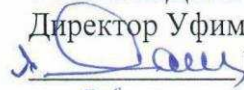


Федеральное государственное образовательное бюджетное
учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)

Уфимский филиал Финуниверситета
Кафедра «Философия, история и право»

УТВЕРЖДАЮ
Директор Уфимского филиала
 Р.М. Сафуанов
« 02 » 09 2021 г.

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

Рабочая программа дисциплины
для студентов, обучающихся по образовательной программе
40.03.01 «Юриспруденция»
Образовательная программа «Юриспруденция»
(Экономическое право)

Рекомендовано Ученым советом филиала
(протокол № 39 от «31» августа 2021г.)

Одобрено кафедрой «Философия, история и право»
(протокол № 1 от «27» августа 2021г.)

Уфа 2021

СОДЕРЖАНИЕ	Стр
1. Наименование дисциплины	3
2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	3
3. Место дисциплины в структуре образовательной программы	4
4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	4
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	4
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	11
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	16
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	21
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	22
10. Методические указания для обучающихся по освоению дисциплины	23
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	24
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	24

1. Наименование дисциплины.

«Правовое обеспечение кибербезопасности»

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине.

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с компетенциями / индикаторами достижения компетенции
ПКП-1	Способность использовать фундаментальные знания в области частного права и публичного права в современных условиях и оказывать помощь в реализации правовых норм субъектами гражданского оборота	1. Анализирует юридические факты и возникающие в связи с ними правоотношения, толкует и правильно применяет правовые нормы.	знать: нормы российского законодательства о информационной безопасности уметь: грамотно применять законодательство об информационной безопасности в правовой деятельности
		2. Принимает решения и совершает юридические действия в точном соответствии с законом.	знать: структуру, основные цели, задачи, организационные формы и методы информационной безопасности в России уметь: ориентироваться в основных понятиях кибербезопасности в Российской Федерации
		3. Демонстрирует навыки анализа правоприменительной практики, обеспечивает реализацию норм процессуального права.	знать: способы работы с документами, относящимися к информационной безопасности уметь: грамотно и правильно составлять и оформлять документы о кибербезопасности
ПКП-2	Способность действовать с учетом кризисных ситуаций в экономике, вызываемых рисками правового экономического характера, анализировать проблемные ситуации на рынке товаров, работ, услуг, а	1. Выявляет и предлагает способы устранения проблем, связанных с кризисными ситуациями в экономике.	знать: основы законодательства о информационной безопасности с точки зрения государственного регулирования экономики уметь: применять на практике законодательство Российской Федерации, в том числе Конституцию Российской Федерации, федеральные конституционные законы и федеральные законы, а также общепризнанные принципы, нормы международного права относительно кибербезопасности
		2. Анализирует проблемные ситуации на рынке товаров,	знать: способы соблюдения законодательства Российской Федерации субъектами права в сфере

	также выявлять правонарушения при осуществлении предпринимательской деятельности и давать юридически обоснованные предложения по их преодолению и устранению	работ, услуг, выявляет правонарушения при осуществлении предпринимательской деятельности	кибербезопасности уметь: применять нормативные правовые акты, реализовывать нормы материального и процессуального права в сфере информационной безопасности
		3. Находит пути решения ситуаций, связанных с преодолением правонарушений при осуществлении предпринимательской деятельности	знать: основы законодательства в области защиты интересов предпринимателей в сфере информационной безопасности уметь: представлять интересы предпринимателей в судах в сфере кибербезопасности

3. Место дисциплины в структуре образовательной программы

Дисциплина «Правовое обеспечение кибербезопасности» входит в цикл профиля (элективный), модуль 2 «Право цифровой экономики» образовательной программы «Юриспруденция» (Экономическое право) по направлению подготовки 40.03.01 Юриспруденция.

4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Таблица 1

Очная/заочная формы обучения

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 7/8 (в часах)
Общая трудоемкость дисциплины	3 е. /108	108 /108
<i>Контактная работа - Аудиторные занятия</i>	34/12	34/12
<i>Лекции</i>	16/4	16/4
<i>Семинары, практические занятия</i>	18/8	18/8
<i>Самостоятельная работа</i>	74/96	74/96
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	зачет	зачет

5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Введение в дисциплину «Правовое обеспечение кибербезопасности».

Система правовой защиты информации как предмет изучения. Место правовой защиты информации в системе комплексной защиты информации организации. Виды угроз информационной безопасности РФ. Источники угроз информационной безопасности. Задачи обеспечения информационной безопасности в различных сферах деятельности. Методы обеспечения информационной безопасности Российской Федерации. Функции и структура государственной системы обеспечения информационной безопасности. Правовые основы защиты информации. Основные направления и принципы обеспечения комплексной безопасности объектов информатизации.

Тема 2. Законодательство, подзаконные нормативные акты и основы технического регулирования Российской Федерации по вопросам защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

Законодательство Российской Федерации по вопросам защиты конфиденциальной информации. Системы технического регулирования по вопросам защиты информации. Регулирование ФСБ России по вопросам защиты конфиденциальной информации. Регулирование ФСТЭК России по вопросам защиты конфиденциальной информации. Регулирование защиты персональных данных. Отраслевые требования по вопросам защиты конфиденциальной информации.

Тема 3. Системный подход к обеспечению кибербезопасности объекта.

Разработка концепции и создание системы защиты информации на объекте. Основные направления защиты информации в кредитно-финансовой сфере. Создание системы обеспечения информационной безопасности объекта в кредитно-финансовой сфере.

Тема 4. Особенности системы организационной защиты информации, составляющей государственную и коммерческую тайну.

Государственная тайна и порядок отнесения к ней информации. Защита государственной тайны. Организация режима секретности, его особенности и содержание. Коммерческая тайна и порядок её определения. Организация работ с информацией, составляющей коммерческую тайну.

Тема 5. Допуск к секретной информации.

Положения российского законодательства, регламентирующие допуск к государственной тайне. Процедура оформления и переоформления допусков к государственной тайне и ее документирование. Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне (формы учетной документации).

Тема 6. Организация доступа к информации ограниченного доступа. Разрешительная система доступа к сведениям, составляющим коммерческую тайну предприятия (фирмы). Мероприятия по реализации разрешительной системы доступа к сведениям, составляющим коммерческую тайну предприятия (фирмы).

Тема 7. Организация деятельности службы безопасности объекта. Проведение служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. Задачи службы безопасности организации. Организационная структура службы безопасности. Организация

внутриобъектового режима предприятия. Организация охраны объектов предприятия. Организация и обеспечение защиты коммерческой тайны в организации. Организация инженерно-технической защиты. Организация безопасности функционирования информационных систем. Проверка наличия документов, дел и носителей информации. Организация служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. Проведение аналитико-разведывательной работы.

Тема 8. Организация защиты информации при проведении совещаний по конфиденциальным вопросам, приеме посетителей и осуществлении научно-публицистической и рекламной деятельности.

Защита информации при проведении совещаний и переговоров. Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей. Организация защиты информации в кадровой службе. Общие правила работы с документами в организации. Организация защиты информации в работе пресс-служб, при осуществлении научно-публицистической и рекламной деятельности.

Тема 9. Задачи, методы, стратегии, способы и средства защиты информации.

Задачи и методы обеспечения информационной безопасности. Стратегии защиты информации. Способы и средства защиты информации.

Тема 10. Лицензирование и сертификация в области защиты информации

Правовая основа системы лицензирования и сертификации в Российской Федерации. Лицензирование деятельности по защите информации. Сертификация средств защиты информации.

Тема 11. Аудит информационной безопасности систем, информационных технологий и организаций

Общая характеристика состояния аудиторской деятельности в области информационной безопасности. Основные виды и способы аудита информационной безопасности. Основные принципы проведения аудита информационной безопасности. Критерии аудита информационной безопасности. Организационно-методологические основы проведения аудита информационной безопасности. Взаимоотношение аудиторов с представителями проверяемой организации. Управление программой аудита информационной безопасности. Этапы проведения аудита информационной безопасности. Инструментальное обеспечение аудита информационной безопасности. Требования к кадровому обеспечению аудиторской деятельности в области информационной безопасности. Реализация первоочередных мероприятий по обеспечению аудиторской деятельности в области информационной безопасности.

5.2. Учебно-тематический план

Таблица 2

Очная/заочная формы обучения

№ п/ п	Наименования тем (разделов) дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа – Аудиторная работа			Самостоятель ная работа	
			Общая	Лекци и	Семинары, практическ ие занятия		
1	Тема 1. Введение в дисциплину «Правовое обеспечение кибербезопас- ности»	9/9	2/1	1/0,5	1/0,5	7/8	Дискуссия. Семинар в диалоговом режиме Решение практико- ориентированн ых заданий
2	Тема 2. Законодательст во, подзаконные нормативные акты и основы технического регулирования Российской Федерации по вопросам защиты.	9/9	2/1	1/0,5	1/0,5	7/8	Дискуссия, опрос. Решение практико- ориентированн ых заданий
3	Системный подход к обеспечению кибербезопас- ности объекта.	10/10	2/1	1/0,5	1/0,5	8/9	Опрос, решение задач, дискуссия
4	Тема 4. Особенности системы организацион- ной защиты информации, составляющей государствен- ную и коммерческую тайну.	10/10	2/1	1/0,5	1/0,5	8/9	Опрос, дискуссия, решение задач
5	Тема 5. Допуск к секретной информации.	10/10	3/1,5	1/0,5	2/1	7/8,5	Дискуссия. Решение задач. Анализ правовой практики
6	Тема 6.	10/10	3/1	1/0,5	2/0,5	7/8,5	Дискуссия.

	Организация доступа к информации ограниченного доступа.						Семинар в диалоговом режиме. Решение задач. Анализ правовой практики
7	Тема 7. Организация деятельности службы безопасности объекта.	10/10	4/0,5	2/-	2/0,5	6/9,5	Опрос. Решение задач. Анализ правовой практики
8	Тема 8. Организация защиты информации при проведении совещаний по конфиденциальным вопросам, приеме посетителей и осуществлении научно-публицистической и рекламной деятельности.	10/10	4/1	2/-	2/1	6/9	Дискуссия. Решение задач. Анализ правовой практики
9	Тема 9. Задачи, методы, стратегии, способы и средства защиты информации.	10/10	4/1,5	2/0,5	2/1	6/8,5	Дискуссия. Решение задач. Анализ правовой практики.
10	Тема 10. Лицензирование и сертификация в области защиты информации	10/10	4/1,5	2/0,5	2/1	6/8,5	Дискуссия. Решение задач. Анализ правовой практики.
11	Тема 11. Аудит информационной безопасности систем, информационных	10/10	4/1	2/-	2/1	6/9	Дискуссия. Решение задач. Анализ правовой практики.

	технологий и организаций						
	В целом по дисциплине	108/108	34/12	16/4	18/8	74/96	Согласно учебному плану: контрольная работа

5.3. Содержание семинаров, практических занятий

Таблица 4

Наименование темы дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8, 9	Формы проведения занятий
Тема 1. Введение в дисциплину «Правовое обеспечение кибербезопасности»	Система правовой защиты информации как предмет изучения. Место правовой защиты информации в системе комплексной защиты информации организации. Виды угроз информационной безопасности РФ. Источники угроз информационной безопасности. Задачи обеспечения информационной безопасности в различных сферах деятельности. Методы обеспечения информационной безопасности Российской Федерации. Функции и структура государственной системы обеспечения информационной безопасности. Правовые основы защиты информации. Основные направления и принципы обеспечения комплексной безопасности объектов информатизации. Рекомендуемые источники из раздела 8: 1-12 из раздела 9: 1-9	Дискуссия. Семинар в диалоговом режиме. Решение практико-ориентированных заданий.
Тема 2. Законодательство, подзаконные нормативные акты и основы технического регулирования Российской Федерации по вопросам защиты информации.	Законодательство Российской Федерации по вопросам защиты конфиденциальной информации. Системы технического регулирования по вопросам защиты информации. Регулирование ФСБ России по вопросам защиты конфиденциальной информации. Регулирование ФСТЭК России по вопросам защиты конфиденциальной информации. Регулирование защиты персональных данных. Отраслевые требования по вопросам защиты конфиденциальной информации. Рекомендуемые источники из раздела 8: 1-12 из раздела 9: 1-9	Дискуссия. Опрос. Решение практико-ориентированных заданий.
Тема 3. Системный подход к обеспечению кибербезопасности объекта.	Разработка концепции и создание системы защиты информации на объекте. Основные направления защиты информации в кредитно-финансовой сфере. Создание системы обеспечения информационной безопасности объекта в кредитно-финансовой сфере. Рекомендуемые источники	Опрос, решение задач, дискуссия.

	из раздела 8: 1-12 из раздела 9: 1-9	
Тема 4. Особенности системы организационной защиты информации, составляющей государственную и коммерческую тайну.	Государственная тайна и порядок отнесения к ней информации. Защита государственной тайны. Организация режима секретности, его особенности и содержание. Коммерческая тайна и порядок её определения. Организация работ с информацией, составляющей коммерческую тайну. Рекомендуемые источники из раздела 8: 1-12 из раздела 9: 1-9	Опрос, дискуссия, решение задач.
Тема 5. Допуск к секретной информации.	Положения российского законодательства, регламентирующие допуск к государственной тайне. Процедура оформления и переоформления допусков к государственной тайне и ее документирование. Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне (формы учетной документации). Рекомендуемые источники из раздела 8: 1-12 из раздела 9: 1-9	Дискуссия. Опрос. Семинар в диалоговом режиме.
Тема 6. Организация доступа к информации ограниченного доступа.	Разрешительная система доступа к сведениям, составляющим коммерческую тайну предприятия (фирмы). Мероприятия по реализации разрешительной системы доступа к сведениям, составляющим коммерческую тайну предприятия (фирмы). Рекомендуемые источники из раздела 8: 1-12 из раздела 9: 1-9	Дискуссия. Семинар в диалоговом режиме. Решение задач.
Тема 7. Организация деятельности службы безопасности объекта.	Проведение служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. Задачи службы безопасности организации. Организационная структура службы безопасности. Организация внутриобъектового режима предприятия. Организация охраны объектов предприятия. Организация и обеспечение защиты коммерческой тайны в организации. Организация инженерно-технической защиты. Организация безопасности функционирования информационных систем. Проверка наличия документов, дел и носителей информации. Организация служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. Проведение аналитико-разведывательной работы. Рекомендуемые источники из раздела 8: 1-12 из раздела 9: 1-9	Опрос. Решение задач. Семинар в диалоговом режиме.

Тема 8. Организация защиты информации при проведении совещаний по конфиденциальным вопросам, приеме посетителей и осуществлении научно-публицистической и рекламной деятельности.	Защита информации при проведении совещаний и переговоров. Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей. Организация защиты информации в кадровой службе. Общие правила работы с документами в организации. Организация защиты информации в работе пресс-служб, при осуществлении научно-публицистической и рекламной деятельности. Рекомендуемые источники из раздела 8: 1-12 из раздела 9: 1-9	Дискуссия. Решение задач. Семинар в диалоговом режиме.
Тема 9. Задачи, методы, стратегии, способы и средства защиты информации.	Задачи и методы обеспечения информационной безопасности. Стратегии защиты информации. Способы и средства защиты информации. Рекомендуемые источники из раздела 8: 1-12 из раздела 9: 1-9	Дискуссия. Решение задач. Семинар в диалоговом режиме.
Тема 10. Лицензирование и сертификация в области защиты информации	Правовая основа системы лицензирования и сертификации в Российской Федерации. Лицензирование деятельности по защите информации. Сертификация средств защиты информации. Рекомендуемые источники из раздела 8: 1-12 из раздела 9: 1-9	Дискуссия. Решение задач. Семинар в диалоговом режиме.
Тема 11. Аудит информационной безопасности систем, информационных технологий и организаций	Общая характеристика состояния аудиторской деятельности в области информационной безопасности. Основные виды и способы аудита информационной безопасности. Основные принципы проведения аудита информационной безопасности. Критерии аудита информационной безопасности. Организационно-методологические основы проведения аудита информационной безопасности. Взаимоотношение аудиторов с представителями проверяемой организации. Управление программой аудита информационной безопасности. Этапы проведения аудита информационной безопасности. Инструментальное обеспечение аудита информационной безопасности. Требования к кадровому обеспечению аудиторской деятельности в области информационной безопасности. Реализация первоочередных мероприятий по обеспечению аудиторской деятельности в области информационной безопасности. Рекомендуемые источники из раздела 8: 1-12 из раздела 9: 1-9	Дискуссия. Решение задач. Семинар в диалоговом режиме.

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Таблица 5

Наименование темы (раздела дисциплины)	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Тема 1. Введение в дисциплину «Правовое обеспечение кибербезопасности»	Система правовой защиты информации как предмет изучения. Место правовой защиты информации в системе комплексной защиты информации организации. Виды угроз информационной безопасности РФ. Источники угроз информационной безопасности. Задачи обеспечения информационной безопасности в различных сферах деятельности. Методы обеспечения информационной безопасности Российской Федерации. Функции и структура государственной системы обеспечения информационной безопасности. Правовые основы защиты информации. Основные направления и принципы обеспечения комплексной безопасности объектов информатизации.	Разбор вопросов по теме занятия из рабочей программы дисциплины. Изучение рекомендованных к занятию правовых актов и литературных источников.
Тема 2. Законодательство, подзаконные нормативные акты и основы технического регулирования Российской Федерации по вопросам защиты информации.	Законодательство Российской Федерации по вопросам защиты конфиденциальной информации. Системы технического регулирования по вопросам защиты информации. Регулирование ФСБ России по вопросам защиты конфиденциальной информации. Регулирование ФСТЭК России по вопросам защиты конфиденциальной информации. Регулирование защиты персональных данных. Отраслевые требования по вопросам защиты конфиденциальной информации.	Разбор вопросов по теме занятия из рабочей программы дисциплины. Изучение рекомендованных к занятию правовых актов и литературных источников.
Тема 3. Системный подход к обеспечению кибербезопасности объекта.	Разработка концепции и создание системы защиты информации на объекте. Основные направления защиты информации в кредитно-финансовой сфере. Создание системы обеспечения информационной безопасности объекта в кредитно-финансовой сфере.	Разбор вопросов по теме занятия из рабочей программы дисциплины. Изучение рекомендованных к занятию правовых актов и литературных источников.
Тема 4. Особенности	Государственная тайна и порядок	Разбор вопросов по теме

системы организационной защиты информации, составляющей государственную и коммерческую тайну.	отнесения к ней информации. Защита государственной тайны. Организация режима секретности, его особенности и содержание. Коммерческая тайна и порядок её определения. Организация работ с информацией, составляющей коммерческую тайну.	занятия из рабочей программы дисциплины. Изучение рекомендованных к занятию правовых актов и литературных источников.
Тема 5. Допуск к секретной информации.	Положения российского законодательства, регламентирующие допуск к государственной тайне. Процедура оформления и переоформления допусков к государственной тайне и ее документирование. Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне (формы учетной документации).	Разбор вопросов по теме занятия из рабочей программы дисциплины. Изучение рекомендованных к занятию правовых актов и литературных источников.
Тема 6. Организация доступа к информации ограниченного доступа.	Разрешительная система доступа к сведениям, составляющим коммерческую тайну предприятия (фирмы). Мероприятия по реализации разрешительной системы доступа к сведениям, составляющим коммерческую тайну предприятия (фирмы).	Разбор вопросов по теме занятия из рабочей программы дисциплины. Изучение рекомендованных к занятию правовых актов и литературных источников. Анализ правовой практики.
Тема 7. Организация деятельности службы безопасности объекта.	Проведение служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. Задачи службы безопасности организации. Организационная структура службы безопасности. Организация внутриобъектового режима предприятия. Организация охраны объектов предприятия. Организация и обеспечение защиты коммерческой тайны в организации. Организация инженерно-технической защиты. Организация безопасности функционирования информационных систем. Проверка наличия документов, дел и носителей информации. Организация служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. Проведение аналитико-разведывательной работы.	Разбор вопросов по теме занятия из рабочей программы дисциплины. Изучение рекомендованных к занятию правовых актов и литературных источников.
Тема 8. Организация защиты информации при проведении совещаний по конфиденциальным	Защита информации при проведении совещаний и переговоров. Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных	Разбор вопросов по теме занятия из рабочей программы дисциплины. Изучение рекомендованных к занятию правовых актов и

вопросам, приеме посетителей и осуществлении научно-публицистической и рекламной деятельности.	представителей. Организация защиты информации в кадровой службе. Общие правила работы с документами в организации. Организация защиты информации в работе пресс-служб, при осуществлении научно-публицистической и рекламной деятельности.	литературных источников.
Тема 9. Задачи, методы, стратегии, способы и средства защиты информации.	Задачи и методы обеспечения информационной безопасности. Стратегии защиты информации. Способы и средства защиты информации.	Разбор вопросов по теме занятия из рабочей программы дисциплины. Изучение рекомендованных к занятию правовых актов и литературных источников.
Тема 10. Лицензирование и сертификация в области защиты информации	Правовая основа системы лицензирования и сертификации в Российской Федерации. Лицензирование деятельности по защите информации. Сертификация средств защиты информации.	Разбор вопросов по теме занятия из рабочей программы дисциплины. Изучение рекомендованных к занятию правовых актов и литературных источников.
Тема 11. Аудит информационной безопасности систем, информационных технологий и организаций	Общая характеристика состояния аудиторской деятельности в области информационной безопасности. Основные виды и способы аудита информационной безопасности. Основные принципы проведения аудита информационной безопасности. Критерии аудита информационной безопасности. Организационно-методологические основы проведения аудита информационной безопасности. Взаимоотношение аудиторов с представителями проверяемой организации. Управление программой аудита информационной безопасности. Этапы проведения аудита информационной безопасности. Инструментальное обеспечение аудита информационной безопасности. Требования к кадровому обеспечению аудиторской деятельности в области информационной безопасности. Реализация первоочередных мероприятий по обеспечению аудиторской деятельности в области информационной безопасности.	Разбор вопросов по теме занятия из рабочей программы дисциплины. Изучение рекомендованных к занятию правовых актов и литературных источников.

6.2. Методическое обеспечение для аудиторной и внеаудиторной самостоятельной работы

Перечень примерных тем контрольной работы:

1. Основное содержание понятия «обеспечение кибербезопасности» человека на территории Российской Федерации; коммерческой и некоммерческой организаций; федерального органа исполнительной власти.
2. Определите функциональную направленность правового режима информационной безопасности для сети связи общего пользования.
3. Основные цели государственной политики в области обеспечения национальной безопасности.
4. Основные приоритеты устойчивого развития общества.
5. Основные факторы, обуславливающие влияние информационной безопасности на национальную безопасность.
6. Основное содержание понятия «информационная инфраструктура».
7. Основные угрозы безопасности информационной инфраструктуры.
8. Основные формы существования и свойства информации.
9. Особенности основных видов информации как объектов обеспечения безопасности.
10. Основные угрозы безопасности информации и способы их возможного проявления.
11. Основные источники права в области обеспечения безопасности информации.
12. Понятие «правового режима безопасности информации» и его содержание.
13. Раскройте содержание организационного обеспечения информационной безопасности Российской Федерации.
14. Какова система организационного обеспечения информационной безопасности?
15. Основные документы стратегического планирования.
16. Основные уполномоченные федеральные органы исполнительной власти в области информационной безопасности.
17. Раскройте содержание права на доступ к информации и его ограничение в целях защиты интересов личности, общества и государства.
18. Раскройте содержание понятия тайны.
19. Проведите классификацию тайн.
20. Приведите определение и признаки государственной тайны
21. Охарактеризуйте порядок отнесения сведений к государственной тайне и их засекречивания.
22. Как происходит распоряжение сведениями, составляющими государственную тайну?
23. Охарактеризуйте процедуру допуска к государственной тайне
24. Какой орган осуществляет контроль и надзор за обеспечением защиты государственной тайны?
25. Раскройте понятие коммерческой тайны и признаки информации, составляющей коммерческую тайну.

26. Какие права и обязанности установлены в законодательстве для обладателя информации, составляющей коммерческую тайну?
27. Какая предусмотрена ответственность за нарушение законодательства о коммерческой тайне?
28. Раскройте понятие и виды персональных данных.
29. Охарактеризуйте принципы и условия обработки персональных данных.
30. Какие права и обязанности установлены для оператора при обработке персональных данных?
31. Какой орган осуществляет контроль и надзор за обработкой персональных данных?
32. Перечислите полномочия государственного органа, осуществляющего контроль и надзор за обработкой персональных данных.
33. Понятие об информационном объекте и его элементах. Концептуальные основы формирования системы обеспечения информационной безопасности
34. Право и его роль в регулировании комплекса отношений в информационной сфере, объекты и субъекты правоотношений. Юридические особенности и свойства информации
35. Проблемы принятия международных конвенций по информационной безопасности. Исходные данные для формирования политики информационной безопасности предприятия
36. Отнесение сведений к коммерческой, служебной и профессиональной тайнам.
37. Критерии определения лицензируемых видов деятельности.
38. Уточнение перечня средств защиты информации, подлежащих сертификации.
39. Расследование компьютерных преступлений.
40. Судебная защита и самозащита прав обладателя собственности на информацию.
41. Реализация интеллектуальных прав.
42. Роль и возможности акционеров по формированию требований к информационной безопасности корпорации и контролю эффективности их выполнения.
43. Порядок проведения дознания по инцидентам нарушения информационной безопасности. Порядок возмещения ущерба от нарушения информационной безопасности.
44. Охрана территории предприятия и функциональных зон от проникновения нарушителей. Обеспечение порядка в местах массовых мероприятий. Профилактическая работа с участниками совещаний и заседаний по конфиденциальным вопросам.
45. Информационная безопасность персонала при работе со СМИ. Противодействие манипуляции в ходе восприятия потребительской рекламы и при заключении деловых соглашений.
46. Оценка достоверности сведений. Аналитическое выявление угроз информационной безопасности.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине содержится в разделе 2 «Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

Таблица 6

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ПКП-1 Способность использовать фундаментальные знания в области частного права и публичного права в современных условиях и оказывать помощь в реализации правовых норм субъектами гражданского оборота	Анализирует юридические факты и возникающие в связи с ними правоотношения, толкует и правильно применяет правовые нормы.	знать: нормы российского законодательства о информационной безопасности уметь: грамотно применять законодательство об информационной безопасности в правовой деятельности	Задание: Проведите анализ видов угроз кибер (информационной) безопасности Российской Федерации Задание: Проведите анализ отраслевых требований Центрального Банка России по вопросам защиты конфиденциальной информации.
	Принимает решения и совершает юридические действия в точном соответствии с законом.	знать: структуру, основные цели, задачи, организационные формы и методы информационной безопасности в России уметь: ориентироваться в основных понятиях кибербезопасности в Российской Федерации	Задание: Определите этапы создания системы обеспечения информационной безопасности объекта в кредитно-финансовой сфере. Задание: Осуществите разработку методов противодействия несанкционированному доступу к информации на объекте КФС
	Демонстрирует навыки анализа	знать: способы работы с	Задание: Изучите и предложите методы

	правоприменительной практики, обеспечивает реализацию норм процессуального права.	документами, относящимися к информационной безопасности уметь: грамотно и правильно составлять и оформлять документы о кибербезопасности	организация работ с информацией, составляющей коммерческую тайну Задание: Разработайте план мероприятий по обеспечению засекречивания и рассекречивания информации на объекте КФС.
ПКП -2 Способность действовать с учетом кризисных ситуаций в экономике, вызываемых рисками правового экономического характера, анализировать проблемные ситуации на рынке товаров, работ, услуг, а также выявлять правонарушения при осуществлении предпринимательской деятельности и давать юридически обоснованные предложения по их преодолению и устранению	1. Выявляет и предлагает способы устранения проблем, связанных с кризисными ситуациями в экономике.	знать: основы законодательства о информационной безопасности с точки зрения государственного регулирования экономики уметь: применять на практике законодательство Российской Федерации, в том числе Конституцию Российской Федерации, федеральные конституционные законы и федеральные законы, а также общепризнанные принципы, нормы международного права относительно кибербезопасности	Задание: Изучите различные виды мотивации сотрудников банковской сферы к выполнению требований по защите информации Задание: Изучите порядок организации и проведения служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа Задание: Сформулируйте организацию защиты информации при приеме в организации иностранных представителей. Задание: Изучите методы защиты помещений объекта с помощью технических средств охраны. Задание: Изучите структуру и функции органов защиты информации. в банковской сфере. Задание: Изучите различные стратегии защиты информации в банковской сфере Задание: Изучите требования к архитектуре системы защиты информации в банковской сфере.
	2. Анализирует проблемные ситуации на рынке	знать: способы соблюдения законодательства	Задание: Изучите процедуру оформления и переоформления допусков к

	товаров, работ, услуг, выявляет правонарушения при осуществлении предпринимательской деятельности	Российской Федерации субъектами права в сфере кибербезопасности уметь: применять нормативные правовые акты, реализовывать нормы материального и процессуального права в сфере информационной безопасности	государственной тайне и ее документирования. Задание: Изучите и предложите мероприятия по реализации разрешительной системы доступа к сведениям, составляющим коммерческую тайну на объекте информатизации КФС Задание: Изучите особенности подбора и подготовки кадров. Определите виды проверки персонала на благонадежность
	3. Находит пути решения ситуаций, связанных с преодолением правонарушений при осуществлении предпринимательской деятельности	знать: основы законодательства в области защиты интересов предпринимателей в сфере информационной безопасности уметь: представлять интересы предпринимателей в судах в сфере кибербезопасности	Задание: Изучите методы подбора сотрудников, ответственных за обеспечение безопасности информации в банковской сфере. Задание: Изучите методы оценки защищенности информации в банковской сфере. Задание: Изучите правовые основы системы лицензирования и сертификации в Российской Федерации Задание: Изучите организационно-методологические основы проведения аудита информационной безопасности в банковской сфере.

Типовые задания, необходимые для освоения компетенций при изучении дисциплины

Задание 1. Провести анализ стратегии, способов и средства защиты информации на объекте кредитно-финансовой сферы.

Задание 2. Определить возможного ущерба объекту информатизации кредитно-финансовой сферы (КФС) при реализации наиболее вероятных угроз.

Задание 3. Провести оценку эффективности системы обеспечения комплексной безопасности объекта информатизации кредитно-финансовой сферы.

Задание 4. Провести анализ методов противодействия несанкционированному доступу к информации на объекте кредитно-финансовой сферы.

Задание 5. Провести анализ методов организация работ с информацией, составляющей коммерческую тайну.

Задание 6. Разработать план мероприятий по обеспечению засекречивания и рассекречивания информации на объекте кредитно-финансовой сферы.

Задание 7. Изучить процедуру оформления и переоформления допусков к государственной тайне и ее документирования.

Задание 8. Изучить мероприятия по реализации разрешительной системы доступа к сведениям, составляющим коммерческую тайну на объекте информатизации кредитно-финансовой сферы.

Задание 9. Провести анализ методов проверок на полиграфе в финансовых организациях.

Задание 10. Изучить порядок организации и проведения служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа.

Задание 11. Определить методы защита помещений объекта с помощью технических средств охраны.

Задание 12. Провести оценку и изучение структуры и функций органов защиты информации в банковской сфере.

Задание 13. Провести изучение методов оценки защищенности информации в банковской сфере

Примерные вопросы для подготовки к зачету:

1. Что сказано в Законе Российской Федерации «О государственной тайне» о полномочиях органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты?
2. Что сказано в Законе Российской Федерации «О государственной тайне» об отнесение сведений к государственной тайне и их засекречивание?
3. Что сказано в Законе Российской Федерации «О государственной тайне» о степени секретности сведений и грифы секретности носителей этих сведений?
4. Что сказано в Законе Российской Федерации «О государственной тайне» об ограничении прав собственности предприятий, учреждений, организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием?
5. Что сказано в Законе Российской Федерации «О государственной тайне» о допуске должностных лиц и граждан к государственной тайне?
6. Что сказано в Законе Российской Федерации «О государственной тайне» об ответственности за нарушение законодательства Российской Федерации о государственной тайне?
7. Как реализуется разрешительная система доступа исполнителей к классифицированным документам и сведениям в организации?
8. Соблюдение, каких правил позволяет обеспечить эффективную работу разрешительной системы доступа исполнителей к классифицированным документам и сведениям, составляющим коммерческую тайну?
9. Каким требованиям должна отвечать разрешительная система доступа исполнителей к классифицированным документам и сведениям, составляющим

коммерческую тайну?

10. Какие мероприятия по реализации разрешительной системы доступа к сведениям, составляющим коммерческую тайну, должны выполняться в организации?
11. Какие внутренние организационно-распорядительные документы должны входить в перечень документов по защите информации в организации?
12. Назовите основные этапы профотбора сотрудников для работы на коммерческом предприятии.
13. Назовите группы людей, от которых могут исходить угрозы информационным ресурсам предприятия.
14. Какие функции должна выполнять служба безопасности по проверке сотрудников организаций на благонадежность?
15. Какие методы сбора информации о гражданине могут использовать сотрудники службы безопасности предприятия?
16. Какие методы используются для обучения сотрудников правилам работы с конфиденциальной информацией?
17. Как проводится инструктирование сотрудников правилам работы с конфиденциальной информацией?
18. Какими нормативными документами руководствуется служба безопасности в своей деятельности?
19. Как оценивается эффективность системы защиты организации?
20. Назовите, какие существуют виды охраны объектов?
21. Как происходит разглашение коммерческой тайны?
22. На каких принципах организуется защита информации, обрабатываемой в информационных системах?
23. Назовите основные этапы проведения совещания по конфиденциальным вопросам.
24. Кто несет ответственность за обеспечение безопасности ценной информации при проведении конфиденциального совещания?
25. Какие мероприятия необходимо провести для обеспечения защиты информации при проведении переговоров и совещаний по конфиденциальным вопросам?
26. Что следует сделать для обеспечения безопасности конфиденциальной информации в рекламно-выставочных материалах?
27. Что необходимо сделать для организации защиты персональных данных в кадровой службе?
28. Сформулируйте правила, которые следует соблюдать при работе с конфиденциальными документами.
29. Приведите структуру органов, ответственных за защиту информации.
30. Назовите и раскройте основные положения концепции построения и работы центров защиты информации.
31. Каково содержание работы центров защиты информации по формированию методологического базиса и инструментальных средств защиты?
32. Раскройте назначение центров защиты информации и основные задачи служб защиты информации.

33. Приведите структуру системы типовых документов по защите информации и дайте краткую характеристику основных типов документов.
34. Какие задачи решаются для защиты содержания обрабатываемой, хранимой и передаваемой информации?
35. Какие задачи решаются для защиты от информационного воздействия?
36. Какие цели ставятся при формировании стратегии защиты информации?
37. По каким критериям определяется число и содержание необходимых стратегий защиты информации?
38. Чем отличаются формальные от неформальных средств защиты информации?
39. Какие подсистемы входят в состав функционального построения системы защиты информации на объекте информатизации?
40. Какие функции возложены на ядро системы защиты информации?
41. В чем преимущества семи рубежной модели защиты объекта информатизации?
42. Какие компоненты входят в организационное построение системы защиты информации?
43. Какие основные задачи должна решать служба защиты информации?
44. Какие общие функции возлагаются на службу защиты информации?
45. Какими правами должна обладать служба защиты информации?
46. Какие основные виды деятельности по работе с персоналом должны осуществляться для защиты информатизации на объекте?
47. Какие основные показатели защищенности и оптимальные наборы мер защиты должны быть определены при построении общей модели управления системой защиты информации?
48. Какие основные задачи оперативного управления защитой информации должны быть решены в комплексных системах обработки данных?
49. Как классифицируются чрезвычайные ситуации, создающие угрозы безопасности защищаемой информации?
50. Какие меры по противодействию чрезвычайным ситуациям должна включать система защиты информации?
51. Что представляет собой процесс лицензирования деятельности по защите информации в Российской Федерации?
52. Какие нормативные правовые документы Российской Федерации, являются базовыми для лицензирования и сертификации в области защиты информации?
53. Какие государственные органы Российской Федерации уполномочены на ведение лицензионной деятельности в области защиты информации?

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

Нормативные акты

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.06.2006 г. №149 // СПС «Консультант Плюс» (в действующей редакции).

2. Стратегия национальной безопасности Российской Федерации (Утверждена Указом Президента Российской Федерации от 31 декабря 2015 года N 683).
3. Доктрина информационной безопасности Российской Федерации. Указ Президента РФ от 09.09.2000 г. № Пр-1895. // СПС «Консультант Плюс».
4. Федеральный закон «О государственной тайне» от 21.06.1993 г. №5485-1 (с изменениями и дополнениями). // СПС «Консультант Плюс» (в действующей редакции).
5. Федеральный закон «О персональных данных» от 27 июля 2006 года № 152-ФЗ. // СПС «Консультант Плюс» (в действующей редакции).
6. Федеральный закон «О коммерческой тайне» от 29.06.2004 г. № 98-ФЗ // СПС «КонсультантПлюс» (в действующей редакции).
7. Закон Российской Федерации «Об аудиторской деятельности» от 7 августа 2001 года №119-ФЗ. // СПС «Консультант Плюс» (в действующей редакции).
8. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 года. // СПС «Консультант Плюс» (в действующей редакции).
9. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 года. // СПС «Консультант Плюс» (в действующей редакции).

Рекомендуемая литература:

а) основная:

10. Баранова Е. К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Е.К. Баранова, А.В. Бабащ, - 4-е изд., перераб. и доп. – Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2019. – 322 с. – Режим доступа: <http://znanium.com/catalog/product/1009606>
11. Вдовин В.М. Информационные технологии в финансово-банковской сфере [Электронный ресурс] / В.М. Вдовин, Л.Е. Суркова – Москва: Дашков и К, 2018. – 304. – Режим доступа: <http://znanium.com/catalog/product/450752>

б) дополнительная:

12. Воронцова С.В. Обеспечение информационной безопасности в банковской сфере (Законность и правопорядок) [Электронный ресурс]: монография / С.В. Воронцова. – Москва: КноРус, 2017. – 160 с. – Режим доступа: <https://www.book.ru/book/921936>

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Сайт Центрального банка Российской Федерации: www.cbr.ru;
2. Сайт Федеральной службы по техническому и экспортному контролю: www.fstec.ru;
3. Сайт Федерального агентства по техническому регулированию и метрологии: www.gost.ru.

4. Электронная библиотека Финансового университета (ЭБ)// <http://elib.fa.ru/>
(<http://library.fa.ru/files/elibfa.pdf>)
5. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН»
<http://biblioclub.ru/>
6. «Деловая онлайн библиотека» издательства «Альпина Паблишер»//
<http://lib.alpinadigital.ru/en/library>
7. Научная электронная библиотека eLibrary.ru// <http://elibrary.ru>
8. Справочная правовая система Консультант Плюс». [Электронный ресурс. Режим доступа: <http://www.consultant.ru/>
9. Справочная правовая система «Гарант». [Электронный ресурс]. Режим доступа: <http://www.garant.ru/iv/>

10. Методические указания для обучающихся по освоению дисциплины

Наименование методических материалов для обучающихся	Год утверждения	Местонахождение материала (ссылка на ИОП, информационный стенд кафедры/филиала, др.)
Методические указания к лекциям	2021	http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx
Методические указания к практическим занятиям	2021	http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx
Методические указания к самостоятельной работе	2021	http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx
Методические указания по выполнению контрольной работы, проектной работы, расчетно-аналитической работы, домашнего творческого задания	2021	http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx

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

11.1. Комплект лицензионного программного обеспечения:

Продукты компании Microsoft, включая ОС Windows и Office.

11.2. Современные профессиональные базы данных и информационные справочные системы.

Электронное периодическое издание Справочная Правовая Система Консультант Бюджетные организации: версия Проф.

11.3. Сертифицированные программные и аппаратные средства защиты информации.

Сертифицированные программные и аппаратные средства защиты информации – не используются.

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

Учебная аудитория для проведения всех видов занятий, предусмотренных программой бакалавриата, оснащенная оборудованием и техническими средствами обучения.