационные, системные, банковские
2) организационные, технические, организационно-технические
3) технические, банковские, внебанковские
4) организационные, инженерные

9. Какие виды защиты информации используются в линиях связи?

1) магнитные преобразования информации
2) незащищенные волоконно-оптические линии связи
3) жучки
4) криптографические преобразования информации и защищенные волоконно-оптические линии связи

10. Вход для клиентов оборудуется следующими техническими средствами:

1) учрежденческими АТС
2) специальными сетями связи и информационными системами
3) кнопкой тревожной сигнализации, устройствами дистанционного управления, входными и выходными дверями
4) монтажным оборудованием и инструментом

11. Входной тамбур и место дежурства сотрудника охраны должны быть оборудовано следующими техническими средствами:

1) телефонным аппаратом прямой связи с центральным пунктом охраны, кнопкой тревожной сигнализации, датчиком открывания дверей
2) аварийно-спасательным инструментом
3) оборудованием для специальных автомобилей, судами, катерами и другими плавсредствами
4) контрольно- измерительной аппаратурой

12. Зона кассиров должна иметь следующие технические средства:

1) автомобили для перевозки денежных средств и ценностей
2) кнопку тревожной сигнализации (ручную или ножную) телекамеру, датчики открытия, закрытия дверей

3) оборудование для специальных автомобилей

4) обнаружители наркотических средств, металлодетекторы

13. Защита от перехвата побочных, электромагнитных измерений и наводок самого различного характера обеспечивается…

1) экранированием помещений средств канальных коммуникаций, использованием автономных телефонных систем, локальных систем ЭВМ, не имеющих выхода за пределы охраняемой территории и др.

2) аварийно-спасательной техникой, оборудованием для специальных автомобилей

3) системой вентиляции и кондиционированием воздуха, контрольно-измерительной аппаратурой

4) страхованием и детективной деятельностью, физической охраной объектов

14. К антитеррористическому и досмотровому оборудованию относятся:

1) стенографические средства защиты и передачи информации

2) металлодетекторы, рентгеновское оборудование, системы радиа-ционного мониторинга, обнаружители наркотических веществ

3) автоматизированные системы управления интеллектуальным зданием, комплекс систем информации

4) автоматизированные средства защиты

15. Инкассаторская автомашина НЕ отвечает требованиям:

1) бронированная защита кузова

2) улучшенные ходовые характеристики

3) двери кабины водителя и кузова имеют специальные внутренние запорные устройства

4) звукоизоляция кузова

16. На какие группы подразделяются технические средства защиты?

1) средства труда, оборотные средства

2) средства оповещения, средства первой медицинской помощи

3) средства охраны, средства защиты информации

4) нет верного ответа

17. Какие из перечисленных средств относятся к информационной безопасности компьютерных сетей?

1) управляющая электроника и программное обеспечение

2) средства учёта и контроля автотранспорта

3) антикражная система

4) биометрические средства защиты информации

18. К инженерно-техническим средствам защиты относятся:

1) сейфы и оборудование банковских хранилищ, банкоматы и др.

2) транкинговые системы

3) средства производственной и пожарной информатики

4) информационные системы

19. Какие технологии средства НЕ относятся к системам связи и оповещения?

1) транкинговые системы

2) профессиональные, носимые, мобильные и базовые радиостанции

3) учрежденческие АТС, системы конференц-связи

4) аварийно-спасательная техника

20. Какие технологические средства относятся к системам связи и оповещения?

1) сейфы и специальные шкафы

2) оборудование банковских хранилищ

3) системы тревожного оповещения

4) пожарная техника

21. Услуги, средства поддержки и обслуживания систем безопасности…

1) системы бесперебойного питания и автономные энергоустановки

2) суда, катера и другие плавсредства
3) транкинковые системы
4) специальная одежда, обувь и обмундирование

22. Утечка конфиденциальной информации - это…
1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним
3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений
4) нет верного ответа

23. Разглашение - это…
1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним
3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений
4) нет верного ответа

24. Несанкционированный доступ - это…
1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним
3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений
4) нет верного ответа

25. В какой форме оформляется обязательство о неразглашении конфиденциальной информации при переводе сотрудника на другую работу, связанную с конфиденциальной информацией, а так же при увольнении сотрудника?
1) в письменном
2) в устном
3) по усмотрению службы безопасности
4) нет правильного ответа

26. К угрозам информационных ресурсов относится:
1) разглашение конфиденциальной информации
2) подслушивание конфиденциальных переговоров в служебных помеще-ниях
3) подлог платёжных документов и пластиковых карт
4) информационно-психологическое воздействие

27. Правовой основой банковского бизнеса служит:
1) страхование
2) залог
3) закон "О банках и банковской деятельности"
4) нет верного ответа

28. Правовая основа защиты конфиденциальной банковской информации базируется на:
1) депозитах
2) кредитах
3) банковской тайне (профессиональной тайне)
4) нет верного ответа

29. Понятие и состав конфиденциальной тайны включает:
1) понятие банковской тайны
2) хищение кредитов
3) лжекредиты
4) нет верного ответа
30. Источниками утечки банковской информации является:
1) закон
2) указ
3) отсутствие персональной ответственности
4) нет верного ответа

4 Система оценивания комплекта ФОС текущего контроля и промежуточной аттестации

При оценивании практической и самостоятельной работы студента учитывается следующее:

- качество выполнения практической части работы;

- качество оформления отчета по работе;

- качество устных ответов

Каждый вид работы оценивается по пяти бальной шкале.

«5» (отлично) – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся свободно и уверенно ориентируется; за умение практически применять теоретические знания, высказывать и обосновывать свои суждения. Оценка «5» (отлично) предполагает грамотное и логичное изложение ответа.

«4» (хорошо) – если обучающийся полно освоил учебный материал, владеет научно-понятийным аппаратом, ориентируется в изученном материале, осознанно применяет теоретические знания на практике, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности.

«3» (удовлетворительно) – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности, в применении теоретических знаний при ответе на практико-ориентированные вопросы; не умеет доказательно обосновать собственные суждения.

«2» (неудовлетворительно) – если обучающийся имеет разрозненные, бессистемные знания, допускает ошибки в определении базовых понятий, искажает их смысл; не может практически применять теоретические знания.

Критерии оценивания ответа по устному опросу.

«5» (отлично) – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся свободно и уверенно ориентируется; за умение практически применять теоретические знания, высказывать и обосновывать свои суждения; за грамотное и логичное изложение ответа.

«4» (хорошо) – если обучающийся полно освоил учебный материал, владеет научно-понятийным аппаратом, ориентируется в изученном материале, осознанно применяет теоретические знания на практике, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности.

«3» (удовлетворительно) – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в применении теоретических знаний при ответе на практико-

ориентированные вопросы; не умеет доказательно обосновать собственные суждения.

«2» (неудовлетворительно) – если обучающийся имеет разрозненные, бессистемные знания, допускает ошибки в определении базовых понятий, искажает их смысл; не может практически применять теоретические знания.

Критерии оценивания опорных конспектов.

«5» (отлично) – аккуратность выполнения, читаемость текста, грамотность (терминологическая и орфографическая), полное раскрытие темы конспекта.

«4» (хорошо) – тема конспекта раскрыта, однако материал изложен недостаточно логично; аккуратность выполнения, читаемость конспекта, грамотность (терминологическая и орфографическая).

«3» (удовлетворительно) – материал изложен недостаточно логично, неаккуратное выполнение, читаемость конспекта, грамотность (терминологическая и орфографическая), тема конспекта раскрыта не в полной мере.

«2» (неудовлетворительно) – материал изложен нелогично, допущены терминологические и орфографические ошибки, неразборчивый почерк, тема конспекта не раскрыта.

Критерии оценивания заданий по составлению таблиц.

«5» (отлично) – выполнены все требования по составлению таблицы: логически последовательно изложен весь необходимый материал; присутствует логическая последовательность в суждениях; оформлено эстетично и аккуратно; присутствует логически верный вывод.

«4» (хорошо) – основные требования к таблице выполнены, но при этом допущены недочёты, в частности, имеются неточности в изложении материала; имеются упущения в оформлении; отсутствует логически верный вывод.

«3» (удовлетворительно) – имеются существенные отступления от темы таблицы, в частности, тема освещена частично; допущены фактические ошибки в содержании; отсутствует логическая последовательность в суждениях; отсутствует вывод.

«2» (неудовлетворительно) – таблица не завершена, обнаруживается существенное непонимание ее темы.

Критерии оценивания заданий по составлению схем.

«5» (отлично) – выполнены все требования по составлению схемы: логически последовательно изложен весь необходимый материал; присутствует логическая последовательность построении элементов; оформлено эстетично и аккуратно.

«4» (хорошо) – основные требования к схеме выполнены, но при этом допущены недочёты, в частности, имеются неточности в изложении материала; имеются упущения в оформлении.

«3» (удовлетворительно) – имеются существенные отступления от темы схемы, в частности, тема освещена частично; отсутствует логическая последовательность построении элементов; допущены фактические ошибки в содержании элементов схемы.

«2» (неудовлетворительно) – схема не завершена, обнаруживается существенное непонимание ее темы.

Критерии оценивания заданий практических работ.

Практическая работа оценивается максимально оценкой «5» (отлично).

Каждое задание оценивается максимально оценкой «5» (отлично).

По результатам оценивания всех заданий оценка соответствует средней.

Критерии оценивания решений задач.

«5» (отлично) – составлен правильный алгоритм решения задачи, в логическом рассуждении, в выборе нормативных источников и решении нет ошибок, получен верный ответ, задача решена рациональным способом.

«4» (хорошо) – составлен правильный алгоритм решения задачи, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор нормативных источников; есть объяснение решения, но задача решена нерациональным

способом или допущено не более двух несущественных ошибок, получен верный ответ.

«3» (удовлетворительно) – задание выполнено, в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в выборе нормативных источников; задача решена не полностью или в общем виде.

«2» (неудовлетворительно) – задача решена неправильно.

Критерии оценивания заданий по составлению схемы.

«5» (отлично) – выполнены все требования по составлению схемы: логически последовательно изложен весь необходимый материал; присутствует логическая последовательность построении элементов; оформлено эстетично и аккуратно.

«4» (хорошо) – основные требования к схеме выполнены, но при этом допущены недочёты, в частности, имеются неточности в изложении материала; имеются упущения в оформлении.

«3» (удовлетворительно) – имеются существенные отступления от темы схемы, в частности, тема освещена частично; отсутствует логическая последовательность построении элементов; допущены фактические ошибки в содержании элементов схемы.

«2» (неудовлетворительно) – схема не завершена, обнаруживается существенное непонимание ее темы.

Критерии оценивания заданий по составлению таблиц.

«5» (отлично) – выполнены все требования по составлению таблицы: логически последовательно изложен весь необходимый материал; присутствует логическая последовательность в суждениях; оформлено эстетично и аккуратно; присутствует логически верный вывод.

«4» (хорошо) – основные требования к таблице выполнены, но при этом допущены недочёты, в частности, имеются неточности в изложении материала; имеются упущения в оформлении; отсутствует логически верный вывод.

«3» (удовлетворительно) – имеются существенные отступления от темы таблицы, в частности, тема освещена частично; допущены фактические ошибки в содержании; отсутствует логическая последовательность в суждениях; отсутствует вывод.

«2» (неудовлетворительно) – таблица не завершена, обнаруживается существенное непонимание ее темы.

Критерии оценивания тестовых заданий контрольных работ.

«5» (отлично) – 30 верных ответов (100%).

«4» (хорошо) – 22-29 верных ответов (75%-95%).

«3» (удовлетворительно) – 15-21 верных ответов (50%-70%).

«2» (неудовлетворительно) – менее 15 верных ответов (менее 50%).