Приложение 7. ОП ВО

Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ФАКУЛЬТЕТ ФИНАНСОВ И БАНКОВСКОГО ДЕЛА
(наименование структурного подразделения (института/факультета/филиала)
Кафедра «Фондовые рынки и финансовый инжиниринг»
(наименование кафедры)

УТВЕРЖДЕНА
Кафедрой «Фондовые рынки и финансовый инжиниринг»
Факультета финансов и банковского дела
Протокол от «04» сентября 2019 г.
№5

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.02.01 «Информационная безопасность и защита банковской тайны»

(индекс, наименование дисциплины , в соответствии с учебным планом)

38.04.08 Финансы и кредит

(код, наименование направления подготовки (специальности)

"Денежно-кредитное и финансовое регулирование экономики"

(направленность(и) (профиль (и)/специализация(ии)

Магистр
(квалификация)

Очная/очно-заочная/заочная
(форма(ы) обучения)

Год набора: 2020

Москва, 2019 г.

Автор–составитель:
к.и.н., доцент кафедры «Фондовые рынки и финансовый инжиниринг»
Козлов Е.С.

Заведующий кафедрой
«Фондовые рынки и финансовый инжиниринг» д.э.н., проф. Корищенко К.Н.

СОДЕРЖАНИЕ

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

1.1. Дисциплина Б1.В.ДВ.02.01 «Информационная безопасность и защита банковской тайны» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-5	Способность на основе комплексного экономического и финансового анализа дать оценку результатов и эффективности финансово-хозяйственной деятельности организаций различных организационно-правовых форм, включая финансово-кредитные, органов государственной власти и местного самоуправления	ПК-5.2	Способность оценивать результаты банковской деятельности, проводить комплексный анализ цифрового банкинга с использованием IT.
ДПК-4	Способность применять методы анализа и информационного обеспечения управления финансовыми рисками; владеть способами снижения финансовых рисков; применять методы маркетинговых исследований для изучения рынка банковских, финансовых, инвестиционных продуктов и услуг; способностью анализировать и использовать различные источники информации на иностранном языке для своей практической деятельности и представлять результат проведенного исследования в виде презентации, мини-презентации, доклада или статьи	ДПК-4.2	Способность применять методы анализа и информационного обеспечения управления финансовыми рисками в банковском деле.

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ (при наличии профстандарта)	Код этапа освоения компетенции	Результаты обучения
ПС «Специалист по	ПК-5.2	**на уровне знаний**

управлению рисками»: ОТФ Обеспечение эффективной работы системы управления рисками (B) (ч.). ТФ Разработка системы управления рисками (B/04.7) (ч.).	ДПК-4.2	Национальные и международные акты, стандарты, лучшие практики по построению систем управления рисками
		На уровне умений Адаптировать элементы системы риск-менеджмента к условиям функционирования организации, а также новым бизнес-процессам и направлениям Анализировать и применять методики оценки управления рисками и реагирования на риски Владеть программным обеспечением (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) для работы с информацией на уровне продвинутого пользователя
		На уровне навыков Построение модели корпоративной системы управления рисками, включающей общую конфигурацию системы, общую схему управления рисками, принципы организационно-функциональной структуры и информационного обмена
ПС «Специалист по платежным системам» ОТФ Управление разработкой, внедрением, эксплуатацией и модернизацией информационных систем для автоматизации операций в платежной системе (ее части) (F) (ч.); ТФ Формирование требований к разработке и внедрению информационной системы для автоматизации операций в платежной системе (ее части) (F/01.7) (ч.); ТФ Формирование требований к интеграции информационной	ПК-5.2 ДПК-4.2	**на уровне знаний** Современные инструментальные средства представления информации Анализ последних мировых тенденций в области развития платежных сервисов и инструментов Анализ возможностей и подготовка предложений по модернизации платежных сервисов и инструментов в составе информационной системы
		На уровне умений Анализировать технические возможности интеграции информационной системы с платежными сервисами и инструментами Формулировать требования к информационной системе в целом Формулировать требования к функциям (задачам), выполняемым информационной системой Формулировать задания по устранению выявленных недостатков для специалистов - разработчиков информационной системы Владеть различными методами и инструментами получения информации Оценивать достоверность полученной информации Работать с большими объемами информации Анализировать полученную информацию

системы с платежными сервисами и инструментами (F/02.7) (ч.); ТФ Участие в тестировании и приемке информационной системы для автоматизации операций в платежной системе (ее части) (F/03.7) (ч.); ТФ Обеспечение эксплуатации и модернизации информационной системы для автоматизации операций в платежной системе (ее части) (F/04.7);		**На уровне навыков** Анализ возможностей интеграции информационной системы с платежными сервисами и инструментами Подготовка технического задания на разработку и внедрение информационной системы для автоматизации операций в платежной системе (ее части) Формирование требований по устранению недостатков, выявленных в процессе тестирования информационной системы
ПС Специалист по финансовому консультированию ОТФ Управление процессом финансового консультирования в организации (подразделении) (C) ТФ Разработка методологии и стандартизация процесса финансового консультирования и финансового планирования (C/01.7)	ПК-5.2 ДПК-4.2	**на уровне знаний** согласование позиций и выработка единых подходов по вопросам регламентации процесса финансового консультирования совместно с другими подразделениями организации и внешними финансовыми консультантами
		На уровне умений оценивать ресурсные затраты, необходимые для обеспечения эффективного внедрения и функционирования процесса финансового консультирования - анализировать и выносить суждение о применимости методик финансового планирования для отдельных категорий клиентов - оценивать ресурсные затраты на внедрение и функционирование аппаратно-информационной составляющей процесса финансового консультирования
		На уровне навыков создание методологии финансового консультирования финансового планирования; - утверждение методик по финансовому парированию, методик определения инвестиционного профиля клиентов внедрение единой методологии финансового планирования Установление требований к функционированию аппаратно-информационного обеспечения

		процесса финансового консультирования и финансового планирования

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Дисциплина Б1.В.ДВ.02.01 «Информационная безопасность и защита банковской тайны» составляет 2 зачетные единицы, т.е. 72 академических часа.

Для студентов очной и очно-заочной формы обучения на контактную работу с преподавателем выделено 16 часов из них 8 часов лекций и 8 часов практических занятий, на самостоятельную работу обучающихся выделено 56 часов. Для студентов заочной формы обучения на контактную работу с преподавателем выделено 12 часов, из них 4 часа лекций и 8 часов практических занятий, на самостоятельную работу обучающихся выделено 58 часов, в том числе 2 часа на контроль самостоятельной работы.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.02.01 «Информационная безопасность и защита банковской тайны» изучается на 2 курсе, в 3 семестре студентами очной и очно-заочной формы обучения; студентами заочной формы обучения изучается на 2 курсе.

Дисциплина Б1.В.ДВ.02.01 «Информационная безопасность и защита банковской тайны» реализуется после изучения дисциплин бакалавриата.

Форма промежуточной аттестации в соответствии с учебным планом - зачет.

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины , час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРС	
			Л	ЛР	ПЗ	КСР		
Тема 1	Основы информационной безопасности	8	2				6	
Тема 2	Угрозы информационной безопасности в банковской сфере	9	2		1		6	*Р, Дис, ПЗ*
Тема 3	Информационная безопасность коммерческого банка	7			1		6	*Дис. ПЗ*
Тема 4	Основные методы и технические средства промышленного шпионажа	8	2				6	

Тема 5	Система информационной безопасности банка	9			1		8	*Дис. ПЗ*
Тема 6	Требования к информационной безопасности банка	9			1		8	*Дис. ПЗ*
Тема 7	Проверка и оценка информационной безопасности банка	10			2		8	*Дис. ПЗ*
Тема 8	Мероприятия по защите банковской тайны. Юридическая ответственность за нарушение норм в области информационной безопасности	12	2		2		8	*Дис.*
Промежуточная аттестация								*За*
Всего по курсу:		**72**	**8**		**8**		**56**	

Очно-заочная форма обучения

№ п/п	**Наименование тем (разделов)**	**Объем дисциплины , час.**						**Форма текущего контроля успеваемости**, промежуточной аттестации*****
		Всего	**Контактная работа обучающихся с преподавателем по видам учебных занятий**				**СРС**	
			Л	**ЛР**	**ПЗ**	**КСР**		
Тема 1	Основы информационной безопасности	8	2				6	
Тема 2	Угрозы информационной безопасности в банковской сфере	9	2		1		6	*Р, Дис, ПЗ*
Тема 3	Информационная безопасность коммерческого банка	7			1		6	*Дис. ПЗ*
Тема 4	Основные методы и технические средства промышленного шпионажа	8	2				6	
Тема 5	Система информационной безопасности банка	9			1		8	*Дис. ПЗ*
Тема 6	Требования к информационной безопасности банка	9			1		8	*Дис. ПЗ*
Тема 7	Проверка и оценка информационной безопасности банка	10			2		8	*Дис. ПЗ*
Тема 8	Мероприятия по защите банковской тайны. Юридическая ответственность за нарушение норм в области информационной	12	2		2		8	*Дис.*

	безопасности							
	Промежуточная аттестация							*За*
	Всего по курсу:	**72**	**8**		**8**		**56**	

Заочная форма обучения

№ п/п	**Наименование тем (разделов)**	**Объем дисциплины , час.**						**Форма текущего контроля успеваемости**, промежуточной аттестации*****
		Всего	**Контактная работа обучающихся с преподавателем по видам учебных занятий**				**СРС**	
			Л	**ЛР**	**ПЗ**	**КСР**		
Тема 1	Основы информационной безопасности	6	2				4	*СР*
Тема 2	Угрозы информационной безопасности в банковской сфере	10			2		8	*Р, Дис, ПЗ*
Тема 3	Информационная безопасность коммерческого банка	10			2		8	*Дис. ПЗ*
Тема 4	Основные методы и технические средства промышленного шпионажа	6	2				4	*СР*
Тема 5	Система информационной безопасности банка	10			2		8	*Дис. ПЗ*
Тема 6	Требования к информационной безопасности банка	8					8	*ПЗ*
Тема 7	Проверка и оценка информационной безопасности банка	10			2		8	*ПЗ*
Тема 8	Мероприятия по защите банковской тайны. Юридическая ответственность за нарушение норм в области информационной безопасности	10					10	*СР*
	Промежуточная аттестация							*За*
	Всего по курсу:	**72**	**4**		**8**		**58**	

Примечание:

*** – формы текущего контроля успеваемости: реферат (Р), дискуссии (Дис), практическое задание (ПЗ), самостоятельная работа (СР).*

**** формы промежуточной аттестации: зачет (За).*

Содержание дисциплины

Тема 1. «Основы информационной безопасности»

Основы теории информационной безопасности. Доктрина информационной безопасности РФ. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы: цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов. Информация и информационные отношения. Субъекты информационных отношений, их безопасность. Основные классы источников информации в банке: люди, документы, публикации, технические средства обеспечения, технические носители, мусор. Стратегии, функции и задачи защиты информации.

Тема 2. «Угрозы информационной безопасности в банковской сфере»

Уязвимость банковских компьютерных систем. Модель угроз информационной безопасности организаций банковской системы. Компьютерные вирусы и методы борьбы с ними. Противоправные воздействия на компьютерную систему банков (компьютерные: загрязнение, злоупотребление, подлог, саботаж, шпионаж). Компьютерные преступления (виды преступлений, причины и условия их совершения). Наиболее типичные виды мошенничества в банке с использованием информационных технологий. Основные способы подделки пластиковых карт. Кардинг – мошенничество с кредитными каточками (кража номеров кредитных карт, продажа поддельных кредитных карт и т.д.). Фишинг – получение информации от владельцев пластиковых карточек путем рассылки по электронной почте с фальшивыми веб-страницами, имитирующие легитимные сайты, запросов от имени банков и платежных систем. Классификация компьютерных сбоев. Несанкционированное проникновение в компьютерные сети банка. По оценкам специалистов, 85% случаев несанкционированного проникновения в компьютерные сети банков остаются нераскрытыми. Классификация нарушителей: первая группа – хакеры; вторая группа – преступники, сотрудники фирмы, преследующие цели обогащения путем несанкционированного получения или использования коммерческой, банковской и другой информации для организации действий уголовного характера; третья группа – террористы и другие экстремистские группы, использующие внедрение в информационные системы для совершения устрашающих действий, шантажа и т.д.; четвертая группа – различные коммерческие организации и структуры, стремящиеся вести промышленный шпионаж и борьбу с конкурентами путем добывания или искажения конфиденциальной, финансовой,

технологической, рекламной и другой информации. Модель нарушителя – мотивы; степень воздействия на информационную среду; возможные места проникновения в информационную систему, области доступные нарушителю; оценка последствий несанкционированных действий нарушителя.

Тема 3. «Информационная безопасность коммерческого банка»

Концептуальная схема (парадигма) обеспечения информационной безопасности коммерческого банка. Основные классы защиты информации. Комплексный подход к обеспечению безопасности компьютерных систем. Общая и частные политики по информационной безопасности в банке. Цель политики информационной безопасности: обеспечение решения вопросов информационной безопасности и вовлечение высшего руководства организации в данный процесс. Основные требования к защите информации в коммерческом банке. Механизмы защиты информации.

Тема 4. «Методы и технические средства промышленного шпионажа»

Промышленный шпионаж – собирание сведений, составляющих коммерческую тайну, путем похищения документов, подкупа или угроз в отношении лиц, владеющих коммерческой тайной, или их близких, перехвата информации в средствах связи, незаконного проникновения в компьютерные системы, использования специальных технических средств, а равно иным незаконным способом с целью разглашения либо непосредственного использования этих сведений. Сущность и содержание промышленного шпионажа. Постановление сената США S226 от 1991 года требует, чтобы американское экспортное оборудование содержало "ловушки", "закладки", известные лишь АНБ (Агентству Национальной Безопасности США). Задачи и методы промышленного шпионажа.

Два основных метода промышленного шпионажа в банковской сфере: обязательный доступ в банк; не требующая доступа. Основные технические средства промышленного шпионажа: закладные устройства; направленные микрофоны; системы магнитной записи звука; средства проводного канала утечки, в который входят все кабельные линии; электронные устройства, установленные в офисах; оптические средства, по которым идет утечка информации за счет модуляции яркости освещения или инфракрасных излучателей и т.д. Предназначение и основные характеристики некоторых технических средств промышленного шпионажа. Алгоритм действий сотрудника банка при обнаружении средств технического съема информации.

Тема 5 . «Система информационной безопасности банка»

Совокупность защитных мер, реализующих обеспечение информационной

безопасности коммерческой организации банковской системы России, и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение, составляет систему информационной безопасности банка. Требования к системе информационной безопасности банка. Основные положения при использовании сети Интернет. Четыре группы процессов для реализации и поддержания информационной безопасности в коммерческом банке. Механизмы защиты информации в банковском секторе: правовые, организационные, инженерно-технические, программно-аппаратные. Система менеджмента информационной безопасности банковской организации. Цикличная модель Деминга «планирование-реализация-проверка-совершенствование-планирование». Полномочия службы информационной безопасности банка. Организация документооборота. Коммерческая тайна. Режим коммерческой тайны – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране её конфиденциальности. Банковская тайна и её содержание. Порядок допуска сотрудников к сведениям составляющих коммерческую и банковскую тайны.

Тема 6. «Требования к информационной безопасности банка»

Требования к информационной безопасности банка: назначения и распределения ролей и обеспечения доверия к персоналу; защиты от несанкционированного доступа к информации и нерегламентированных действий в рамках предоставленных полномочий, управления доступом и регистрацией всех действий в автоматизированных банковских системах, в телекоммуникационном оборудовании, автоматических телефонных станциях и т.д.; антивирусной защиты; использования ресурсов сети Интернет; использования средств криптографической защиты информации; защиты банковских платежных и информационных технологических процессов, в том числе банковских технологических процессов, в рамках которых обрабатываются персональные данные. Обеспечение информационной безопасности автоматизированных банковских систем на стадии жизненного цикла. Организационно-технические мероприятия по защите информации (лицензирование, аттестация, сертификация, ограничение режимов использования, защитные системы управления, средства защиты, контроль). Система сертификации средств защиты информации. Обязательной сертификации подлежат средства защиты информации, предназначенные для защиты сведений, составляющих государственную тайну, а также другой информации с ограниченным доступом. Требования к защите информации в информационно - телекоммуникационной системе.

Тема 7. «Проверка и оценка информационной безопасности банка»

Проверка и оценка информационной безопасности организаций банковской

системы РФ проводится путем выполнения следующих процессов: мониторинга и контроля защитных мер; самооценки информационной безопасности; аудита информационной безопасности; анализа функционирования системы обеспечения информационной безопасности (в том числе со стороны руководства). Основные виды аудита информационной безопасности. Основные группы методов расчета рисков безопасности. Меры безопасности при проведении аудита. Требования к анализу функционирования системы обеспечения информационной безопасности. Защита информационного пространства от наличия в нем контрафактной продукции.

Тема 8. «Мероприятия по защите банковской тайны. Юридическая ответственность за нарушение норм в области информационной безопасности»

Сущность и содержание банковской тайны. Объект, обладатели, условия получения сведений. Тайна банковского счета и вклада. Правовая охрана прав владельца банковской тайны. Ответственность в случае не предоставления сведений, составляющих банковскую тайну клиента, пользователям из числа государственных органов и их должностным лицам. Защита персональных данных клиента коммерческого банка: шифрование баз данных; шифрование каналов связи, по которым ведется работа операциониста с базами данных клиента; разграничение прав доступа к базам данных, содержащих банковскую информацию. Режим банковской тайны. Ответственность за разглашение банковской тайны.

Ответственность представляет собой сложное и многоплановое социальное явление, а также субъективную обязанность субъекта (человека) отвечать за поступки и действия, за их последствия. В отличие от преступления проступок не представляет серьезной общественной опасности, хотя и нарушает правовые предписания государства. Действующее законодательство различает три вида проступков: гражданско-правовые, административно-правовые и дисциплинарные.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Текущий контроль успеваемости

4.1.1. Формы текущего контроля успеваемости

Тема (раздел)	Методы текущего контроля успеваемости
Основы информационной безопасности	Самостоятельная работа
Угрозы информационной безопасности в банковской сфере	Вопросы для дискуссии, темы рефератов. Практическое задание.
Информационная безопасность коммерческого банка	Вопросы для дискуссии. Практическое задание.
Основные методы и технические средства промышленного шпионажа	Самостоятельная работа
Система информационной безопасности банка	Вопросы для дискуссии. Практическое задание.
Требования к информационной безопасности банка	Вопросы для дискуссии. Практическое задание.
Проверка и оценка информационной безопасности банка	Вопросы для дискуссии. Практическое задание.
Мероприятия по защите банковской тайны. Юридическая ответственность за нарушение норм в области информационной безопасности	Вопросы для дискуссии

4.1.2. Материалы текущего контроля успеваемости обучающихся.

Типовые оценочные материалы по теме 1. «Основы информационной безопасности».

Примерные вопросы для самостоятельной работы

1. Основные понятия теории информационной безопасности.
2. Сущность и содержание информации, информационных технологий и их классификация.
3. Основные классы источников информации в банке.
4. Стратегии, функции и задачи защиты информации.

Типовые оценочные материалы по теме 2. «Угрозы информационной безопасности в банковской сфере».

Примерные вопросы для самостоятельной работы

1. Условия и факторы, влияющие на уязвимость банковских компьютерных систем.
2. Сущность и содержание компьютерных преступлений.
3. Классификация нарушителя информационной безопасности.

Примерные темы рефератов

1. Основные внутренние источники угроз в финансово-кредитной сфере.
2. Внешние источники угрозы и их проявление в банковской сфере.
3. Информационно-психологическое воздействие (приёмы и способы) на банковских работников со стороны злоумышленников.
4. Основные пути реализации информационных угроз в финансово-кредитной сфере.
5. Основные условия и факторы информационной безопасности.
6. Информационно-техническое воздействие со стороны злоумышленников на информационную систему банков.

Вопросы для дискуссии

1. Роль и значение информационно-технического воздействия на банковские информационные системы.
2. Угрозы в социальных медиа-ресурсах для банковских работников.
3. В чём заключаются угрозы технологической безопасности программного обеспечения.

Практическое задание

1. Сформировать модель угроз информационной безопасности.
2. Исходя из угроз информации, построить модель реализации угроз.

Типовые оценочные материалы по теме 3. «Информационная безопасность коммерческого банка».

Примерные вопросы для самостоятельной работы

1. Концептуальная схема (парадигма) обеспечения информационной безопасности коммерческого банка.
2. Цель политики информационной безопасности.
3. Механизмы защиты информации.

Вопросы для дискуссии

1. Основные требования, предъявляемые к защите информации в коммерческом банке.
2. Актуальные проблемы обеспечения информационной безопасности в финансово-кредитной сфере.

Практическое задание

Разработать схему, в которой отражены основные составляющие политики банка по информационной безопасности.

Типовые оценочные материалы по теме 4. «Основные методы и технические средства промышленного шпионажа».

Примерные вопросы для самостоятельной работы

1. Сущность и содержание промышленного шпионажа.
2. Задачи и методы промышленного шпионажа.
3. Основные технические средства промышленного шпионажа.
4. Механизмы и средства противодействия промышленному шпионажу в банковском секторе.

Типовые оценочные материалы по теме 5. «Система информационной безопасности банка».

Примерные вопросы для самостоятельной работы

1. Сущность и основные элементы системы информационной безопасности банка.
2. Процессы, направленные на реализацию и поддержание информационной безопасности в коммерческом банке.
3. Основные механизмы защиты информации в банковском секторе.

Вопросы для дискуссии

1. Современное состояние системы информационной безопасности банковского сектора.
2. Актуальные проблемы, связанные с развитием системы информационной безопасности банка в условиях развития информационных технологий.

Практическое задание

Используя метод «Дерева целей» определить основные компоненты системы безопасности банка и отобразить её в виде схемы.

Типовые оценочные материалы по теме 6. «Требования к информационной безопасности банка».

Примерные вопросы для самостоятельной работы

1. Основные требования к информационной безопасности банка.
2. Обеспечение информационной безопасности автоматизированных банковских систем на стадии жизненного цикла.
3. Система сертификации средств защиты информации.

4. Требования к защите информации в информационно - телекоммуникационной системе банка.

Вопросы для дискуссии

1. Основные проблемы обеспечение информационной безопасности автоматизированных банковских систем в современных условиях.

2. Организационно-технические мероприятия по защите информации в банковском секторе: проблемы и пути решения.

Практическое задание

Разработать схему организационных мер по защите информации от воздействия.

Типовые оценочные материалы по теме 7. «Проверка и оценка информационной безопасности банка».

Примерные вопросы для самостоятельной работы

1. Основные виды аудита информационной безопасности.
2. Меры безопасности при проведении аудита.
3. Основные группы методов расчета рисков безопасности.
4. Требования к анализу функционирования системы обеспечения информационной безопасности.

Вопросы для дискуссии

1. Мероприятия по проверке и оценке информационной безопасности организаций банковской системы РФ: проблемы и пути их решения.

2. Защита информационного пространства в банковском секторе от наличия в нем контрафактной продукции.

Практическое задание

Разработать общую структуру (схему) порядка проведения внешнего аудита в финансово-кредитном учреждении.

Типовые оценочные материалы по теме 8. «Мероприятия по защите банковской тайны».

Примерные вопросы для дискуссии

1. Сущность и содержание банковской тайны.
2. Нормативно-правовые аспекты по защите банковской тайны.
3. Персональные данные клиента банка и механизмы защиты данных.
4. Режим банковской тайны.
5. Ответственность за разглашение банковской тайны.

6. Сущность и содержание юридической ответственности за нарушение норм в области информационной безопасности

7. Основные принципы юридической ответственности.

8. Виды правонарушений, юридической ответственности и наказаний

9. Принципы законодательства в области уголовной ответственности.

10. Основное содержание уголовной, административной и дисциплинарной ответственности за нарушение норм в области информационной безопасности.

Методические материалы, позволяющие оценивать знания и умения

Критерии оценивания дискуссии

Оценка «Отлично» выставляется студенту, если он дал научно обоснованный ответ на поставленный вопрос в процессе дискуссии.

Оценка «Хорошо» выставляется студенту, если он дал убедительный ответ на поставленный вопрос в процессе дискуссии.

Оценка «Удовлетворительно» выставляется студенту, если он дал недостаточно обоснованный ответ на поставленный вопрос в процессе дискуссии.

Оценка «Неудовлетворительно» выставляется студенту, если он не дал никакого ответа на дискуссионный вопрос.

Критерии оценивания докладов, рефератов и эссе

Оценка «Отлично» выставляется студенту, если подготовлен научно обоснованный доклад на выбранную тему с анализом информации, выводами и предложениями.

Оценка «Хорошо» выставляется студенту, если подготовлен доклад на выбранную тему в виде аналитической записки без выводов и предложений.

Оценка «Удовлетворительно» выставляется студенту, если подготовлена информация на выбранную тему без обоснования выводов и предложений.

Оценка «Неудовлетворительно» выставляется студенту, если подготовлена информация, не соответствующая выбранной теме без выводов и предложений.

Критерии оценивания результатов быстрого письменного опроса на практическом занятии

Каждому студенту выдается свой собственный, узко сформулированный вопрос. Ответ должен быть четким и кратким, содержащим все основные характеристики описываемого понятия, института, категории.

Шкала оценивания:

«Отлично» - вопрос раскрыт полностью, точно обозначены основные понятия и характеристики по теме.

«Хорошо» - вопрос раскрыт, однако нет полного описания всех необходимых элементов.

«Удовлетворительно» - вопрос раскрыт не полно, присутствуют грубые ошибки, однако есть некоторое понимание раскрываемых понятий.

«Неудовлетворительно» - ответ на вопрос отсутствует или в целом не верен.

4.2. Промежуточная аттестация

4.2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-5	Способность на основе комплексного экономического и финансового анализа дать оценку результатов и эффективности финансово-хозяйственной деятельности организаций различных организационно-правовых форм, включая финансово-кредитные, органов государственной власти и местного самоуправления	ПК-5.2	Способность оценивать результаты банковской деятельности, проводить комплексный анализ цифрового банкинга с использованием IT.
ДПК-4	Способность применять методы анализа и информационного обеспечения управления финансовыми рисками; владеть способами снижения финансовых рисков; применять методы маркетинговых исследований для изучения рынка банковских, финансовых, инвестиционных продуктов и услуг; способностью анализировать и использовать различные источники информации на иностранном языке для своей практической деятельности и представлять результат проведенного исследования в виде презентации, мини-презентации, доклада или статьи	ДПК-4.2	Способность применять методы анализа и информационного обеспечения управления финансовыми рисками в банковском деле.

Этап освоения компетенции	Критерий оценивания	Показатель оценивания
ПК-5.2.Способность оценивать результаты банковской деятельности, проводить комплексный анализ цифрового банкинга с использованием IT.	Способность анализировать деятельность Центральных Банков в глобальной экономике. Способность использовать методы оценки результатов банковской деятельности. Способность комплексно анализировать цифровой банкинг. Способность проводить научные исследования, акцентируя внимание на информационной безопасности. Способность проводить научные исследования, учитывая банковскую тайну.	Анализирует деятельность Центральных Банков в глобальной экономике. Использует методы оценки результатов банковской деятельности. Применяет комплексный анализ цифрового банкинга. Применяет информационные технологии в деятельности организации. Обобщает и представляет в виде отчета исследования в области финансов и кредита, учитывая информационную безопасность и защиту банковской тайны.
ДПК-4.2. Способность применять методы анализа и информационного обеспечения управления финансовыми рисками в банковском деле.	Способность использования современных инструментов и методов в сфере информационных технологий в области цифрового банкинга и умение практического применения полученных инструментов и методов, позволяющих проектировать и создавать готовые, завершенные проекты в области цифрового банкинга, ориентированные на внедрение в отечественных банках и инвестиционных компаниях.	Способен анализировать макроэкономические тенденции. Способен оценивать влияние деятельности Центральных банков на мировую финансовую систему. Способен анализировать цифровой банкинг. Способен анализировать корпоративные финансы. Способен обеспечить управление финансовыми рисками. Проводит анализ деловой активности корпорации, анализирует финансовые риски, использует полученные сведения для принятия управленческих решений финансовых и экономических служб, формирует практические предложения по совершенствованию их работы, самостоятельного анализирует показатели финансовой деятельности корпораций. Способен оценить новых банковских продуктов Способен обеспечить

		управление финансовыми рисками. Способен использовать информационные технологии в деятельности организации. Способен применять новые банковские продукты и использовать цифровой банкинг. Использует современные инструменты и методы в сфере информационных технологий в области цифрового банкинга и умение практического применения полученных инструментов и методов, позволяющих проектировать и создавать готовые, завершенные проекты в области цифрового банкинга, ориентированные на внедрение в отечественных банках и инвестиционных компаниях.

4.2.2 Форма и средства (методы) проведения промежуточной аттестации

Зачет проводится в форме устного опроса.

4.2.3. Типовые оценочные средства

Список вопросов для подготовки к зачету

1. Субъект и объект информационной безопасности банка.
2. Что такое информация и её классификация?
3. Информационные технологии и их категорирование.
4. Информационные системы, их классификация, функции информационных систем.
5. Конфиденциальность информации, сущность и содержание.
6. Информационный ресурс, понятие и содержание.
7. Виды информационных ресурсов и их содержание.
8. Деление информационных ресурсов по видам, способам и содержанию.
9. Информация как объект правовых отношений.
10. Основные классы источников информации.
11. Сущность и содержание информационной безопасности.
12. Основные условия и факторы, влияющие на формирование и проявление угроз информационной безопасности банка.
13. Сущность и содержание внутренних угроз информационной безопасности банка.

14. Основные источники внешних угроз информационной безопасности банка и их проявление.

15. Что такое угрозы конфиденциальной безопасности?

16. Модель угроз информационной безопасности, структура и содержание.

17. Модель реализации угроз информационной безопасности.

18. Модель нарушителя информационной безопасности.

19. Основные способы получения «нужной» информации.

20. В чем заключается технологическая безопасность программного продукта, сущность и содержание.

21. Основные способы несанкционированного доступа к информации.

22. Информационные и иные активы в сфере информационной безопасности.

23. Минимальные требования к информационной безопасности.

24. Что такое политика информационной безопасности, цель и основное содержание?

25. Основные механизмы защиты информации.

26. Организационные меры по защите информации, сущность и содержание мероприятий.

27. Что такое физическая защита информационных ресурсов?

28. Сущность и содержание криптографической защиты информации.

29. Методы противодействия вирусным программам.

30. Сущность и содержание организации делопроизводства в интересах защиты информации.

31. Основные признаки подделки документов и способы их выявления.

32. Основные мероприятия по защите конфиденциальной информации.

33. Основные мероприятия по защите персональных данных.

34. Основные способы неправомерного доступа к информационным ресурсам.

35. Основные технические средства съема информации.

36. Основные методы противодействия по неправомерному снятию информации в помещении.

37. Основные направления по защите банковских информационных сетей.

38. Программно-технические методы обнаружения вирусов.

39. Классификация вирусов.

40. Что такое идентификация, аутентификация и авторизация?

41. Основные технические каналы утечки информации и мероприятия по их защите.

42. Защита от встроенных и узконаправленных микрофонов.

43. Основы защиты персональных ЭВМ.

44. Действия работников кредитной организации при обнаружении закладного устройства.

45. Что включает в себя сертификация средств защиты информации по требованиям безопасности информации?

46. Что такое коммерческая тайна, и какие мероприятия проводятся по её защите?

47. Как обеспечивается защита банковской тайны?

48. На каких принципах организуется служба информационной безопасности, и чем она руководствуется?

49. Что включает в себя понятие информационной безопасности банка?

50. Каковы последствия несанкционированного проникновения в компьютерные системы и как им противостоять?

51. Назовите основные способы ведения промышленного шпионажа.

52. Почему необходимо обучать персонал фирмы (офиса) навыкам ведения встреч и переговоров?

53. Виды технических средств, используемых для несанкционированного доступа к конфиденциальной информации.

54. Назовите основные механизмы безопасности информации.

55. Что такое банковская тайна?

56. Назовите основные мероприятия по защите банковской тайны.

57. Юридическая ответственность банковского работника за нарушение норм в области информационной безопасности.

58. Административная ответственность банковского работника за нарушение норм в области информационной безопасности.

59. Уголовная ответственность банковского работника за нарушение норм в области информационной безопасности.

60. Дисциплинарная ответственность банковского работника за нарушение норм в области информационной безопасности.

Примеры билетов

Билет № ____

1. Сущность и содержание внутренних угроз информационной безопасности банка.
2. Алгоритм работников кредитной организации при обнаружении закладного устройства (схема).

Билет № ____

1. Дайте определение информации и её классификацию.
2. Основное содержание модели угроз информационной безопасности банка.

(принципиальную модель показать схемой).

Билет № ____

1. Основные направления по защите банковских информационных сетей.
2. Основные источники угроз информационной безопасности для финансово-кредитной сферы (показать схемой).

Билет № ____

1. Назовите основные признаки подделки документов и способы их выявления.
2. Основное содержание реализации угроз информационной безопасности (принципиальную модель показать схемой).

Билет № ____

1. Информация как объект правовых отношений: сущность и содержание.
2. Компьютерные вирусы и их классификация (классификацию показать схемой).

Шкала оценивания

Зачтено	Обобщает и представляет в виде отчета исследования в области финансов и кредита, учитывая информационную безопасность и защиту банковской тайны. Демонстрирует анализировать информацию в масштабах всего спектра банковских, финансовых, инвестиционных продуктов и услуг. Способен соблюдать условия информационной безопасности и банковской тайны.
	Обобщает и представляет в виде отчета исследования в области финансов и кредита, но не учитывает информационную безопасность и защиту банковской тайны. Демонстрирует способность анализировать информацию в масштабах всего спектра банковских, финансовых, инвестиционных продуктов и услуг, но не в полной мере. Способен соблюдать условия информационной безопасности и банковской тайны.
	Обобщает, но не умеет представлять в виде отчета исследования в области финансов и кредита, учитывая информационную безопасность и защиту банковской тайны. Демонстрирует способность анализировать информацию в масштабах очень узкого спектра банковских, финансовых, инвестиционных продуктов и услуг. Не способен соблюдать условия информационной безопасности и банковской тайны.
Не зачтено	Не обобщает и не представляет в виде отчета исследования в области финансов и кредита, учитывая информационную безопасность и защиту банковской тайны. Не демонстрирует способность анализировать информацию в масштабах всего спектра банковских, финансовых, инвестиционных продуктов и услуг.

	Не способен соблюдать условия информационной безопасности и банковской тайны.

4.3. Методические материалы

Процедура проведения устного зачета

Аттестационные испытания проводятся преподавателем, ведущим лекционные занятия по данной дисциплине. Инвалиды и лица с ограниченными возможностями здоровья, имеющие нарушения опорно-двигательного аппарата, допускаются на аттестационные испытания в сопровождении ассистентов-сопровождающих.

Во время аттестационных испытаний обучающиеся могут пользоваться программой учебной дисциплины, а также с разрешения преподавателя калькуляторами. Время подготовки ответа при сдаче в устной форме должно составлять не менее 20 минут (по желанию обучающегося ответ может быть досрочным). Время ответа – не более 15 минут. При подготовке, как правило, ведутся записи в листе устного ответа, который затем (по окончании) сдается экзаменатору.

При проведении устного зачета билет выбирает сам экзаменуемый в случайном порядке. Экзаменатору предоставляется право задавать обучающимся дополнительные вопросы в рамках программы дисциплины текущего семестра, а также, помимо теоретических вопросов, давать задачи, которые изучались на практических занятиях. Оценка результатов устного аттестационного испытания объявляется обучающимся в день его проведения. При проведении устного зачета в аудитории могут одновременно находиться не более шести экзаменующихся. По окончании ответа на вопросы билета экзаменатор может задать экзаменуемому дополнительные и уточняющие вопросы в пределах учебного материала, вынесенного на зачет.

5. Методические указания для обучающихся по освоению дисциплины

Методика организации самостоятельной работы студента по подготовке реферата

Работа по углублённому изучению дисциплины может выполняется в виде проработки отдельных тем исследований и представления полученных результатов устно или в виде эссе, доклада с презентацией. Тему для углублённого изучения студент выбирает из приведенного списка.

По согласованию с преподавателем студент может выполнять углублённое изучение темы, связанной с его профессиональной деятельностью. Поощряется представление полученных итогов в виде оформленных результатов научно-

исследовательской или практической разработки (статьи, доклады, документы о внедрении полученных результатов.).

Подготовка темы не должна выражаться исключительно в подборе материала из литературных источников, указанных в программе. Обучаемый должен продемонстрировать глубокое знание предмета, логично и аргументированно излагать свою точку зрения.

Изучение должно носить завершенный характер: иметь внутреннюю логику, содержать постановку и грамотное решение задач управления, оценку результативности и дальнейшие положения по их использованию. Полученные результаты должны основываться на собственных разработках автора, полученных им оригинальных решениях и рекомендациях.

В случае предоставления итогов изучения в виде доклада, эссе рекомендуется следующая его структура:

- титульный лист;
- содержание;
- основная текстовая часть;
- заключение;
- библиографический список;
- приложения.

В разделах следует придерживаться следующей структуры.

Во "Введении" следует обосновать актуальность темы, степень разработанности проблемы (с указанием имен авторов и литературы), цель, задачи, объект и предмет исследования, теоретическую концепцию, методологию и методы, практическую значимость, информационно-эмпирическую базу, структуру доклада (эссе), при этом в эссе в большей степени отражаются собственные взгляды по изучаемой проблеме.

В основной текстовой части должны быть указаны как минимум три части: теоретико-методологическая, описание исследования и особенности его теоретико-практического применения.

Во второй главе дается обзор литературы по проблеме, формируется концепция, обосновывается методика анализа проблемы, и в третьей главе должно быть обоснование практических аспектов и выводов исследования

Материалы, служащие базой для обоснования и анализа, должны быть достаточно полными и достоверными, чтобы, опираясь на них, можно было бы проанализировать положение дел, вскрыть и наметить пути их использования, а также устранить вскрытые недостатки в работе. Следует избегать ненужных сведений, отбирая только те, которые

наиболее точно отражают суть исследуемого процесса или явления.

В "Заключении" должны быть основные выводы.

Самоподготовка к практическим занятиям

При подготовке к практическому занятию необходимо помнить, что та или иная дисциплина тесно связана с ранее изучаемыми курсами. Более того, именно синтез полученных ранее знаний и текущего материала по курсу делает подготовку результативной и всесторонней.

На семинарских занятиях студент должен уметь последовательно излагать свои мысли и аргументированно их отстаивать.

Для достижения этой цели необходимо:

1) ознакомиться с соответствующей темой программы дисциплины;

2) осмыслить круг изучаемых вопросов и логику их рассмотрения;

3) изучить рекомендованную литературу по данной теме;

4) тщательно изучить лекционный материал;

5) ознакомиться с вопросами очередного семинарского занятия;

6) подготовить краткое выступление по каждому из вынесенных на семинарское занятие вопросу.

Изучение вопросов очередной темы требует глубокого усвоения теоретических основ дисциплины, раскрытия сущности основных экономических категорий, проблемных аспектов темы и анализа фактического материала.

При презентации материала на семинарском занятии можно воспользоваться следующим алгоритмом изложения темы: определение и характеристика основных категорий, эволюция предмета исследования, оценка его современного состояния, существующие проблемы, перспективы развития.

Методические рекомендации по подготовке к дискуссии (научным обсуждениям)

Дискуссия представляет собой обсуждение заданной темы. Требуется проявить логику изложения материала, представить аргументацию, ответить на вопросы участников дискуссии.

Участвуя в дискуссии студентам следует высказываться свободно и открыто, не оглядываясь на авторитеты и устоявшиеся мнения, критично оценивать рассматриваемый материал, указывать на нечетко или непонятно сформулированные позиции, противоречия, замеченные при ознакомлении с тем или иным источником информации. При этом критика должна быть аргументированной и конструктивной. Студенту необходимо высказать именно собственную точку зрения, свое согласие или несогласие с имеющимися позициями и высказываниями по данному вопросу. Дискуссия не

предполагает простого изложения полученных сведений. Участие в дискуссии быть должно быть основано на предварительном изучении обсуждаемого вопроса.

При подготовке к дискуссии необходимо внимательно прочитать вопрос и подготовить аргументированные суждения.

Методические рекомендации по подготовке к промежуточной аттестации

При подготовке к промежуточной аттестации ознакомьтесь со списком представленных вопросов. Формулируйте ответ с точки зрения применения различных методов анализа данных. Необходимо дать аргументированный ответ, подтверждающий уровень освоения компетенции.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература.

1. Одинцов, Б. Е. Информационные системы управления эффективностью бизнеса : учебник и практикум для вузов / Б. Е. Одинцов. — Москва : Издательство Юрайт, 2020. — 206 с. — (Высшее образование). — ISBN 978-5-534-01052-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450638

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772

6.2. Дополнительная литература.

1. Шапцев, В. А. Теория информации. Теоретические основы создания информационного общества : учебное пособие для вузов / В. А. Шапцев, Ю. В. Бидуля. — Москва : Издательство Юрайт, 2020. — 177 с. — (Высшее образование). — ISBN 978-5-534-02989-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451811

2. Пичугин, В. Безопасность бизнеса: Защита от уголовного преследования / В. Пичугин. — Москва : Альпина Паблишер, 2019. — 176 с. — ISBN 978-5-9614-1076-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/83081.html

3. Пичугин, В. Г. Безопасность бизнеса [Электронный ресурс] : защита от уголовного преследования / В. Г. Пичугин ; под ред. Ю. Быстрова. — Электрон. текстовые данные. —

М. : Альпина Паблишер, 2016. — 175 c. — 978-5-9614-1076-1. — Режим доступа: http://www.iprbookshop.ru/42026.html

6.3. Учебно-методическое обеспечение самостоятельной работы

Не предусмотрено.

6.4. Нормативные правовые документы.

1. О банках и банковской деятельности. Федеральный закон от 3 февраля 1996 г. № 17 – ФЗ, (последняя редакция)
2. О безопасности. Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 05.10.2015)
3. Федеральный закон от 06.03.2006 N 35-ФЗ (ред. от 06.07.2016) "О противодействии терроризму" (с изм. и доп., вступ. в силу с 01.01.2017)
4. О государственной тайне. Федеральный закон от 21 июля 1993г. № 5485-1 (с ред. от 08.03.2015).
5. Федеральный закон 26 января 1996 года № 14-ФЗ «Гражданский кодекс Российской Федерации» (ред. от 28.03.2017).
6. Федеральный закон от 13 июня 1996 года № 63-ФЗ «Уголовный кодекс Российской Федерации» (ред. от 17.04.2017).
7. Федеральный закон от 18 декабря 2001 года № 174 - ФЗ «Уголовно – процессуальный кодекс Российской Федерации» (ред. от 07.06.2017)
8. Федеральный закон 30 декабря 2001 года № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (ред. от 07.06.2017)
9. Федеральный закон от 30 декабря 2001 года № 197-ФЗ «Трудовой кодекс Российской Федерации» (ред. от 01.05.2017).
10. Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (ред. от 01.05.2017)
11. Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «Об утверждении Стратегии национальной безопасности Российской Федерации».
12. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 5 декабря 2016 г. № 6469.
13. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утверждена Президентом Российской Федерации от 9 мая 2017 года № 203.
14. Об персональных данных. Федеральный закон от 27 июля 2006 г. № 152 – ФЗ.
15. ISO/IEC IS 27001-2005 Information technology. Security techniques. Information security management systems. Requirements

16. Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

17. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/Общие положения»

18. О коммерческой тайне. Федеральный закон от 29 июля 2004 г. № 98-ФЗ. (последняя редакция)

19. О противодействии легализации (отмыванию) доходов, полученных преступным путем. Федеральный закон от 7 августа 2001 г. № 115 (последняя редакция 2016 г.).

20. О рынке ценных бумаг. Федеральный закон от 22 апреля 1996 г. № 39-ФЗ. (последняя редакция 2016 г.).

21. Защита информации. Основные термины и определения. ГОСТ Р50922-96.

22. Письмо от 28 ноября 2001 г. №137-т «О рекомендациях по разработке кредитными организациями правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (в ред. письма ЦБ РФ от 16.01.2003 n 6-т).

23. Ведомственные нормы проектирования «Здания территориальных главных управлений, национальных банков и расчетно-кассовых центров Центрального банка Российской Федерации» ВНП 001-01/Банк России.

24. Разведзащищенность. Термины и определения. ОСТ В 4.0007 – 95.

25. Средства вычислительной техники. Защита от несанкционированного доступа к информации. ГОСТ Р 50739-95.

26. Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации: Руководящий документ //Сборник руководящих документов по защите информации от несанкционированного доступа. – М.: Гостехкомиссия России, 1998.

27. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (последняя редакция).

6.5. Интернет ресурсы.

www.minfin.ru – Министерство финансов Российской Федерации

www.pfrf.ru – Пенсионный Фонд Российской Федерации

www.fss.ru – Фонд обязательного страхования Российской Федерации

www.ffoms.ru - Федеральный Фонд обязательного медицинского страхования

www.cbr.ru – Центральный Банк Российской Федерации

www.asv.org.ru – Агентство по страхованию вкладов

www.kfm.ru – Федеральная служба по финансовому мониторингу

www.arb.ru – Ассоциация российских банков

www.asros.ru – Ассоциация региональных банков России

6.6. Иные источники

1. Лукаш, Ю.А. Противодействие враждебным и преступным проявлениям и их профилактика как составляющая обеспечения безопасности и развития бизнеса. [Электронный ресурс] : Учебные пособия М.: ФЛИНТА, 2012

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Базы данных, информационно-справочные и поисковые системы

1. www.biblio-online.ru –Электронно-библиотечная система [ЭБС] Юрайт;
2. http://www.iprbookshop.ru – Электронно-библиотечная система [ЭБС] «Iprbooks»
3. https://e.lanbook.com - Электронно-библиотечная система [ЭБС] «Лань».
4. http://elibrary.ru/ - Научная электронная библиотека Elibrary.ru.
5. https://new.znanium.com Электронно-библиотечная система [ЭБС] «Znanium.com».
6. https://dlib.eastview.com – Информационный сервис «East View».
7. https://www.jstor.org - Jstor. Полные тексты научных журналов и книг зарубежных издательств.
8. https://elibrary.worldbank.org - Электронная библиотека Всемирного Банка.
9. https://link.springer.com - Полнотекстовые политематические базы академических журналов и книг издательства Springer.
10. https://ebookcentral.proquest.com - Ebook Central. Полные тексты книг зарубежных научных издательств.
11. https://www.oxfordhandbooks.com - Доступ к полным текстам справочников Handbooks издательства Oxford по предметным областям: экономика и финансы, право, бизнес и управление.
12. https://journals.sagepub.com - Полнотекстовая база научных журналов академического издательства Sage.
13. Справочно-правовая система «Консультант».
14. Электронный периодический справочник «Гарант».

Программные, технические и электронные средства обучения и контроля знаний.

Для проведения занятий по дисциплине необходимо материально-техническое обеспечение учебных аудиторий (наглядными материалами, экраном, мультимедийным проектором с ноутбуками (ПК) для презентации учебного материала, выходом в сеть Интернет, программными продуктами Microsoft Office (Excel, Word, PowerPoint)) в зависимости от типа занятий: семинарского и лекционного типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Для самостоятельной работы обучающимся необходим доступ в читальные залы библиотеки и/или помещение, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет», доступ в электронную информационно-образовательную среду организации и ЭБС.