Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.24 «Управление цифровой безопасностью»
(индекс, наименование дисциплины в соответствии с учебным планом)

38.05.01 Экономическая безопасность
(код, наименование направления подготовки/специальности)

Экономико-правовое обеспечение экономической безопасности
(наименование образовательной программы)

Очная, заочная формы обучения
(форма обучения)

Год набора - 2026

Санкт-Петербург

Автор(ы)-составитель(и) РПД:

Будко Александра Павловна, старший преподаватель кафедры безопасности

Заведующий кафедрой:

Дмитриев Александр Викторович, доктор экономических наук, доцент, заведующий кафедрой безопасности

Рабочая программа дисциплины Б1.В.24 «Управление цифровой безопасностью» одобрена на заседании кафедры безопасности факультета безопасности и таможни СЗИУ РАНХиГС.

протокол № 8 от «13» апреля 2026 г.

СОДЕРЖАНИЕ

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

Дисциплина Б1.В.24 «Управление цифровой безопасностью» обеспечивает формирование у обучающихся следующих универсальных, общепрофессиональных и профессиональных компетенций*:

ОТФ/ТФ и реквизиты ПС *(при наличии)***	**Код компетенции ****	**Наименование Компетенции ****	**Код индикатора достижения компетенций ****	**Наименование индикатора достижения компетенций ****	**Образовательный результат ****
08.021 специалист по финансовому мониторингу (в сфере противодействия легализации доходов, полученных преступным путем, и финансированию терроризма) утв. приказом Минтруда и социальной защиты РФ от 24 июля 2015 года №512н B/02.7 Анализ материалов финансовых расследований, схем отмывания преступных доходов в целях ПОД/ФТ	ПКс-17	Способен выявлять цифровые угрозы	ПКс-17.1	Знает цифровые технологии, сетевые структуры и платформы и методы управления цифровой репутаций	ПКс-17.1.ТД.7 Выявление типологий подозрительной деятельности в целях ПОД/ФТ ПКс-17.1.У.8 Осуществлять сбор дополнительной информации ПКс-17.1.Зн.2 Приемы и способы поиска и отбора информации в информационно-телекоммуникационной сети "Интернет"

** Дисциплина может формировать компетенцию полностью или частично.*
***Должно соответствовать Приложению 1 к образовательной программе*

2. Объем и место дисциплины в структуре образовательной программы

Объем дисциплины

Объем дисциплины и виды учебной работы.

Общая трудоемкость дисциплины (очная/заочная) составляет 4 зачетные единицы / 144 академических часов / 108 астрономических часов.

Дисциплина реализуется с применением дистанционных образовательных технологий (далее – ДОТ). Доступ к системе дистанционных образовательных технологий осуществляется каждым обучающимся самостоятельно с любого устройства на портале:

https://lms.ranepa.ru/. Пароль и логин к личному кабинету/профилю предоставляется студенту в деканате.

Очная форма: Теоретические занятия (лекции) проводятся по потокам. Общий объем лекционного курса составляет 16 академических часов.

Практические занятия организуются по группам. Общий объем практических занятий 16 академических часов. Программой предусмотрена самостоятельная работа студентов в объеме 103 академических часа.

Заочная форма: Общий объем лекционного курса составляет 8 академических часа.

Практические занятия организуются по группам в виде семинаров в диалоговом режиме. Общий объем практических занятий 8 академических часов.

Программой предусмотрена самостоятельная работа студентов в объеме 124 академических часа. В рамках самостоятельной работы студенты изучают теоретический материал в целях подготовки к устному опросу и тестированию, выполняют практические задания, разрабатывают итоговый проект.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.24 «Управление цифровой безопасностью» входит в обязательную часть, формируемая участниками образовательных отношений дисциплин по специальности 38.05.01 «Экономическая безопасность», направленность (профиль) «Экономико-правовое обеспечение экономической безопасности». Изучается во 2-ом семестре (второй семестр 1-го курса). По заочной форме изучается на 1 курсе в зимнюю и летнюю сессии.

Дисциплина Б1.В.24 «Управление цифровой безопасностью» является базисной и имеет усиленную практическую направленность.

Объем дисциплины, реализуемый с применением СДО: количество академических часов, выделенных на самостоятельную работу обучающихся: всего с применением СДО – 103/124 ак.ч.

Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при подготовке и сдаче государственного экзамена.

Формой промежуточной аттестации в соответствии с учебным планом является **зачет с оценкой**.

3. Содержание и структура дисциплины

3.1. Структура дисциплины
Очная форма обучения

№ п/п	Наименование тем и (или) разделов		Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
		ВСЕГО	Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Кат тэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Тема 1	Цифровая репутация организации и личности	**16**		**2**		**2**								**12**	Т, ПЗ, УО
Тема 2	Основные угрозы цифровой репутации	17		2		2								13	Т, ПЗ, УО

Тема 3	Управление репутационными рисками	17		2		2							13	Т, ПЗ, УО
Тема 4	Управление личным цифровым следом	17		2		2							13	Т, ПЗ, УО
Тема 5	Правовая защита репутации в цифровой среде	17		2		2							13	Т, ПЗ, УО
Тема 6	Организационные инструменты цифровой безопасности	17		2		2							13	Т, ПЗ, УО
Тема 7	Технологии мониторинга и анализа репутации.	17		2		2							13	Т, ПЗ, УО
Тема 8	Комплексное управление инцидентами и восстановление репутации	17		2		2							13	Т, ПЗ, УО
Промежуточная аттестация														Зачет с оценкой
Итого		144		16		16				9			103	

Зачная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Кат тэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Тема 1	Цифровая репутация организации и личности	**18**		**1**		**1**								**16**	Т, ПЗ, УО
Тема 2	Основные угрозы цифровой репутации	18		1		1								16	Т, ПЗ, УО
Тема 3	Управление репутационными рисками	18		1		1								16	Т, ПЗ, УО

Тема 4	Управление личным цифровым следом	17		1		1							15	Т, ПЗ, УО
Тема 5	Правовая защита репутации в цифровой среде	18		1		1							16	Т, ПЗ, УО
Тема 6	Организационные инструменты цифровой безопасности	17		1		1							15	Т, ПЗ, УО
Тема 7	Технологии мониторинга и анализа репутации.	17		1		1							15	Т, ПЗ,УО
Тема 8	Комплексное управление инцидентами и восстановление репутации	17		1		1							15	Т, ПЗ,УО
Промежуточная аттестация														Зачет с оценкой
Итого		144		8		8				4			124	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции.

ЛР – лабораторные работы.
ПЗ – практические занятия (за исключением лабораторных работ).
ИК – индивидуальные консультации.
КСР – контроль самостоятельной работы
КЭ – консультации перед экзаменом
Каттэк – контактная работа на аттестацию в период экзаменационных сессий
Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения
СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.
СРэк – самостоятельная работа на подготовку к экзамену.
СР – самостоятельная работа в семестре на подготовку к учебным занятиям.
Т – тест.

В процессе обучения применяются следующие интерактивные формы: лекция-диалог, работа в малых группах, кейс-анализ, дискуссия, деловая игра, индивидуальное задание, групповое обсуждение, практикум, ролевая игра, разработка чек-листов. Темы 1-8 могут быть освоены с применением ЭО и ДОТ с контролем в системе электронного обучения Академии.

3.2. Содержание дисциплины

Тема 1. Цифровая репутация организации и личности (ПКс-17.1)

Теоретическая часть:

Понятие цифровой репутации, её отличие от имиджа и бренда. Репутационный капитал: структура (доверие клиентов, партнёров, регуляторов, сотрудников). Метрики оценки репутации: Индекс потребительской лояльности, медиаиндекс, стоимость привлечения клиента, индекс лояльности, рейтинги надёжности. Экономические последствия потери репутации: отток клиентов, падение капитализации, рост операционных расходов, штрафы, уголовное преследование руководства. Личная репутация специалиста по экономической безопасности: роль в карьерном росте, допуске к сведениям, доверии со стороны работодателя. Взаимосвязь цифровой безопасности и репутации: инциденты как триггеры репутационных потерь.

Практическая часть:

Кейс анализ утечки персональных данных финансовой организации — расчёт финансовых потерь (отток клиентов, штрафы). Построение карты репутационных угроз для типовой организации (банк, онлайн ритейлер, ИТ компания) и её руководителя. Дискуссия: «Может ли личная репутация сотрудника стать системным риском для организации?».

Тема 2. Основные угрозы цифровой репутации (ПКс-17.1)

Классификация угроз: внешние (кибератаки, фейк ньюс, дипфейки, атаки конкурентов) и внутренние (ошибки сотрудников, инсайдеры, публикации в соцсетях). Новые угрозы личным данным: Сим свопинг – перевыпуск SIM карты злоумышленниками для получения SMS кодов доступа к банкам, соцсетям, криптокошелькам; Сбор биометрии из открытых источников – использование фото, видео, голоса из соцсетей для создания дипфейков или обхода биометрической аутентификации; Уязвимости умных устройств (IoT) – взлом камер, колонок, часов для слежки, сбора данных о привычках и местоположении; Трекинг и профилирование без согласия – сбор данных мобильными приложениями, сайтами, ОС для формирования профилей (местоположение, интересы); Утечки через облачные синхронизации – компрометация одного аккаунта даёт доступ к заметкам, фото, паролям, документам; Фишинг через QR коды – подмена QR кодов в общественных местах (кафе, парковки) для кражи данных или установки вредоносного ПО; Дипфейк звонки и видео – использование нейросетей для подделки голоса или видео руководителя с целью мошенничества или дискредитации; Угрозы, связанные с использованием ИИ сервисов: утечка данных при работе с публичными нейросетями, риски использования корпоративных данных в неконтролируемых облачных ИИ сервисах; Угрозы OSINT-сбора: злоумышленники используют открытые источники (соцсети, форумы, базы

данных и др.) для сбора информации о сотрудниках, структуре компании, используемых технологиях. Факторы, усиливающие репутационный ущерб: скорость распространения, виральность, отсутствие плана реагирования.

Практическое занятие

Работа в малых группах: составление перечня актуальных репутационных угроз для организации (онлайн кинотеатр) и её ключевых сотрудников с учётом новых угроз. Анализ реального инцидента: взлом аккаунта известного человека и публикация оскорбительного контента — последствия для личной и корпоративной репутации. Кейс: «Сим свопинг и утечка корпоративных данных» – студенты анализируют, как компрометация номера телефона руководителя привела к доступу к корпоративной почте и финансовым потерям. Кейс по OSINT: студентам предоставляется открытый профиль человека (публичный). Они должны за 10 минут найти максимум информации (должность, контакты, место работы, связи) и обсудить, как эта информация может быть использована злоумышленниками. Индивидуальное задание: описать 3 угрозы личной цифровой репутации, актуальные для студентов, с учётом всех возможных угроз

Тема 3. Управление репутационными рисками (ПКс-17.1)

Понятие репутационного риска, этапы управления рисками (идентификация, оценка, выбор мер, мониторинг). Качественная оценка: матрица «вероятность – последствия», экспертные оценки. Количественная оценка: расчёт ожидаемых потерь (SLE, ARO, ALE) применительно к репутационным последствиям. Стратегии реагирования: принятие, снижение, передача, избегание. Связь технических средств защиты с управлением рисками: внедрение антивирусов, DLP, SIEM, WAF, средств защиты от DDoS как способ снижения вероятности и последствий инцидентов. Роль страхования репутационных рисков.

Практическое занятие (2 ч)

Построение матрицы рисков для условной компании (интернет-магазин) по трём угрозам: утечка данных клиентов, взлом сайта, негативный отзыв топ блогера. Деловая игра: «Выбор стратегии реагирования» — каждая группа предлагает стратегию для одного риска с обоснованием, включая предложения по техническим мерам защиты. Расчёт кейса: утечка данных → отток клиентов → расчёт годовой потери выручки. Групповое обсуждение: какие технические средства могли бы снизить риск утечки (DLP, шифрование, SIEM) и какова их примерная стоимость?

Тема 4. Управление личным цифровым следом (ПКс-17.1)

Цифровой след: понятие, виды (активный, пассивный). Как формируется, какие данные оставляют пользователи. Почему важно управлять личным цифровым следом: угрозы (социальная инженерия,

дискредитация, шантаж, утечки) и профессиональные риски для специалиста по экономической безопасности. Привязка аккаунтов к номеру телефона: риски и альтернативы. Единая точка отказа, сим свопинг. Использование виртуальных номеров, временных номеров. Методы «заметания следов» и снижения видимости: Удаление учётных записей, запрос на удаление данных (право на забвение); Использование псевдонимов, сегментация цифровых профилей (личный, рабочий, публичный); Временные email-адреса, временные номера телефонов для регистрации в сервисах; Настройки приватности в соцсетях, ограничение видимости старых публикаций, Защита от трекинга: браузеры с фокусом на приватность, режим инкогнито, использование шифрования и туннелирования для подключения к сети; Противодействие fingerprinting (отпечаткам браузера); Управление файлами cookie, отказ от отслеживания; Управление метаданными из файлов (фото, документы). Безопасное использование ИИ сервисов: минимизация данных, использование временных аккаунтов. Инструменты мониторинга своего цифрового следа: поиск по себе, сервисы утечек.

Практическое занятие

Индивидуальная работа: глубокий анализ собственного цифрового следа – поиск по ФИО, email, телефону, никам. Студенты фиксируют, какую информацию о них можно найти, и оценивают риски. Работа с метаданными: студентам выдаётся фотография, они с помощью онлайн-инструментов (или через свойства файла) просматривают метаданные (геолокацию, дату, модель устройства) и удаляют их перед «публикацией». Кейс: «Как я могу стать невидимым для OSINT?» – студенты в группах разрабатывают чек-лист действий для снижения цифровой видимости (не менее 10 пунктов). Рефлексия: обсуждение баланса между анонимностью и необходимостью быть найденным (для карьеры, деловых контактов).

Тема 5. Правовая защита репутации в цифровой среде (ПКс-17.1)

Конституция РФ**.**

Управление репутацией: Основные нормативные акты, касающиеся защиты чести, достоинства и деловой репутации в цифровой среде: Федеральный закон от 02.10.2007 №229-ФЗ «Об исполнительном производстве». Гражданский кодекс РФ (ст. 152 ГК РФ). Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Защита персональных данных в сети: Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных». Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации». Постановление Правительства РФ от 29.06.2021 №1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных». Приказ Роскомнадзора от 24.02.2021 №18 «Об утверждении требований к содержанию согласия на обработку

персональных данных, разрешённых субъектом персональных данных для распространения».

Нормативное регулирование идентификации через номер телефона: ФЗ № 149 ФЗ, требования к операторам связи, закон «о приземлении».

Уголовная и Административная ответственность в сфере управления цифровой репутацией и безопасности. Правовые аспекты использования ИИ-сервисов в России.

Процедуры: досудебное обращение, внесудебная блокировка (Роскомнадзор), судебная защита.

Практическое занятие.

Анализ судебной практики: решение суда о защите деловой репутации юридического лица (удаление отзыва с сайта отзовика). Составление заявления в Роскомнадзор о признании информации запрещённой. Разработка локального акта: «Порядок использования ИИ сервисов в организации» – запрет на загрузку персональных данных и коммерческой тайны, обязательное согласование. Кейс: компания оштрафована за утечку данных, произошедшую из-за использования сотрудниками публичного ИИ сервиса. Анализ правовых последствий. Кейс: «Бывший сотрудник пишет негативные посты о компании в соцсетях, называя руководителей мошенниками» – какие правовые механизмы применимы?

Тема 6. Организационные инструменты: политики, кодексы, взаимодействие подразделений (ПКс-17.1)

Роль внутренних документов в управлении репутацией: Политика информационной безопасности; Кодекс цифровой этики (поведение в соцсетях, использование корпоративных и личных устройств); Регламент реагирования на инциденты. Взаимодействие подразделений при репутационном кризисе: служба информационной безопасности; юридический отдел; служба связей с общественностью; служба управления персоналом. Назначение ответственных. Регуляторные требования к раскрытию информации об инцидентах (Банк России, Роскомнадзор, ФСТЭК).

Практическое занятие:

Разработка фрагмента «Кодекса цифровой этики сотрудника» в малых группах, презентация. Ролевая игра: инцидент «утечка данных клиентов» — распределение ролей (директор, начальник ИБ, юрист, PR менеджер), каждая роль озвучивает действия в первые 2 часа. Анализ типовой Политики информационной безопасности (выделение положений, влияющих на репутацию).

Тема 7. Технологии мониторинга и анализа репутации. (ПКс-17.1)

Технические средства защиты информации, влияющие на репутацию: Антивирусное ПО – защита от вредоносного ПО, которое может привести к утечке данных или взлому аккаунтов; DLP (Data Loss Prevention) – контроль

передачи данных, предотвращение утечек через email, облачные сервисы, мессенджеры, включая отправку данных в ИИ-сервисы; SIEM (Security Information and Event Management) – централизованный сбор и анализ событий безопасности для раннего обнаружения инцидентов; WAF (Web Application Firewall) – защита веб-приложений от взлома, подмены страниц.; Средства защиты от DDoS-атак – предотвращение недоступности сервисов; Шифрование данных – защита информации при хранении и передаче; Многофакторная аутентификация (MFA) – защита от сим-свопинга и компрометации аккаунтов. Инструменты мониторинга СМИ и соцмедиа: принципы работы, метрики (тон, охват, вовлечённость).

OSINT (Open Source Intelligence) как инструмент защиты: Что такое OSINT, отличие от разведки. Легальные методы OSINT: поисковые операторы, сервисы проверки утечек, анализ метаданных, сбор информации из соцсетей. Использование OSINT для мониторинга репутации: выявление упоминаний, угроз, инсайдерской активности, утечек данных. Защита от OSINT-сбора. Поисковые операторы для выявления негатива. SEO-репутация (SERM): методы вытеснения негатива. ИИ-инструменты для мониторинга репутации: использование нейросетей для анализа тональности, прогнозирования репутационных рисков.

Практическое занятие:

Анализ открытых профилей сотрудников (без перехода в закрытые разделы) – студенты ищут данные, которые могли бы использовать злоумышленники. Задание: составить список из 3 ключевых слов для мониторинга репутации (включая номер телефона руководителя, если он публичен). Групповое задание: разработать краткий чек-лист «Как защититься от OSINT-сбора» для сотрудников организации.

Тема 8. Комплексное управление инцидентами и восстановление репутации (ПКс-17.1)

Понятие инцидента с репутационными последствиями. Этапы реагирования: обнаружение, сбор доказательств, сдерживание, коммуникация, пост инцидентный анализ. Инциденты, связанные с современными угрозами: сим свопинг и компрометация всех аккаунтов; дипфейк звонки и видео с использованием голоса/изображения руководителя; загрузка конфиденциальных данных в публичные ИИ сервисы; quishing атаки на сотрудников; OSINT-атаки (сбор информации для социальной инженерии). Роль технических средств и OSINT в расследовании инцидентов. Использование OSINT для выявления утекших данных, фейковых аккаунтов, распространителей негатива. Антикризисные коммуникации: принципы, тайминг, ответственные лица. Примеры успешного и неуспешного управления инцидентами. Восстановление репутации: программы лояльности, прозрачность, обучение персонала.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1 Оценочные материалы по дисциплине Б1.В.24 «Управление цифровой безопасностью» входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа — это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа — это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.	Ответ считается верным, если правильно установлены все соответствия (позиции из

правильных ответов из нескольких вариантов предложенных		2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	Ответ считается верным, если правильно указана вся последовательность цифр
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа.	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа

		5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3.Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

Итоговая балльная оценка	**Традиционная система**	**Бинарная система**	**ECTS**	
			Для традиционной системы	**Для бинарной системы**
95-100	Отлично	Зачтено	A	P/ Passed
85-94			B	P/ Passed
75-84	Хорошо		C	P/ Passed
65-74			D	P/ Passed
55-64	Удовлетворительно		E	P/ Passed
0-54	Неудовлетворительно	Не зачтено	F	F/Failed

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

Максимальная сумма баллов за текущий контроль успеваемости	Максимальная сумма баллов за промежуточную аттестацию	Максимальная итоговая балльная оценка	Максимальная сумма баллов за повторную промежуточную аттестацию
60 баллов	40 баллов	100 баллов	100 баллов

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

— тестирование (включая задания закрытого типа с выбором одного ответа, с выбором нескольких ответов, на установление соответствия, на установление последовательности, а также задания комбинированного типа с обоснованием);

— практические задания (ПЗ) в формах: кейс-анализ, работа в малых группах, деловая игра, ролевая игра, дискуссия, групповое обсуждение, индивидуальное задание, разработка чек-листов и локальных актов, практикум

— устный опрос.

— Профессионально-исследовательское задание (ПИЗ)

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

Тема 1. Цифровая репутация организации и личности

Вопросы для устного опроса (УО):

1. Дайте определение цифровой репутации. В чём её отличие от имиджа и бренда?
2. Из каких элементов складывается репутационный капитал организации?
3. Какие метрики используются для количественной оценки репутации? Поясните экономический смысл каждой.
4. Какие экономические последствия влечёт потеря репутации для финансовой организации?
5. Почему личная репутация специалиста по экономической безопасности важна для организации? Приведите аргументы.

Тестовые задания (Т):

1. **Какая метрика измеряет готовность клиента рекомендовать компанию другим?**
   a) Медиаиндекс
   b) Индекс потребительской лояльности (NPS)
   c) Стоимость привлечения клиента (CAC)
   d) Коэффициент автономии

2. **Что из перечисленного относится к прямым экономическим последствиям утечки персональных данных?**
   a) Рост капитализации
   b) Отток клиентов и падение выручки
   c) Увеличение налоговой ставки
   d) Снижение курса национальной валюты

Практические задания (ПЗ):

Задача 1. У финансовой организации произошла утечка данных 10 000 клиентов. Штраф Роскомнадзора – 500 тыс. руб. Отток клиентов – 4% от утекшей базы. Средний доход от одного клиента в год – 6 000 руб. Рассчитайте финансовые потери от утечки (штраф + отток). Сделайте вывод о репутационном ущербе.

Задача 2. Постройте карту репутационных угроз для типовой ИТ-компании (не менее 3 угроз). Для каждой укажите источник угрозы, возможные последствия и предложите одну меру предотвращения.

Задание 1. Найдите в открытых источниках (СМИ, базы судебных решений) пример реального судебного спора о защите деловой репутации организации в связи с утечкой данных. Опишите суть дела, решение суда и размер компенсации. Сделайте вывод о достаточности существующих

правовых механизмов.

Задание 2. Проведите сравнительный анализ NPS (индекса потребительской лояльности) двух российских банков за последние 2 года. Как связаны изменения NPS с публичными инцидентами информационной безопасности? Представьте выводы в виде краткого отчёта (1–2 стр.).

Тема 2. Основные угрозы цифровой репутации

Вопросы для устного опроса (УО):

1. Приведите классификацию угроз цифровой репутации (внешние, внутренние, новые). Приведите примеры.
2. Что такое SIM-свопинг? Опишите механизм атаки и её последствия.
3. Как злоумышленники могут использовать дипфейк-звонки для дискредитации репутации?
4. Какие риски создаёт использование публичных ИИ-сервисов сотрудниками?
5. Какие факторы усиливают репутационный ущерб при наступлении инцидента?
6.

Тестовые задания (Т):

Какие угрозы относятся к новым угрозам личным данным (последние 5 лет)?

a) SIM-свопинг
b) Вирус-шифровальщик
c) Quishing (фишинг через QR-коды)
d) Дипфейк-звонки с использованием ИИ

Практические задания (ПЗ):

Задача 1 (кейс «Сим-свопинг»). Злоумышленники перевыпустили SIM-карту финансового директора компании, получили доступ к корпоративной почте и разослали ложные счета контрагентам. Опишите репутационные последствия для компании и предложите не менее трёх мер предотвращения.

Задача 2 (OSINT-кейс). Студенту предоставляется открытый профиль человека (ФИО, город, место работы, фото). Используя поисковые операторы, найдите максимум информации о нём (должность, контакты, связи). Опишите, как эта информация может быть использована злоумышленниками для социальной инженерии.

Задание 1. Проанализируйте три реальных случая SIM-свопинга в РФ за последние 2 года (по материалам судебной практики или СМИ). Опишите схемы атаки, нанесённый ущерб и меры, которые предприняли пострадавшие. Сформулируйте рекомендации для физических лиц и организаций.

Задание 2. Подготовьте аналитическую справку на тему «Дипфейк-атаки как угроза корпоративной репутации: текущее состояние и прогноз на 2

года». Используйте не менее 5 источников (включая зарубежные исследования). Объём – 3–5 стр.

Тема 3. Управление репутационными рисками

Вопросы для устного опроса (УО):

1. Раскройте понятие репутационного риска и перечислите этапы управления им.
2. Как строится матрица «вероятность – последствия» для качественной оценки рисков?
3. Что такое SLE, ARO, ALE? Приведите формулу расчёта ожидаемых годовых потерь.
4. Назовите стратегии реагирования на репутационные риски (принятие, снижение, передача, избегание). Приведите примеры.
5. Какие технические средства (DLP, SIEM, WAF, MFA) помогают снизить репутационные риски?

Тестовые задания (Т): Установите соответствие.

Стратегия реагирования	**Пример применения**
1. Принятие риска	А. Внедрение DLP-системы
2. Снижение риска	Б. Признание единичного негативного отзыва без затрат
3. Передача риска	В. Запрет использования публичных ИИ-сервисов
4. Избегание риска	Г. Страхование репутационных рисков

Практические задания (ПЗ):

Задача 1. Для интернет-магазина рассчитаны SLE для трёх рисков: утечка данных – 3 млн руб., взлом сайта – 2 млн руб., негативный отзыв блогера – 0,5 млн руб. ARO соответственно: 0,2; 0,1; 0,6. Рассчитайте ALE для каждого риска. Какой риск является наиболее критичным? Постройте матрицу «вероятность – последствия».

Задача 2. Стоимость внедрения DLP-системы с ежегодным обслуживанием – 800 тыс. руб. ALE для риска утечки данных составляет 2,5 млн руб. Целесообразно ли внедрять DLP? Обоснуйте ответ.

Задание 1. Проанализируйте российский рынок страхования репутационных рисков. Какие страховые компании предлагают такие продукты? Какие события признаются страховым случаем? Каковы типичные лимиты и франшизы? Оцените эффективность этого инструмента для малого

бизнеса.

Задание 2. Разработайте сценарий деловой игры «Выбор стратегии реагирования на репутационные риски» для компании из сферы e-commerce. Опишите пять репутационных рисков, варианты стратегий, роли участников и критерии оценки принятых решений.

Тема 4. Управление личным цифровым следом

Вопросы для устного опроса (УО):

1. Что такое цифровой след? Чем отличается активный след от пассивного?
2. Почему управление личным цифровым следом критически важно для специалиста по экономической безопасности?
3. Какие методы «заметания следов» вы знаете? (не менее 4)
4. Что такое право на забвение и как оно реализуется в РФ?
5. Как злоумышленники могут использовать метаданные фотографий?

Тестовые задания (Т):

Что из перечисленного является активным цифровым следом?

a) IP-адрес пользователя
b) Публикация поста в соцсетях
c) История посещённых сайтов (логи сервера)
d) Геолокация, переданная приложением без ведома

Практические задания (ПЗ):

Задача 1 (анализ метаданных). Студенту выдаётся фотография в формате JPG. Необходимо с помощью онлайн-инструментов (или свойств файла) определить: модель устройства, дату и время съёмки, GPS-координаты. Записать найденные данные и предложить, как удалить метаданные перед публикацией.

Задача 2 (чек-лист). Разработайте чек-лист действий для сотрудника организации по снижению цифровой видимости (не менее 8 пунктов). Включите методы защиты от OSINT-сбора, управления профилями в соцсетях, использования временных номеров и email.

Задание 1. Проведите исследование собственного цифрового следа: выполните поиск по ФИО, email, никам в Яндекс. Опишите, какую информацию о вас можно найти, оцените риски (низкий, средний, высокий) и составьте план действий по их снижению. Результаты оформите в виде отчёта (2–3 стр.).

Задание 2. Проанализируйте судебную практику по ст. 152.2 ГК РФ (охрана изображения гражданина) и «праву на забвение» (ст. 15.5 ФЗ-149). Найдите 2–3 решения судов, где граждане требовали удалить информацию о себе из поисковой выдачи. Сделайте вывод об эффективности этого механизма

в РФ.

Тема 5. Правовая защита репутации в цифровой среде

Вопросы для устного опроса (УО):

1. Какие нормативные правовые акты РФ регулируют защиту чести, достоинства и деловой репутации в интернете?
2. Что гласит ст. 152 Гражданского кодекса РФ о защите деловой репутации?
3. Какие требования к обработке персональных данных установлены ФЗ №152-ФЗ?
4. Опишите порядок внесудебной блокировки порочащей информации через Роскомнадзор.
5. Какая ответственность предусмотрена за утечку персональных данных (административная, уголовная)?

Тестовые задания (Т):

Какие органы или процедуры участвуют во внесудебной блокировке информации?

a) Суд
b) Роскомнадзор
c) Прокуратура
d) Реестр запрещённой информации (Единый реестр)

Практические задания (ПЗ):

Задача 1 (кейс «Бывший сотрудник»). Бывший сотрудник публикует в соцсетях посты, где называет компанию «мошеннической» и призывает клиентов расторгать договоры. Какие правовые механизмы доступны компании? Опишите последовательность действий (досудебные, судебные) со ссылками на нормы права.

Задача 2 (локальный акт). Разработайте фрагмент локального акта «Порядок использования ИИ-сервисов в организации». Включите не менее 4 пунктов: запреты, согласования, ответственность.

Задание 1. Проанализируйте судебную практику по делам о защите деловой репутации в сети Интернет за 2023–2025 гг. (не менее 5 дел). Выявите наиболее частые основания для удовлетворения иска, размеры компенсаций и проблемы доказывания. Результаты оформите в виде аналитической записки.

Задание 2. Подготовьте шаблон заявления в Роскомнадзор о признании информации (порочащей деловую репутацию) запрещённой к распространению. Укажите ссылки на ФЗ №149-ФЗ, описание информации, доказательства (скриншоты). Обоснуйте, почему этот способ может быть эффективнее судебного.

Тема 6. Организационные инструменты цифровой безопасности

Вопросы для устного опроса (УО):

1. Какие внутренние документы организации регулируют управление цифровой безопасностью?
2. Что должно содержаться в Кодексе цифровой этики сотрудника?
3. Как распределяются роли (ИБ, юрист, PR, HR) при репутационном кризисе?
4. Какие регуляторные требования к раскрытию информации об инцидентах существуют (Банк России, Роскомнадзор)?

Тестовые задания (Т): установите соответствие.

Роль при инциденте	**Основная функция**
1. Начальник ИБ	А. Внешние коммуникации
2. Юрист	Б. Техническое сдерживание и сбор логов
3. PR-менеджер	В. Оценка правовых последствий, уведомление регуляторов

Практические задания (ПЗ):

Задача 1 (ролевая игра). Инцидент – утечка данных клиентов. Распределите роли (директор, начальник ИБ, юрист, PR-менеджер). Для каждой роли опишите конкретные действия в первые 2 часа после обнаружения утечки.

Задача 2 (Кодекс цифровой этики). Разработайте 5 положений для Кодекса цифровой этики сотрудника организации, работающей с персональными данными (правила использования соцсетей, личных устройств, упоминания компании).

Задание 1. Проведите сравнительный анализ типовых Политик информационной безопасности трёх российских компаний (из открытых источников). Выделите положения, которые наиболее сильно влияют на репутационные риски. Предложите улучшения.

Задание 2. Разработайте регламент взаимодействия подразделений (ИБ, юридического, PR и HR) при репутационном кризисе, вызванном дипфейк-атакой. Опишите последовательность действий, сроки и ответственных в виде блок-схемы.

Тема 7. Технологии мониторинга и анализа репутации.

Вопросы для устного опроса (УО):

1. Что такое OSINT и чем отличается от разведки?

2. Какие технические средства (DLP, SIEM, WAF, MFA) помогают предотвратить репутационные потери?
3. Какие поисковые операторы (site:, intitle:, filetype:) вы знаете? Приведите примеры.
4. Как используются сервисы проверки утечек (HaveIBeenPwned) в мониторинге репутации?
5. Что такое SERM и какие методы вытеснения негатива существуют?

Тестовые задания (Т):

Какие инструменты относятся к OSINT?
a) Поисковые операторы
b) Антивирус Касперского
c) Сервис HaveIBeenPwned
d) Анализ метаданных фотографий

Практические задания (ПЗ):

Задача 1 (OSINT-поиск). Студенту выдаётся открытый профиль (гипотетический): ФИО, должность, компания. Используя поисковые операторы, найдите: возможные утекшие пароли, публикации, где упоминается этот человек, фотографии с метаданными. Опишите, как найденная информация может быть использована злоумышленниками.

Задача 2 (чек-лист). Разработайте чек-лист «Как защититься от OSINT-сбора» для сотрудников организации (не менее 8 пунктов). Включите рекомендации по настройкам приватности, использованию псевдонимов, управлению метаданными.

Задание 1. Проведите исследование: какую информацию о вашем учебном заведении можно собрать с помощью OSINT-методов за 30 минут (не нарушая закон). Составьте отчёт о найденных данных (публичные документы, email-адреса сотрудников, фотографии, сведения об инфраструктуре). Предложите меры по снижению рисков.

Задание 2. Сравните функциональность 2–3 сервисов мониторинга упоминаний бренда в соцмедиа и СМИ. Оцените их возможности по анализу тональности, обнаружению кризисов и интеграции с системой оповещения. Результаты оформите в виде таблицы.

Тема 8. Комплексное управление инцидентами и восстановление репутации

Вопросы для устного опроса (УО):

1. Дайте определение инцидента с репутационными последствиями. Назовите этапы реагирования.
2. Каковы принципы антикризисных коммуникаций?

3. Как OSINT может помочь в расследовании инцидента?
4. Приведите пример успешного и неуспешного управления репутационным кризисом.
5. Что включает программа восстановления репутации после утечки данных?

Тестовые задания (Т):

Какой этап реагирования на инцидент предполагает сбор и сохранение доказательств для возможного суда?

a) Обнаружение
b) Сдерживание
c) Сбор доказательств
d) Пост-инцидентный анализ

Практические задания (ПЗ):

Задача 1 (дипфейк-кейс). В компании произошёл дипфейк-звонок от имени генерального директора: сотрудник перевёл деньги мошенникам. Клиенты узнали об этом из MAX-каналов. Опишите план антикризисных коммуникаций на первые 24 часа (для сотрудников, клиентов, регуляторов). Предложите меры предотвращения повторения.

Задача 2 (план восстановления). Разработайте программу восстановления репутации после утечки персональных данных (не менее 5 шагов, указать сроки, ответственных, примеры сообщений).

Задание 1. Проанализируйте два публичных репутационных кризиса в российских компаниях за последние 2 года (один – успешное управление, другой – неуспешное). Опишите причины, действия компаний, реакцию СМИ и итоги. Сформулируйте уроки и рекомендации.

Задание 2. Разработайте сценарий командно-штабной тренировки по отработке действий при инциденте «утечка данных клиентов и появление фейковых аккаунтов в соцсетях». Опишите легенду, роли участников, временные рамки, контрольные точки и критерии успешности.

Приведённые задания являются типовыми и могут варьироваться преподавателем в зависимости от уровня подготовки обучающихся и формы обучения (очная/заочная). Полный перечень заданий содержится в Фонде оценочных средств (ФОС).

5.3. Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает не менее 2 (двух) и не более 10 (десяти) КТ в течение периода освоения дисциплины.

Максимальное количество баллов за любой тип работ в рамках КТ составляет 100 (сто) баллов.

Распределение весовых коэффициентов по КТ в рамках текущего контроля успеваемости по дисциплине и формулы расчета:

Необходимо составить расчет по конкретной дисциплине. НАПРИМЕР

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать студент	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,15	15
КТ 2	100	0,15	15
КТ 3	100	0,15	15
КТ 4	100	0,15	15
Итого:	х	0,6	60

Формула расчета результата контрольной точки:
Результат контрольной точки = Количество баллов за работу в рамках КТ х Коэффициент веса контрольной точки.

5.4. Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

КТ – 1 (темы 1–2):

Формы контроля: тестирование (Т), практические контрольные задания (ПКЗ), профессионально-исследовательское задание (ПИЗ).

Тестовые задания (примеры)

1. Задание закрытого типа с выбором одного правильного ответа:
Инструкция: выберите один верный ответ.
Вопрос: Какая метрика измеряет готовность клиента рекомендовать компанию другим?
a) Медиаиндекс
b) Индекс потребительской лояльности (NPS)
c) Стоимость привлечения клиента (CAC)
d) Коэффициент автономии

2. Задание закрытого типа с выбором нескольких правильных ответов:
Инструкция: выберите все верные варианты.
Вопрос: Какие угрозы относятся к новым угрозам цифровой репутации (последние 3–5 лет)?

a) SIM-свопинг
b) Классический фишинг по email
c) Quishing (фишинг через QR-коды)
d) Дипфейк-звонки с использованием ИИ

3. Задание закрытого типа на установление соответствия:
Инструкция: установите соответствие между типом угрозы и её примером.

Тип угрозы	Пример
1. Внешняя кибератака	А. Сотрудник случайно опубликовал базу email-адресов
2. Внутренняя ошибка	Б. Дипфейк-видео с генеральным директором
3. SIM-свопинг	В. Перевыпуск SIM-карты для доступа к корпоративной почте

Практические контрольные задания (ПКЗ)

Задача 1 (расчёт финансовых потерь).

У финансовой организации произошла утечка персональных данных 15 000 клиентов. Штраф Роскомнадзора – 500 тыс. руб. Отток клиентов – 4% от утекшей базы. Средний доход от одного клиента в год – 7 000 руб. Рассчитайте прямые финансовые потери (штраф + отток). Обоснуйте, почему реальный ущерб может быть выше.

Задача 2 (карта угроз).

Постройте карту репутационных угроз для онлайн-кинотеатра (не менее 4 угроз). Для каждой укажите: источник угрозы, возможные последствия для репутации, одну меру предотвращения.

Задача 3 (кейс «Сим-свопинг»).

Злоумышленники с помощью SIM-свопинга получили доступ к корпоративной почте финансового директора и разослали ложные счета контрагентам. Опишите репутационные последствия для компании и предложите не менее трёх мер предотвращения.

Профессионально-исследовательское задание (ПИЗ)

Тема: Анализ реального инцидента с утечкой персональных данных в российской компании (за последние 2 года).

Найдите информацию об инциденте в открытых источниках (СМИ, сайты регуляторов). Опишите:

- что произошло и какие данные утекли;
- реакцию компании (коммуникации, меры);
- штрафы и репутационные последствия (отток клиентов,

падение капитализации).

Сформулируйте не менее трёх уроков для других компаний. Объём – 2–3 стр.

КТ – 2 (темы 3–4):

Формы контроля: тестирование (Т), практические контрольные задания (ПКЗ), кейс.

Тестовые задания (примеры)

1. Задание закрытого типа (выбор одного ответа)

Вопрос: Какая формула используется для расчёта ожидаемых годовых потерь (ALE)?

a) ALE = SLE + ARO
b) ALE = SLE × ARO
c) ALE = SLE / ARO
d) ALE = ARO / SLE

2. Задание на установление последовательности

Расположите в правильном порядке этапы управления репутационным риском:

a) Мониторинг
b) Идентификация рисков
c) Оценка (качественная и количественная)
d) Выбор мер реагирования

3. Задание комбинированного типа (выбор + обоснование)

Вопрос: Какая стратегия реагирования на риск наиболее целесообразна при высокой вероятности и высоких последствиях (например, утечка данных)? Обоснуйте свой ответ.

a) Принятие
b) Снижение
c) Передача
d) Избегание

Практические контрольные задания (ПКЗ)

Задача 1 (расчёт ALE и выбор стратегии).

Для интернет-магазина риск утечки данных: SLE = 1,8 млн руб., ARO = 0,25. Рассчитайте ALE. Внедрение DLP-системы стоит 500 тыс. руб./год. Целесообразно ли применять стратегию снижения риска? Обоснуйте.

Задача 2 (чек-лист по цифровому следу).

Разработайте чек-лист «Как снизить личный цифровой след для защиты от OSINT-сбора» для сотрудников организации (не менее 8 пунктов). Включите рекомендации по настройкам приватности, использованию псевдонимов, удалению метаданных.

Задача 3 (оценка ущерба от OSINT).

Опишите, какую информацию о сотруднике (ФИО, должность, фотографии, место работы) злоумышленник может найти в открытых источниках. Приведите два сценария использования этой информации для социальной инженерии. Предложите меры защиты.

Кейс (ситуационная задача)

В компании «СтройТех» сотрудник отдела закупок опубликовал в своём аккаунте в социальной сети фотографию пропуска на территорию завода (видна должность, имя, номер пропуска). Через месяц компания пострадала от атаки с использованием социальной инженерии: неизвестный представился сотрудником по имени, назвал номер пропуска и получил доступ к складскому учёту.

1. Оцените репутационный и финансовый риск для компании (качественно).
2. Какие меры из темы 3 (управление рисками) и темы 4 (управление цифровым следом) должны быть приняты?
3. Составьте памятку для сотрудников о недопустимости публикации служебной информации в соцсетях.

КТ – 3 (темы 5–6):

Формы контроля: тестирование (Т), практические контрольные задания (ПКЗ), профессионально-исследовательское задание (ПИЗ).

Тестовые задания (примеры)

1. Задание закрытого типа (выбор одного ответа)

Вопрос: какая статья Гражданского кодекса РФ регулирует защиту деловой репутации юридического лица?

a) Ст. 151
b) Ст. 152
c) Ст. 153
d) Ст. 154

2. Задание на установление соответствия

Соотнесите процедуру защиты и её содержание.

Процедура	**Содержание**
1. Досудебное обращение	А. Иск в суд о признании сведений не соответствующими действительности
2. Внесудебная блокировка	Б. Письменная претензия к администрации сайта

Процедура	Содержание
3. Судебная защита	B. Заявление в Роскомнадзор о признании информации запрещённой

3. Задание с выбором нескольких ответов

Вопрос: Какие положения должны быть включены в Кодекс цифровой этики сотрудника?

a) Запрет на разглашение конфиденциальной информации в соцсетях

b) Требования к сложности паролей

c) Правила использования личных устройств для рабочих целей

d) Технические характеристики серверов

Практические контрольные задания (ПКЗ)

Задача 1 (правовой кейс).

Бывший сотрудник регулярно публикует в соцсетях посты, в которых называет бывшего работодателя «фирмой-однодневкой» и призывает клиентов не оплачивать счета. Какие правовые механизмы доступны компании? Опишите последовательность действий (досудебные, судебные) со ссылками на нормы права.

Задача 2 (локальный акт).

Разработайте фрагмент локального акта «Порядок использования ИИ-сервисов в организации». Включите не менее 4 пунктов: запреты, согласование, ответственность.

Профессионально-исследовательское задание (ПИЗ)

Тема: Анализ судебной практики по защите деловой репутации в сети Интернет.

Найдите два решения российских судов по делам о защите деловой репутации (опубликованные в ГАС «Правосудие» или аналогичных базах). Для каждого дела укажите:

- фабулу (что произошло, кто истец и ответчик);
- правовые основания иска (ст. 152 ГК РФ и др.);
- решение суда и размер компенсации (если присуждена);
- обоснование суда.

Сравните дела и сделайте вывод о факторах, влияющих на удовлетворение иска. Объём – 3–4 стр.

КТ – 4 (темы 7–8):

Формы контроля: тестирование (Т), практические контрольные задания (ПКЗ), комплексный кейс (включает OSINT-исследование и антикризисный план).

Тестовые задания (примеры)

1. Задание закрытого типа (выбор одного ответа)

Вопрос: Какое техническое средство предназначено для централизованного сбора и анализа событий безопасности (раннее обнаружение инцидентов)?

a) DLP
b) SIEM
c) WAF
d) MFA

2. Задание на установление последовательности (этапы реагирования)

Расположите этапы управления инцидентом в правильном порядке:

a) Пост-инцидентный анализ
b) Сдерживание
c) Обнаружение
d) Антикризисные коммуникации

3. Задание с выбором нескольких ответов

Вопрос: Какие методы относятся к OSINT?

a) Поисковые операторы (site:, intitle:)
b) Анализ метаданных фотографий
c) Установка антивируса
d) Проверка email в сервисах утечек

Практические контрольные задания (ПКЗ)

Задача 1 (OSINT-исследование).

Проведите анализ открытых данных публичного профиля (вымышленного) по заданным параметрам: ФИО «Иванов Иван Иванович», город «Санкт-Петербург», место работы – условная компания. Используя поисковые системы и операторы, опишите, какую информацию можно найти (до 5 фактов). Объясните, как эта информация может быть использована для социальной инженерии.

Задача 2 (чек-лист по защите от OSINT).

Разработайте чек-лист для сотрудников организации «Как защититься от OSINT-сбора» (не менее 8 пунктов). Включите рекомендации по настройкам приватности в соцсетях, управлению метаданными, использованию псевдонимов и временных номеров.

Комплексный кейс (управление инцидентами)

В крупной логистической компании произошёл инцидент: злоумышленники с помощью OSINT собрали данные о руководителе (его фото, должность, номер телефона, график поездок), создали дипфейк-звонок от его имени начальнику IT-отдела с требованием срочно перевести

3 млн руб. на указанный счёт. Деньги переведены. Через час информация появилась в MAX-каналах.

1. Опишите пошаговый план реагирования на инцидент (этапы: обнаружение, сдерживание, сбор доказательств, коммуникации, пост-инцидентный анализ).
2. Разработайте план антикризисных коммуникаций на первые 48 часов: для сотрудников, для клиентов и партнёров, для регуляторов (полиция, Роскомнадзор). Укажите тайминг, ответственных (роли), ключевые сообщения.
3. Предложите долгосрочные технические и организационные меры для предотвращения повторения (связь с темами 7–8: MFA, обучение сотрудников, защита от OSINT).

Для каждой формы текущего контроля успеваемости обучающихся в рамках КТ определены критерии оценивания результатов выполнения задания.

Всего в рамках контрольной точки можно набрать 100 баллов, для каждого элемента контрольной точки установлен свой предельный балл.

Критерии оценивания тестирования

Критерии оценки	Диапазон баллов	Описание критерия
Количество правильных ответов	0-20	На все тестовые вопросы дан верный ответ.
Итого максимально:	20	

Критерии оценивания ПКЗ

Критерии оценки	Диапазон баллов	Описание критерия
Полнота выполнения требований	0–15	Выполнены все пункты задания (указано требуемое количество угроз/пунктов чек-листа/этапов плана) – 15 баллов; выполнено 70–80% – 10 баллов; 50–70% – 6 баллов; менее 50% – 0 баллов.
Реалистичность и конкретность	0–15	Все предложения конкретны, выполнимы в реальных условиях организации – 15 баллов; отдельные предложения абстрактны – 8–10 баллов; в целом нереалистичны – 0–5 баллов.
Логическая структура и связь с теорией	0–10	Задание структурировано логично, использована корректная терминология из курса, есть ссылки на изученные методы – 10 баллов; нарушения логики или слабая связь с теорией – 5 баллов; отсутствует – 0 баллов.
Итого максимально:	40	

Критерии оценивания ПИЗ

Критерии оценки	Диапазон баллов	Описание критерия
Полнота раскрытия темы	0–12	Охвачены все требуемые аспекты (например, фабула дела, правовые основания, решение

		суда, последствия) – 12 баллов; отсутствует 1–2 аспекта – 6–8 баллов; раскрыто менее половины – 0–4 балла.
Аналитическая глубина (выводы, сравнения, обобщения)	0–12	Присутствуют аргументированные выводы, сравнения нескольких источников или кейсов, выявлены закономерности – 12 баллов; выводы поверхностны или отсутствует сравнение – 6 баллов; только описание без анализа – 0 баллов.
Использование источников (актуальность, достоверность)	0–8	Приведены ссылки на актуальные источники (не старше 3 лет, официальные данные, судебные решения, СМИ) – 8 баллов; источники устаревшие или сомнительные – 4 балла; источники отсутствуют – 0 баллов.
Оформление и грамотность	0–8	Структурированный текст, логичное изложение, соблюдены правила орфографии и пунктуации – 8 баллов; отдельные нарушения – 4 балла; много ошибок, неструктурированно – 0 баллов.
Итого максимально:	40	

Критерии оценивания Кейса (ситуационной задачи)

Критерии оценки	Диапазон баллов	Описание критерия
Полнота ответа на все вопросы кейса	0–15	Даны развёрнутые ответы на все поставленные вопросы (подвопросы) – 15 баллов; ответы даны на 2/3 вопросов – 10 баллов; на половину – 7 баллов; менее половины – 0–4 балла.
Логичность и обоснованность решения	0–10	Предложенные шаги логически выстроены, каждый шаг обоснован с опорой на теорию (нормативные акты, методы управления рисками и др.) – 10 баллов; логика нарушена или обоснование слабое – 5 баллов; отсутствует – 0 баллов.
Практическая применимость разработанных мер	0–10	Все меры (план, чек-лист, коммуникации) реалистичны, выполнимы в условиях конкретной организации – 10 баллов; отдельные меры абстрактны – 5 баллов; меры невыполнимы – 0 баллов.
Соответствие нормативно-правовой базе (для правовых кейсов)	0–5	Приведены корректные ссылки на статьи законов (ГК РФ, ФЗ №149, №152) – 5 баллов; ссылки общие или отсутствуют – 0 баллов.
Итого максимально:	40	

Критерии оценивания текущего устного опроса в рамках отдельных тем

Критерии оценки	Диапазон баллов	Описание критерия
Качество правильных ответов	0-54	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.
	55-64	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
	65-84	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
	85-100	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий.

Для выполнения проверочных заданий (тестов закрытого и комбинированного типов, практических контрольных заданий, профессионально-исследовательских заданий, кейсов) студенту разрешается использование следующих дополнительных материалов и оборудования:

Нормативные правовые акты (в актуальной редакции): Гражданский кодекс РФ, Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».

Калькулятор (непрограммируемый). Программное обеспечение: текстовый редактор (MS Word или аналоги), табличный процессор (MS Excel или аналоги).

Браузер с доступом к сети «Интернет» – для выполнения OSINT-заданий (поиск информации в открытых источниках и др.) в рамках практических занятий и контрольных точек, если это предусмотрено заданием.

Доступ к электронной информационно-образовательной среде (LMS) – для прохождения тестирования в электронной форме, загрузки выполненных заданий.

Разрешается использование справочных материалов и образцов документов, выданных преподавателем, если это оговорено в задании.

Запрещается: использование мобильной связи (кроме случаев, когда это предусмотрено заданием, например, для двухфакторной аутентификации в учебных целях); использование готовых решений из интернета (копирование готовых ответов) без самостоятельного анализа и оформления; использование систем искусственного интеллекта для генерации ответов вместо самостоятельного выполнения заданий.

Примечание: конкретный перечень разрешённых материалов и оборудования может уточняться преподавателем перед выполнением каждой контрольной точки в зависимости от типа и сложности заданий.

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Промежуточная аттестация проводится в форме зачета с оценкой.

6.2. Типовые оценочные материалы промежуточной аттестации.

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Вопросы для подготовки к зачету с оценкой:

Тема 1. Цифровая репутация организации и личности (ПКс-17.1)

1. Дайте определение цифровой репутации. В чём её отличие от

имиджа и бренда?

2. Перечислите элементы репутационного капитала организации и объясните, почему каждый из них важен для экономической безопасности.

3. Какие метрики используются для количественной оценки цифровой репутации? Раскройте экономический смысл NPS, медиаиндекса и CAC.

4. Назовите экономические последствия потери репутации для финансовой организации. Приведите примеры из практики.

5. Почему личная репутация специалиста по экономической безопасности может стать системным риском для организации? Аргументируйте.

6. Как связаны инциденты информационной безопасности и репутационные потери? Приведите схему причинно-следственных связей.

7. Опишите методику расчёта финансовых потерь от утечки персональных данных (штраф, отток клиентов, операционные расходы).

8. В чём заключается взаимосвязь между репутацией организации и доверием регуляторов (Банк России, Роскомнадзор)?

Тема 2. Основные угрозы цифровой репутации (ПКс-17.1)

9. Приведите классификацию угроз цифровой репутации (внешние / внутренние) с примерами для ИТ-компании.

10. Что такое SIM-свопинг? Опишите механизм атаки и её последствия для организации и её руководителя.

11. Как злоумышленники могут использовать дипфейк-звонки и дипфейк-видео для дискредитации репутации? Приведите сценарий.

12. Что такое quishing (фишинг через QR-коды)? Опишите сценарий атаки на сотрудников организации.

13. Назовите риски, связанные с использованием публичных ИИ-сервисов (нейросетей) в корпоративной среде.

14. Какие угрозы связаны со сбором биометрии из открытых источников? Приведите не менее двух примеров.

15. Перечислите факторы, усиливающие репутационный ущерб при наступлении инцидента (скорость распространения, виральность, отсутствие плана).

16. Опишите кейс «взлом аккаунта известного человека»: какие репутационные последствия наступают для компании, связанной с этим человеком?

17. Какие угрозы для организации создают уязвимости умных устройств (IoT) сотрудников?

Тема 3. Управление репутационными рисками (ПКс-17.1)

18. Раскройте понятие репутационного риска и перечислите этапы

управления им (идентификация, оценка, выбор мер, мониторинг).

19. Как проводится качественная оценка репутационных рисков? Постройте матрицу «вероятность – последствия» с примером.

20. Что такое SLE, ARO, ALE? Приведите формулу расчёта ожидаемых годовых потерь и пример для риска утечки данных.

21. Назовите стратегии реагирования на репутационные риски (принятие, снижение, передача, избегание). Для каждой приведите пример из цифровой безопасности.

22. Как внедрение технических средств защиты (антивирусы, DLP, SIEM, WAF) связано со снижением репутационных рисков?

23. В каких случаях целесообразно страхование репутационных рисков? Назовите его ограничения.

24. Опишите деловую игру «Выбор стратегии реагирования»: какие факторы влияют на выбор стратегии для конкретного риска?

Тема 4. Управление личным цифровым следом (ПКс-17.1)

25. Дайте определение цифрового следа. Чем отличается активный след от пассивного?

26. Почему для специалиста по экономической безопасности важно управлять личным цифровым следом? Назовите не менее трёх причин.

27. Какие риски создаёт привязка всех аккаунтов к одному номеру телефона? Как их минимизировать?

28. Перечислите методы «заметания следов» и снижения цифровой видимости (не менее 5).

29. Как работает право на забвение? В каких случаях оно применимо в РФ?

30. Что такое метаданные файлов? Приведите примеры и объясните, как злоумышленники могут их использовать.

31. Опишите чек-лист действий для защиты от OSINT-сбора (не менее 8 пунктов).

32. Как использовать временные номера телефонов и временные email-адреса для снижения цифрового следа?

Тема 5. Правовая защита репутации в цифровой среде (ПКс-17.1)

33. Какие нормативные правовые акты РФ регулируют защиту чести, достоинства и деловой репутации в цифровой среде?

34. Раскройте содержание статьи 152 Гражданского кодекса РФ применительно к защите деловой репутации юридического лица.

35. Какие требования к обработке персональных данных устанавливает Федеральный закон №152-ФЗ?

36. Опишите порядок внесудебной блокировки порочащей информации через Роскомнадзор (по ФЗ №149-ФЗ).

37. Назовите виды ответственности (административной, уголовной, гражданско-правовой) за нарушения в сфере управления цифровой репутацией.

38. Какие правовые последствия наступают для компании при утечке персональных данных через публичный ИИ-сервис?

39. Составьте алгоритм досудебного обращения к администрации сайта-отзовика с требованием удалить порочащие сведения.

40. Какой локальный акт должна разработать организация для регламентации использования ИИ-сервисов сотрудниками? Приведите 3–4 ключевых пункта.

Тема 6. Организационные инструменты цифровой безопасности (ПКс-17.1)

41. Какие внутренние документы организации влияют на управление цифровой репутацией? Назовите и кратко охарактеризуйте.

42. Что должно содержаться в Кодексе цифровой этики сотрудника? Приведите не менее 5 положений.

43. Опишите регламент взаимодействия подразделений (ИБ, юристы, PR, HR) при репутационном кризисе.

44. Проведите ролевую игру «Утечка данных клиентов»: распределите роли и опишите действия каждой роли в первые 2 часа.

45. Какие обязанности по раскрытию информации об инцидентах перед регуляторами (Банк России, Роскомнадзор, ФСТЭК) предусмотрены законодательством?

46. Как типовые политики информационной безопасности могут влиять на репутацию организации?

47. Разработайте фрагмент регламента реагирования на инциденты, связанные с дипфейк-атаками.

Тема 7. Технологии мониторинга и анализа репутации. (ПКс-17.1)

48. Какие технические средства защиты информации (DLP, SIEM, WAF, MFA) помогают предотвратить репутационные потери? Объясните роль каждого.

49. Что такое OSINT? В чём отличие OSINT от разведки? Назовите легальные методы OSINT.

50. Как с помощью поисковых операторов (site:, intitle:, filetype:) можно выявить утекшие документы компании? Приведите примеры.

51. Перечислите инструменты и сервисы для мониторинга упоминаний бренда в СМИ и соцмедиа. Какие метрики они предоставляют?

52. Как можно использовать OSINT для выявления инсайдерской активности и подготовки к социальной инженерии?

53. Что такое SERM (управление репутацией в поисковой выдаче)?

Какие методы вытеснения негатива существуют?

54. Опишите чек-лист «Как защититься от OSINT-сбора» для сотрудников организации (не менее 8 пунктов).

Тема 8. Комплексное управление инцидентами и восстановление репутации (ПКс-17.1)

55. Дайте определение инцидента с репутационными последствиями. Назовите этапы реагирования на такой инцидент.

56. Опишите план действий при обнаружении дипфейк-звонка от имени руководителя компании (обнаружение, сдерживание, коммуникации).

57. Как OSINT может помочь в расследовании инцидента (выявление утекших данных, фейковых аккаунтов, распространителей негатива)?

58. Сформулируйте принципы антикризисных коммуникаций при репутационном кризисе. Укажите тайминг первых заявлений.

59. Приведите примеры успешного и неуспешного управления репутационными инцидентами (из лекций или известных кейсов).

60. Разработайте программу восстановления репутации после утечки персональных данных (не менее 5 шагов, с указанием сроков и ответственных).

6.3. Критерии и шкала оценивания на основе БРС.

Критерии и балльная шкала определяются преподавателем

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок	40
Дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.	30-39

Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.	20-29
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	0-19

6.4. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (*при необходимости*).

Для выполнения проверочных заданий промежуточной аттестации (зачета с оценкой) студенту разрешается использование следующих дополнительных материалов и оборудования:

Нормативные правовые акты (в актуальных редакциях):

- Гражданский кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».

Непрограммируемый калькулятор – для выполнения расчётных заданий.

Письменные принадлежности (ручка, карандаш, линейка).

Запрещается:

использование сети «Интернет» (кроме случаев, специально оговорённых в задании для выполнения OSINT-заданий в рамках практических занятий, но не на промежуточной аттестации);

использование мобильной связи, смартфонов, смарт-часов и иных устройств с доступом в интернет;

использование готовых шпаргалок, текстов учебников и иных печатных материалов, не разрешённых преподавателем;

использование систем искусственного интеллекта для генерации ответов.

Примечание: при выполнении заданий, не требующих расчётов и работы с нормативными актами, использование дополнительных материалов не предусмотрено. Конкретный перечень разрешённых материалов может быть уточнён преподавателем перед началом промежуточной аттестации в зависимости от формы её проведения (устное собеседование, письменная работа, компьютерное тестирование).

7. Методические материалы по освоению дисциплины (модуля)

Для изучения основных вопросов дисциплины «Управление цифровой безопасностью» необходимо конспектировать материалы лекций, работать с рекомендованной преподавателем литературой, а также ресурсами информационно-телекоммуникационной сети «Интернет» (включая поисковые системы, открытые базы судебных решений, официальные сайты регуляторов). Для приобретения навыков активного использования знаний полезно обсуждать плановые и возникающие вопросы, а также решаемые кейсы и задачи на практических занятиях. Чтобы легче и прочнее усвоить материал, следует постоянно использовать конкретные примеры из реальной практики (инциденты утечек данных, дипфейк-атаки, судебные споры о защите репутации).

Для закрепления изученного материала в рабочей программе приведены вопросы по каждой теме дисциплины, на которые следует самостоятельно найти ответы, а также типовые практические задания (расчёт финансовых потерь от утечки данных, построение карт угроз, разработка чек-листов и локальных актов).

Важной составной частью учебного процесса в вузе являются практические занятия. Практические занятия по дисциплине «Управление цифровой безопасностью» проводятся в форме решения ситуационных кейсов, деловых и ролевых игр, работы в малых группах, анализа открытых источников (OSINT), разработки внутренних документов организации (Кодекс цифровой этики, Порядок использования ИИ-сервисов), а также обсуждения судебной практики. Эти занятия помогают студентам глубже усвоить учебный материал, приобрести умения выявлять цифровые угрозы, оценивать репутационные риски и разрабатывать меры по их снижению.

При подготовке к практическим занятиям необходимо проанализировать конспект лекции, ознакомиться с рекомендованной литературой и нормативными правовыми актами по соответствующей теме, осуществить подготовку по рекомендованным в рабочей программе вопросам для устного опроса, выполнить домашнее задание (например, провести анализ собственного цифрового следа или составить чек-лист по защите от OSINT-сбора).

Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной

литературой и нормативными актами обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение современных угроз (SIM-свопинг, дипфейки, quishing, OSINT), уяснение практического применения рассматриваемых теоретических вопросов (расчёт ALE, выбор стратегии реагирования на риск, порядок внесудебной блокировки информации). В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале (матрицы рисков, карты угроз, образцы документов). В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю (в том числе по электронной почте).

Планируя консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам. Записи имеют первостепенное значение для самостоятельной работы студентов. Они помогают понять построение изучаемого материала, выделить основные положения (классификацию угроз, этапы управления рисками, правовые механизмы), проследить их логику. Кроме того, ведение записей способствует превращению чтения в активный процесс, мобилизует, наряду со зрительной, и моторную память. Следует помнить: у студента, систематически ведущего записи, создается свой индивидуальный фонд методических материалов для быстрого повторения изученных вопросов, для мобилизации накопленных знаний. Особенно важны и полезны записи тогда, когда в них находят отражение мысли, возникшие при самостоятельной работе (например, собственные примеры угроз, варианты антикризисных коммуникаций).

После изучения базовых тем курса проводится текущий контроль знаний студентов в форме тестирования, устного опроса, выполнения практических контрольных заданий (ПКЗ) и профессионально-исследовательских заданий (ПИЗ). Типовые тесты и задания по темам дисциплины приведены в специальных разделах данной рабочей программы (п. 5.2, 5.4, 6.2).

Подготовка к текущему и промежуточному контролю (зачёту с оценкой) предполагает изучение представленных в РПД вопросов к зачёту (60 вопросов по 8 темам), работу над тестовыми заданиями всех шести типов (закрытые, на соответствие, на последовательность, комбинированные, открытые), выполнение практических кейсов (расчёт ALE, построение матрицы рисков, разработка антикризисного плана) и анализ реальных инцидентов из практики.

Работа в малых группах – это одна из самых популярных форм проведения занятий по дисциплине, так как она даёт всем обучающимся (в том числе и стеснительным) возможность участвовать в работе, практиковать

навыки сотрудничества, межличностного общения (в частности, умение активно слушать, вырабатывать общее мнение, разрешать возникающие разногласия). Цель данной формы проведения занятий: продемонстрировать сходство или различия определённых угроз, выработать стратегию реагирования на репутационный риск, разработать план антикризисных коммуникаций или выяснить отношение различных групп участников к одному и тому же инциденту. В ходе этой работы дополнительно решаются следующие задачи: развитие навыков общения и взаимодействия в группе, формирование ценностно-ориентационного единства группы, поощрение к гибкой смене социальных ролей в зависимости от ситуации (например, в ролевой игре «Утечка данных» студенты выступают в ролях директора, начальника ИБ, юриста, PR-менеджера).

Группа студентов делится на несколько малых групп. Количество групп определяется числом творческих заданий (кейсов), которые будут обсуждаться в процессе занятия. Малые группы формируются либо по желанию студентов, либо по родственной тематике для обсуждения. Каждая малая группа обсуждает творческое задание в течение отведенного времени (например, разрабатывает карту угроз для онлайн-кинотеатра или выбирает стратегию реагирования на риск в деловой игре). Основной этап – проведение обсуждения результатов работы. Заслушиваются суждения, предлагаемые каждой малой группой по творческому заданию. Преподаватель даёт оценочное суждение о работе малых групп, по решению творческих заданий и эффективности предложенных путей решения.

В качестве самостоятельной работы студентами выполняются практические контрольные задания (ПКЗ) и профессионально-исследовательские задания (ПИЗ) по всем темам. ПКЗ включают расчёт финансовых потерь от утечек данных, построение карт угроз, разработку чек-листов, локальных актов, антикризисных планов. ПИЗ предполагают анализ реальных инцидентов, судебной практики, сравнительный анализ моделей и методов. При выполнении заданий могут использоваться открытые источники информации (официальные базы судебных решений, сайты Роскомнадзора, публикации СМИ) с соблюдением законодательства РФ. Выполненные задания представляются студентом в системе дистанционного обучения (LMS) или сдаются на практическом занятии.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Доронин, А. И. Бизнес-разведка 2.2 + OSINT : руководство / А. И. Доронин. — Москва : ДМК Пресс, 2023. — 504 с. — ISBN 978-5-93700-255-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/456617

2. Рейн, Т. С. Основы социальной инженерии в компьютерной безопасности : учебное пособие / Т. С. Рейн. — Кемерово : КемГУ, 2025. — 99 с. — ISBN 978-5-8353-3309-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/495473
3. Бирюков, А. А. Информационная безопасность: защита и нападение : руководство / А. А. Бирюков. — 3-е изд. — Москва : ДМК Пресс, 2023. — 440 с. — ISBN 978-5-93700-219-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/455351
4. Цифровая культура : учебник / Ю. Ю. Костюхин, М. В. Черняев, В. Ю. Ершова [и др.] ; под ред. Е. Ю. Сидоровой. — Москва : Русайнс, 2026. — 348 с. — ISBN 978-5-466-12013-4. — URL: https://book.ru/book/963333
5. Цифровой менеджмент : учебник / В. В. Масленников, Ю. В. Ляндау, И. А. Калинина [и др.]. — Москва : КноРус, 2026. — 207 с. — ISBN 978-5-406-14963-8. — URL: https://book.ru/book/960717
6. Максуров, А. А. Защита оборота персональных данных в киберпространстве : монография / А. А. Максуров. — Москва : Русайнс, 2023. — 123 с. — ISBN 978-5-466-03765-4. — URL: https://book.ru/book/950903
7. Ермакова, А. Н. Цифровой след: формирование и управляемость в экономике данных : монография / А. Н. Ермакова. — Ставрополь : СтГАУ, 2024. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/510158
8. Дремлюга, Р. И. Преступность 4.0 (киберпреступность: вчера, сегодня, завтра) : монография / Р. И. Дремлюга. — Москва : Infotropic Media, 2024. — 340 с. — ISBN 978-5-9998-0444-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/388181
9. Фот, Ю. Д. Методы защиты информации : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2019. — 230 с. — ISBN 978-5-7410-2296-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159977
10. Каберова, А. Р. Маркетинг организаций в цифровой среде : учебное пособие / А. Р. Каберова. — Москва : МТУСИ, 2025. — 147 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/501188
11. Каширина, А. М. Управление информационными ресурсами и контентом : учебное пособие / А. М. Каширина. — Новосибирск : НГТУ, 2023. — 72 с. — ISBN 978-5-7782-4858-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/404333

12. Устинова, И. Г. Основы информационного поиска и информационных знаний : учебное пособие / И. Г. Устинова. — Москва : Дело РАНХиГС, 2025. — 190 с. — ISBN 978-5-85006-687-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/511224

8.2. Дополнительная литература

1. Прикладные цифровые технологии и системы XXI века: экономика, менеджмент, управление персоналом, информационная безопасность, право: материалы II Межрегиональной научно-практической конференции 16 декабря 2022 года : материалы конференции. — Москва : Дело РАНХиГС, 2023. — 292 с. — ISBN 978-5-907389-72-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/468344

2. Драгунова, Е. В. Основы цифрового общества : учебное пособие / Е. В. Драгунова. — Новосибирск : НГТУ, 2024. — 120 с. — ISBN 978-5-7782-5168-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/514391

3. Доронина, И. М. Медиаправо и медиабезопасность : учебное пособие для вузов / И. М. Доронина. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 184 с. — ISBN 978-5-507-52147-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/440096

4. Информационные технологии и интеллектуальные системы: Сборник научных трудов по итогам III ежегодной национальной конференции (Москва, 18–20 марта 2025 г.) : сборник научных трудов / под редакцией А. А. Бакаева. — Москва : РТУ МИРЭА, 2025. — 1255 с. — ISBN 978-5-7339-2566-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/504827

5. Защита информации: IT, правовые и экономические аспекты: Сборник научных трудов: Межвузовская студенческая научно-практическая конференция (г. Москва, 16-17 марта 2023 г.) : сборник научных трудов / под редакцией А. А. Бакаева. — Москва : РТУ МИРЭА, 2023. — 209 с. — ISBN 978-5-7339-1914-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/382652

6. Цифровые технологии в прокурорской деятельности: Сборник материалов конференции : материалы конференции / составитель Е. В. Великая ; под редакцией Н. В. Субановой. — Москва : Издательский дом «Городец», 2024. — 320 с. — ISBN 978-5-907762-59-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/436376

8.3. Нормативные правовые документы и иная правовая информация

1. "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) https://www.consultant.ru/document/cons_doc_LAW_28399/
2. Гражданский кодекс Российской Федерации (ГК РФ) https://www.consultant.ru/document/cons_doc_LAW_5142/
3. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ https://www.consultant.ru/document/cons_doc_LAW_10699/
4. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ https://www.consultant.ru/document/cons_doc_LAW_34661/
5. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ https://www.consultant.ru/document/cons_doc_LAW_61798/
6. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ https://www.consultant.ru/document/cons_doc_LAW_61801/
7. Федеральный закон "Об исполнительном производстве" от 02.10.2007 N 229-ФЗ https://www.consultant.ru/document/cons_doc_LAW_71450/
8. Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ https://www.consultant.ru/document/cons_doc_LAW_32834/
9. Федеральный закон "О национальной платежной системе" от 27.06.2011 N 161-ФЗ https://www.consultant.ru/document/cons_doc_LAW_115625/
10. Федеральный закон "О банках и банковской деятельности" от 02.12.1990 N 395-1 https://www.consultant.ru/document/cons_doc_LAW_5842/
11. Федеральный закон "Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации" от 31.07.2020 N 258-ФЗ https://www.consultant.ru/document/cons_doc_LAW_358738/
12. Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» http://www.kremlin.ru/acts/bank/41919
13. Указ Президента Российской Федерации от 07.05.2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» http://www.kremlin.ru/acts/bank/50542
14. Постановление Правительства РФ от 29.06.2021 N 1046 (ред. от 27.08.2025) «О федеральном государственном контроле (надзоре) за обработкой персональных данных» https://www.consultant.ru/document/cons_doc_LAW_388756/

15. Приказ Роскомнадзора от 24.02.2021 N 18 "Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения" https://www.consultant.ru/document/cons_doc_LAW_382687/

8.4 Интернет-ресурсы

Официальный интернет-портал правовой информации — http://pravo.gov.ru

Государственная автоматизированная система «Правосудие» (ГАС «Правосудие») — https://sudrf.ru

Электронное правосудие — https://ej.sudrf.ru

Сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) — http://rkn.gov.ru

Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) — http://www.fstec.ru

Сайт Банка России — http://www.cbr.ru

Сайт Министерства цифрового развития, связи и массовых коммуникаций РФ (Минцифры России) — http://digital.gov.ru

Справочная правовая система «КонсультантПлюс» — http://www.consultant.ru

Справочная правовая система «Гарант» — http://www.garant.ru

Электронно-библиотечная система «BOOK.ru» — https://www.book.ru

Электронно-библиотечная система «Лань» — https://e.lanbook.com

Электронно-библиотечная система «ZNANIUM» — https://znanium.ru

СДО РАНХиГС — https://lms.ranepa.ru

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

№	Наименование
1.	Специализированные залы для проведения лекций, оснащенные персональным компьютером/ноутбуком и мультимедийным проектором
2.	Аудитории и компьютерные классы, оборудованные посадочными местами и персональными компьютерами с выходом в Интернет для проведения практических занятий
3.	«МТС Линк» — российская платформа для онлайн-коммуникаций и совместной работы команд; «Яндекс Телемост» — сервис для видеоконференций от Яндекса; Я-мессенджер
4.	Технические средства обучения: персональные компьютеры; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV; программы для работы с электронными таблицами для обработки, анализа и визуализации данных; соответствующие онлайн-

	инструменты для построения интеллект-карты и моделей в различных нотациях
5.	Научная библиотека (в т.ч. электронные информационные ресурсы научной библиотеки)
6.	СДО Академии https://lms.ranepa.ru/