МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КЕМЕРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Кузбасский гуманитарно-педагогический институт

Факультет истории и права

УТВЕРЖДАЮ
Декан ФИП

Л.А. Юрьева
«17» февраля 2025 г.

Рабочая программа дисциплины

К.М.02.02 Информационная безопасность и кибермошенничество

Код, название дисциплины

Направление подготовки
40.04.01 Юриспруденция

Направленность (профиль) программы
«Правовое обеспечение экономической деятельности в цифровой среде»

Программа магистратуры

Квалификация выпускника
магистр

Формы обучения
Очная, заочная

Год набора 2025

Новокузнецк 2025

Лист внесения изменений
в РПД *К.М.02.02 Информационная безопасность и кибермошенничество*

Сведения об утверждении:
утверждена Ученым советом факультета истории и права
(протокол Ученого совета факультета № 7 от 17.02.2025 г.)

для ОПОП 2025 года набора на 2025–2026 учебный год
по направлению подготовки 40.04.01 Юриспруденция
направленность (профиль) программы «Правовое обеспечение экономической деятельности в цифровой среде»

Одобрена на заседании методической комиссии факультета истории и права
(протокол методической комиссии факультета № 4 от 10.02.2025 г.)

Одобрена на заседании обеспечивающей кафедры информатики и общетехнических дисциплин

Оглавление

1. Цель дисциплины

В результате освоения дисциплины у обучающегося должна быть сформирована компетенция основной профессиональной образовательной программы магистратуры (далее – ОПОП): ОПК-7.

1.1 Формируемые компетенции

Таблица 1 – Формируемые дисциплиной компетенции.

Наименование вида компетенции *(универсальная, общепрофессиональная, профессиональная)*	Наименование категории (группы) компетенций	Код и название компетенции
Общепрофессиональная	Информационные технологии	ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности

1.2 Индикаторы достижения компетенций

Таблица 2 – Индикаторы достижения компетенций, формируемые дисциплиной.

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Дисциплины и практики, формирующие компетенцию ОПОП
ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	ОПК-7.1. Получает из различных источников, включая правовые базы данных, юридически значимую информацию, обрабатывает и систематизирует ее в соответствии с поставленной целью ОПК-7.2. Применяет информационные технологии для решения конкретных задач профессиональной деятельности ОПК-7.3. Демонстрирует готовность решать задачи профессиональной деятельности с учетом требований информационной безопасности	Информационные системы и цифровые технологии в профессиональной деятельности Методы и технологии искусственного интеллекта в профессиональной деятельности Преступления в сфере экономической деятельности и компьютерной информации Ознакомительная практика Преддипломная практика Подготовка к защите и защита выпускной квалификационной работы

1.3 Знания, умения, навыки (ЗУВ) по дисциплине

Таблица 3 – Знания, умения, навыки, формируемые дисциплиной.

Код и название компетенции	Индикаторы достижения компетенции, закрепленные за дисциплиной	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	ОПК-7.1. Получает из различных источников, включая правовые базы данных, юридически значимую информацию, обрабатывает и систематизирует ее в соответствии с поставленной целью ОПК-7.2. Применяет информационные технологии для решения конкретных задач профессиональной деятельности ОПК-7.3. Демонстрирует готовность решать задачи профессиональной деятельности с учетом требований информационной безопасности	**Знать:** ключевые концепции и принципы информационной безопасности; законодательные и нормативные акты, регулирующие информационную безопасность; современные угрозы и методы кибермошенничества; последствия кибератак и мошенничества; методы и средства защиты информации. **Уметь:** использовать правовые базы данных для поиска и анализа нормативных актов, связанных с информационной безопасностью; применять знания законодательства и нормативных актов в области информационной безопасности; устанавливать и настраивать базовые средства защиты; использовать современные инструменты и сервисы для обеспечения информационной безопасности. **Владеть:** антивирусным ПО и другими средствами защиты информации; методами аутентификации и авторизации; методами шифрования для защиты данных.

2. Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации

Таблица 4 – Объем и трудоёмкость дисциплины по видам учебных занятий.

Общая трудоёмкость и виды учебной работы по дисциплине, проводимые в разных формах	Объём часов по формам обучения		
	ОФО	ОЗФО	ЗФО
1 Общая трудоёмкость дисциплины	108	–	108
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	20	–	12
Аудиторная работа (всего):	20	–	12
в том числе:		–	
лекции	10	–	6
практические занятия, семинары	10	–	6
практикумы		–	
лабораторные работы		–	
в интерактивной форме		–	
в электронной форме		–	
Внеаудиторная работа (всего):		–	
в том числе, индивидуальная работа обучающихся с преподавателем		–	

подготовка курсовой работы / контактная работа		–	
групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем)		–	
творческая работа (эссе)		–	
3 Самостоятельная работа обучающихся (всего)	88	–	92
4 Промежуточная аттестация обучающегося: зачет		–	4

3. Учебно-тематический план и содержание дисциплины

3.1 Учебно-тематический план

Таблица 5 – Учебно-тематический план *очной* формы обучения.

№ п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость (*всего час.*)	Трудоёмкость занятий (час.)			Формы текущего контроля и промежуточной аттестации успеваемости
			ОФО			
			Аудиторные занятия		СРС	
			лекц.	практ.		
1	Введение в информационную безопасность. Основные понятия и термины. История и эволюция информационной безопасности. - Роль информационной безопасности в современном обществе.	20	2	0	18	*Устный опрос*
2	Основные угрозы и риски информационной безопасности. Типы угроз: вирусы, трояны, фишинг, DDOS- атаки и др. Примеры реальных инцидентов и их последствия.	22	2	2	18	*Отчет по практической работе № 1*
3	Законодательство и нормативные акты в области информационной безопасности. Российское и международное законодательство. Права и обязанности пользователей и организаций. Ответственность за нарушение информационной безопасности.	22	2	2	18	*Отчет по практической работе № 2*
4	Кибермошенничество. Основные виды кибермошенничества. Методы и техники, используемые кибермошенниками. Примеры распространенных схем мошенничества. Защита от кибермошенничества.	20	2	2	16	*Отчет по практической работе № 3*
5	Технологии и методы защиты информации. Основы криптографии и шифрования. Антивирусное ПО и средства защиты. Методы аутентификации и авторизации.	24	2	4	18	*Отчет по практической работе № 4, 5, Реферат по всем разделам дисциплины*
	Промежуточная аттестация					Зачёт
	Всего:	**108**	**10**	**10**	**88**	

Таблица 5.1 – Учебно-тематический план *заочной* формы обучения.

№ п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость (*всего час.*)	Трудоёмкость занятий (час.)			Формы текущего контроля и промежуточной аттестации успеваемости
			ЗФО			
			Аудиторные занятия		СРС	
			лекц.	практ.		
1	Введение в информационную безопасность. Основные понятия и термины. История и эволюция информационной безопасности. - Роль информационной безопасности в современном обществе.	18	1	0	18	*Устный опрос*
2	Основные угрозы и риски информационной безопасности. Типы угроз: вирусы, трояны, фишинг, DDOS- атаки и др. Примеры реальных инцидентов и их последствия.	19	1	0	18	*Устный опрос*
3	Кибермошенничество. Основные виды кибермошенничества. Методы и техники, используемые кибермошенниками. Примеры распространенных схем мошенничества. Защита от кибермошенничества.	19	1	0	18	–
4	Законодательство и нормативные акты в области информационной безопасности. Российское и международное законодательство. Права и обязанности пользователей и организаций. Ответственность за нарушение информационной безопасности.	23	1	2	20	*Отчет по практической работе № 1*
5	Защита информации. Технологии и методы защиты информации. Основы криптографии и шифрования. Антивирусное ПО и средства защиты. Методы аутентификации и авторизации.	23	1	4	18	*Отчет по практической работе № 2, 3, Реферат по всем разделам дисциплины*
	Промежуточная аттестация **(4 час.)**					Зачёт
	Всего:	**108**	**6**	**6**	**92**	

4. Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации

Для положительной оценки по результатам освоения дисциплины обучающемуся необходимо выполнить все установленные виды учебной работы. Оценка результатов работы обучающегося в баллах (по видам) приведена в таблице 7.

Таблица 6 – Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам (БРС).

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации (шкала и показатели оценивания)	Баллы (мин.-макс.)
Текущая учебная работа				
Текущая учебная работа в семестре (посещение занятий по расписанию и выполнение заданий)	**max 60-80** баллов приведенной шкалы	Лекционные занятия	**1 балл** – посещение 1 лекционного занятия	Количество баллов варьируется в зависимости от формы обучения
		Практические занятия	**2 балла** – посещение 1 практического занятия и выполнение работы на 51–65% **3 балла** – посещение 1 занятия и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 85,1–100%	
		Тестирование, решение кейс-заданий и пр.	**18 баллов** (51–65% правильных ответов) **22 балла** (66–84% правильных ответов) **36 баллов** (85–100% правильных ответов)	
Промежуточная аттестация				
Промежуточная аттестация	**max 40-20** баллов приведенной шкалы	Теоретические вопросы	**10 баллов** (пороговое значение) **20 баллов** (максимальное значение)	10–20
		Решение практико-ориентированный заданий, кейсов и пр.	**10 баллов** (пороговое значение) **20 баллов** (максимальное значение)	10–20
Суммарная оценка по дисциплине: сумма баллов текущей и промежуточной аттестации				**51–100 б.**

Для оценивания результатов учебной работы студентов заочной формы обучения преподавателем может применяться *поправочный коэффициент* с учетом количества оценочных мероприятий.

В промежуточной аттестации оценка выставляется в ведомость в 100-балльной шкале и в буквенном эквиваленте (таблица 7.1).

Таблица 4.1 – Соотнесение 100-балльной шкалы и буквенного эквивалента оценки.

Сумма набранных баллов	*Уровни освоения дисциплины и компетенций*	*Экзамен*		*Зачет*
		Оценка	*Буквенный эквивалент*	*Буквенный эквивалент*
86–100	Продвинутый	5	отлично	Зачтено
66–85	Повышенный	4	хорошо	
51–65	Пороговый	3	удовлетворительно	
0–50	Первый	2	неудовлетворительно	Не зачтено

5. Материально-техническое, программное и учебно-методическое обеспечение дисциплины

5.1 Учебная литература

Основная учебная литература:

1. Информационная безопасность : учебное пособие / составители И. Б. Тесленко [и др.] ; под редакцией И. Б. Тесленко. – Владимир : ВлГУ, 2023. – 212 с. – ISBN 978-5-9984-1783-2. – URL: https://reader.lanbook.com/book/434282 (дата обращения: 20.01.2025). – Текст : электронный

2. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. – Ростов-на-Дону: Южный федеральный университет, 2016. – 74 с.: ISBN 978-5-9275-2364-1. – Текст : электронный. – URL: https://znanium.com/catalog/product/997105 (дата обращения: 20.01.2025). – Режим доступа: по подписке.

Дополнительная учебная литература:

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное

пособие / Е.К. Баранова, А.В. Бабаш. – 4-е изд., перераб. и доп. – Москва : РИОР : ИНФРА-М, 2024. – 336 с. – (Высшее образование). – ISBN 978-5-369-01761-6. – URL: https://znanium.ru/catalog/product/2082642 (дата обращения: 20.01.2025). – Текст : электронный.

2. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. – Новосибирск : НГТУ, 2019. – 83 с. – ISBN 978-5-7782-3918-0. – URL: https://e.lanbook.com/book/152227 (дата обращения: 20.01.2025). – Текст : электронный.

3. Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации: учебник / сост. И. Г. Дровникова, А. В. Калач, И. И. Лившиц [и др]. – Воронеж : Научная книга, 2022. – 304 с. – ISBN 978-5-4446-1743-4. – URL: https://znanium.com/catalog/product/1999941 (дата обращения: 20.01.2025). – Текст: электронный.

5.2 Материально-техническое и программное обеспечение дисциплины

Учебные занятия по дисциплине проводятся в учебных аудиториях КГПИ КемГУ:

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений
1	2
410 Учебная аудитория (мультимедийная) для проведения: – занятий лекционного типа; – занятий семинарского (практического) типа; – групповых и индивидуальных консультаций; – текущего контроля и промежуточной аттестации; – государственной итоговой аттестации. **Специализированная (учебная) мебель**: доска меловая, кафедра, моноблоки аудиторные. **Оборудование для презентации учебного материала:** *стационарное* – компьютер, экран, проектор, акустическая система. Количество посадочных мест – 46. **Используемое программное обеспечение**: LibreOffice (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО). **Интернет с обеспечением доступа в ЭИОС.**	654079, Кемеровская область, г. Новокузнецк, Центральный район, просп. Металлургов, дом № 19
502 Компьютерный класс / Лаборатория компьютерного моделирования. Учебная аудитория (мультимедийная) для проведения: – занятий лекционного типа; – занятий семинарского (практического) типа; – занятий лабораторного типа; – учебных и производственных практик; – курсового проектирования (выполнения курсовых работ); – групповых и индивидуальных консультаций; – самостоятельной работы; – текущего контроля и промежуточной аттестации;	654079, Кемеровская область, г. Новокузнецк, Центральный район, просп. Металлургов, дом № 19

– государственной итоговой аттестации. **Специализированная (учебная) мебель**: доска меловая, столы компьютерные, стулья. **Оборудование для презентации учебного материала**: *стационарное* – компьютер, экран, проектор, наушники. **Лабораторное оборудование**: *стационарное* – компьютеры для обучающихся (20 шт.). Количество посадочных мест – 20. **Используемое программное обеспечение**: LibreOffice (свободно распространяемое ПО), AUTOCAD (Коробочная лицензия № 0730450), AlteraQuartusPrimeLite (бесплатное ПО), AutoLOGIC (разработка составителя Шехтмана), BloodshedDevC++ 4.9.9.2 (свободно распространяемое ПО), FoxitReader (свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО), Java (бесплатная версия), MASM32 (свободно распространяемое ПО), ModelSimAltera (бесплатная версия), Mpich 2 (свободно распространяемое ПО), Netbeans IDE 7.0.1 для Firefox (свободно распространяемое ПО), OpenProject (бесплатная версия), Opera 12 (свободно распространяемое ПО), Oracle VM VirtualBox (бесплатная версия), Paint.NET (свободно распространяемое ПО), PostgreSQL (свободно распространяемое ПО), Qt (свободно распространяемое ПО), Eclipse (свободно распространяемое ПО), Quick-TUTOR (разработка составителя), Scilab (свободно распространяемое ПО), SWI-Prolog (свободно распространяемое ПО), TexasInstruments TINA-TI (бесплатная версия), UML-диаграммы (бесплатная версия), Консультант Плюс (отечественное ПО, договор об инфо поддержке 1.04.2007), OMRON CX-One LITE v4.26 (демонстрационная версия), пакет программирования панелей оператора OMRON серии NBNB-Designer v1.20 (демонстрационная версия), ППП nanoCAD, nanoCADЭлектро, nanoCAD СКС, nanoCAD Схемы (отечественное ПО, демонстрационная версия), ППП GENESIS 32 (демонстрационная версия), GPSS WorldStudentEdition (учебная версия), XAMPP (свободно распространяемое ПО), Denwer (свободно распространяемое ПО), T-FlexCAD (учебная версия), 3ds MaxDesign (Коробочная лицензия № 0730450), Галактика (отечественное ПО, договор 2012/339 от 04.12.2012, Акт 000017 27.02.2013), Среда статистических вычислений Rv.4.0.2 (свободно распространяемое ПО). **Интернет с обеспечением доступа в ЭИОС.**	

5.3 Современные профессиональные базы данных и информационные справочные системы

1. База данных правовых актов «Консультант Плюс»: комп. справ. правовая система / компания «КонсультантПлюс». – электрон. прогр. – URL: http://www.consultant.ru, свободный
2. Судебные и нормативные акты РФ. – URL: https://sudact.ru, свободный.

6. Иные сведения и (или) материалы

6.1 Примерные темы письменных учебных работ

Темы рефератов:

1. Понятие и основные аспекты информационной безопасности в современном обществе.
2. Кибермошенничество: виды, методы и способы защиты.
3. Роль социальных сетей в распространении кибермошенничества.
4. Правовые аспекты борьбы с киберпреступностью: международный и национальный уровень.
5. Психология кибермошенников: мотивация и стратегии обмана.
6. Информационная безопасность в образовательных учреждениях: вызовы и решения.
7. Этические вопросы в области кибербезопасности.
8. Влияние кибермошенничества на личные данные и конфиденциальность граждан.
9. Актуальные угрозы информационной безопасности для бизнеса.
10. Технологические решения для защиты от кибермошенничества.
11. Роль государственного регулирования в обеспечении информационной безопасности.
12. Кибербезопасность и защита прав человека в цифровую эпоху.
13. Образовательные программы по информационной безопасности для гуманитариев.
14. Будущее кибермошенничества.
15. Информационная безопасность в контексте глобализации и цифровизации общества.
16. Биометрические системы идентификации
17. Анализ программ родительского контроля. Родительский контроль в составе антивирусных программ и операционных систем
18. Основные психолого-педагогические приемы и средства по обеспечению информационной безопасности детей в Интернете.
19. Утилизация данных: проблемы повторного использования.
20. Средства взлома парольных систем и противодействие им.

6.2 Примерные вопросы и задания / задачи для промежуточной аттестации

Форма промежуточной аттестации – зачёт.

Таблица 5 – Типовые (примерные) контрольные вопросы и задания.

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания и (или) задачи
Введение в информационную безопасность.		
Основные понятия и термины. История и эволюция информационной безопасности. Роль информационной безопасности в современном обществе.	1. Какие основные понятия и термины используются в области информационной безопасности? 2. Каковы ключевые этапы эволюции информационной безопасности и их влияние на современные практики? 3. Какова роль информационной безопасности в обеспечении устойчивости организаций в условиях цифровой трансформации? 4. Какие социальные и экономические последствия могут	1. Найдите в интернете и опишите три исторических события, которые существенно повлияли на развитие информационной безопасности. 2. Объясните на примерах из повседневной жизни, почему информационная безопасность важна для современного общества.

	возникнуть в результате недостаточной информационной безопасности?	
Основные угрозы и риски информационной безопасности.		
Типы угроз: вирусы, трояны, фишинг, DDOS- атаки и др. Примеры реальных инцидентов и их последствия.	5. Какие основные характеристики различают вирусы, трояны и фишинг в контексте киберугроз, и как они воздействуют на информационные системы? 6. Каковы механизмы проведения DDoS-атак, и какие последствия они могут иметь для организаций и пользователей? 7. Какие меры предосторожности и защиты могут быть предприняты для снижения рисков, связанных с вирусами, троянами и фишингом?	3. Провести исследование и подготовить краткий отчет о реальном инциденте, связанным с кибератаками, описав его основные характеристики, методы, использованные мошенниками, и последствия для жертв. 4. Включить в отчет рекомендации по предотвращению подобных атак.
Кибермошенничество		
Основные виды кибермошенничества.	8. Какие основные виды кибермошенничества существуют и чем они отличаются друг от друга? 9. Каковы характерные признаки кибермошенничества?	5. Найдите и проанализируйте один реальный случай кибермошенничества. Опишите, как произошла атака, какие методы использовались злоумышленниками, какие последствия она имела для организации или пользователей. Опишите, какие меры были предприняты для устранения последствий и предотвращения подобных инцидентов в будущем.
Методы и техники, используемые кибермошенниками. Примеры распространенных схем мошенничества.	10. Какие методы и техники используют кибермошенники для осуществления своих схем? 11. Какие примеры распространенных схем мошенничества можно выделить, и каковы их последствия для жертв?	6. Опишите, как работает фишинговая атака, и приведите пример, с которым вы могли бы столкнуться в интернете. 7. Проанализируйте реальный случай кибермошенничества из новостей и предложите способы, как можно было бы предотвратить этот инцидент.
Защита от кибермошенничества.	12. Какие меры предосторожности и защиты могут быть приняты для предотвращения кибермошенничества? 13. Какие технологии и инструменты используются для мониторинга и предотвращения кибермошеннических атак?	8. Проведите анализ и составьте отчет о трех распространенных схемах кибермошенничества, описав методы защиты, которые могут помочь предотвратить их, с использованием доступных онлайн-ресурсов. 9. Опишите три основных признака фишингового письма и объясните, как их распознать. 10. Разработайте план действий на случай, если вы стали жертвой кибермошенничества.
Законодательство и нормативные акты в области информационной безопасности.		
Российское и международное законодательство.	14. Какие ключевые законодательные акты регулируют сферу информационной	11. Найдите основные положения российского закона, регулирующего защиту

Права и обязанности пользователей и организаций.	безопасности в России и за рубежом? 15. Каковы права и обязанности пользователей в контексте информационной безопасности?	персональных данных. 12. Опишите права и обязанности пользователей при работе с конфиденциальной информацией в организации.
Ответственность за нарушение информационной безопасности.	16. Какова ответственность организаций за нарушение норм и правил информационной безопасности? 17. Как международные соглашения влияют на национальное законодательство в области информационной безопасности?	13. Приведите примеры юридических последствий для организаций, нарушивших требования информационной безопасности. 14. Объясните, какие меры ответственности могут быть применены к пользователям за нарушение правил информационной безопасности.
Защита информации.		
Технологии и методы защиты информации.	18. Каково назначение технических средств защиты информации? 19. Как программные средства защиты информации помогают в обнаружении и предотвращении угроз безопасности цифровых данных? 20. В чем заключается роль организационных средств в обеспечении информационной безопасности?	15. На примере конкретной организации проведите анализ возможностей технических, программных и организационных средств защиты информации. 16. Объясните, что такое двухфакторная аутентификация и как ее настроить на личном устройстве.
Основы криптографии и шифрования.	21. Какие основные принципы криптографии и шифрования используются для защиты информации? 22. Какие существуют основные алгоритмы шифрования?	17. Приведите примеры методов шифрования данных и объясните, как они помогают защитить информацию Зашифровать текст с использованием одного из классических методов шифрования, таких как шифр Цезаря или шифр Виженера. 18.Провести сравнительный анализ двух современных криптографических алгоритмов (например, AES и RSA) .
Антивирусное ПО и средства защиты.	23. Что такое компьютерный вирус? 24. Каково значение антивирусного программного обеспечения в обеспечении информационной безопасности?	19.Проведите анализ функциональных возможностей одного из популярных антивирусных программ, интерфейса и методов обнаружения угроз. 20. Установите и настройте антивирусное программное обеспечение на своем компьютере. Проведите полное сканирование системы и составьте отчет о найденных угрозах
Методы аутентификации и авторизации.	25. Какие методы аутентификации и авторизации применяются для защиты доступа к информации? 26. Какие технологии	21. Создайте учетную запись на одном из популярных веб-сайтов и продемонстрируйте процесс регистрации с использованием

	аутентификации и авторизации наиболее эффективны для защиты информационных систем?	электронной почты и пароля. 22. Проведите анализ различных уровней доступа на примере социальной сети, определив, какие действия могут выполнять пользователи с разными ролями (например, администратор, пользователь, гость).

Примерные кейс-задания для оценки освоения компетенций, закрепленных за дисциплиной:

Компетенция 1

ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности.

Кейс-задание 1: работа с правовыми базами данных.

Ваша юридическая фирма подписала контракт с онлайн-сервисом правовых баз данных для доступа к актуальной информации о законодательстве и судебной практике. Вы, как юрист, должны использовать этот сервис для подготовки документов и анализа правовых вопросов. Однако Вы заметили, что для доступа к некоторым материалам требуется дополнительная аутентификация.

Вопрос 1: Какие действия необходимо предпринять, чтобы получить доступ к дополнительным материалам в правовой базе данных?

1. Выслать запрос на доступ к администратору сервиса.
2. Использовать свой личный аккаунт для входа.
3. Использовать пароль администратора.

Правильный ответ:

1. Выслать запрос на доступ к администратору сервиса.

Вопрос 2: Какой метод аутентификации может быть наиболее безопасным для защиты Ваших данных в правовой базе?

1. Использование пароля.
2. Двухфакторная аутентификация, требующая подтверждения через телефон.
3. Использование пароля администратора.

Правильный ответ:

2. Двухфакторная аутентификация, требующая подтверждения через телефон.

Кейс-задание 2: защита личных данных в базе данных.

Вы работаете в юридической фирме, которая собирает в базу данных личные данные клиентов для предоставления услуг. Ваша задача – обеспечить безопасность этих данных и соблюдение законодательства о защите информации.

Вопрос 1: Какой метод аутентификации наиболее безопасен для защиты личных данных клиентов?

A) Использование простого пароля.

B) Двухфакторная аутентификация (2FA).

C) Отправка пароля по электронной почте.

D) Использование одного и того же пароля для всех аккаунтов.

Правильный ответ:

B) Двухфакторная аутентификация (2FA).

Вопрос 2: Какое законодательство необходимо учитывать при работе с личными данными клиентов?

A) Законодательство о защите авторских прав.

B) Законодательство о защите персональных данных.

C) Законодательство о налогах.

D) Законодательство о защите прав потребителей.

Правильный ответ:

B) Законодательство о защите персональных данных.

Составитель (и): Дробахина А.Н., канд. пед. наук, доцент кафедры ИОТ

(*фамилия, инициалы и должность преподавателя (ей)*)