Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Анатольевна
Должность: Ректор
Дата подписания: 10.10.2023 15:49:29
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Организационное и правовое обеспечение информационной безопасности»

Направление подготовки:
10.03.01 «Информационная безопасность»

Направленность (профиль):
«Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)»

Квалификация выпускника: **бакалавр**

Тольятти 2023

Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации 17.11.2020 № 1427.

Составитель:
Старший преподаватель _Ю.С. Мунирова

РПД обсуждена на заседании ученого совета Высшей школы интеллектуальных систем и кибертехнологий
23.05.2025 г., протокол № 10

Директор Высшей школы интеллектуальных систем и кибертехнологий ___к.э.н. доцент_____ О.А. Филиппова

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Цель освоения дисциплины – формирование у обучающихся системы знаний о правовых основах и организационных механизмах обеспечения информационной безопасности, умений применять нормативные правовые акты и методические документы в области защиты информации, а также навыков разработки организационно-распорядительной документации и участия в реализации комплекса организационных мер по защите информации на объекте.

-формирование у обучающихся общепрофессиональных компетенций *в области использования информационно-коммуникационных технологий и т.п.*

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ИОПК-5.1. Использует нормативные правовые документы в своей профессиональной деятельности	**Знать:** структуру законодательства РФ в области информационной безопасности; правовые режимы информации ограниченного доступа; полномочия регуляторов в области защиты информации; виды ответственности за правонарушения в информационной сфере **Уметь:** определять применимые нормативные правовые акты и методические документы для конкретной ситуации; квалифицировать сведения по видам тайны; анализировать правоприменительную практику **Владеть:** навыками поиска и анализа нормативных документов в справочно-правовых системах; навыками подготовки правовых обоснований решений по защите информации
	ИОПК-5.2. Осуществляет подбор, изучение и обобщение научно- технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности	
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять	ИОПК-10.1. Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики	**Знать:** структуру и содержание политики информационной безопасности, частных политик и регламентов; задачи и функции службы защиты информации; организационные меры защиты информации **Уметь:** разрабатывать проекты положений, инструкций, приказов по защите информации; организовывать допуск персонала к информации ограниченного доступа; планировать мероприятия
	ИОПК-10.2. Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности	

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
процессом их реализации на объекте защиты	ИОПК-10.3. Осуществляет управление процессом обеспечения информационной безопасности	по защите информации **Владеть:** навыками контроля соблюдения требований политики информационной безопасности и режима конфиденциальности; навыками документирования и разбора инцидентов информационной безопасности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к обязательной части, Блока 1. Дисциплины (модули) образовательной программы (Общепрофессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем дисциплины по видам учебной работы

Общая трудоёмкость дисциплины составляет **__3_ з.е. (_108_ час.)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**108**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**60/36**
занятия лекционного типа (лекции)	24/12
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	36/24
лабораторные работы	-
Самостоятельная работа всего, в т.ч.:	**48/68**
Самоподготовка по темам (разделам) дисциплины	48/68
Выполнение курсового проекта /курсовой работы	-/ -
Контроль (часы на экзамен, зачет)	**-/ 4**
Промежуточная аттестация	**зачет**

Примечание: *-/- объем часов соответственно для очной, очно-заочной форм обучения*

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ОПК-5 ИОПК-5.1	Тема 1. Информационная безопасность как объект организационного и правового регулирования . Содержание темы дисциплины: Понятия информации, информационной безопасности, защиты информации. Национальные интересы РФ в информационной сфере. Доктрина информационной безопасности Российской Федерации (2016 г.): угрозы, стратегические цели, основные направления. Соотношение правовых, организационных и технических мер защиты информации. Объекты, субъекты и принципы правового регулирования информационных отношений.	5 / 4				Устный опрос, тест
	Практическое занятие № 1. Анализ Доктрины информационной безопасности РФ: угрозы и направления обеспечения ИБ			5 / 4		
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-5 ИОПК-5.1 ИОПК-5.2	Тема 2. Система законодательства Российской Федерации в области информационной безопасности Содержание темы дисциплины Конституционные основы обеспечения информационной безопасности. Структура законодательства: федеральные законы, указы Президента РФ, постановления Правительства РФ, нормативные акты ФСТЭК России и ФСБ России, национальные стандарты. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: основные понятия, принципы, классификация информации по категориям доступа. Международные договоры и стандарты в сфере информационной безопасности	5 / 4				Устный опрос
	Практическое занятие 2. Поиск и систематизация нормативных правовых			5 / 4		практическое задание

	актов в СПС «КонсультантПлюс»; анализ Федерального закона № 149-ФЗ					
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-5 ИОПК-5.1, ИОПК-5.2,	Тема 3. Правовые режимы информации ограниченного доступа Содержание темы дисциплины Перечень сведений конфиденциального характера (Указ Президента РФ № 188). Государственная тайна: понятие, степени секретности, грифы, допуск и доступ, засекречивание и рассекречивание (Закон РФ «О государственной тайне»). Коммерческая тайна: режим коммерческой тайны, меры по его установлению (Федеральный закон № 98-ФЗ). Служебная информация ограниченного распространения (пометка «Для служебного пользования»). Профессиональные тайны: банковская, врачебная, адвокатская, налоговая, тайна связи.	5 / 4-				устный опрос
	Практическое занятие № 3. Квалификация сведений по видам тайны; разработка перечня сведений, составляющих коммерческую тайну			5 / 4		Практическое задание,
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-5 ИОПК-5.1, ИОПК-5.2,	Тема 4. Правовое регулирование обработки и защиты персональных данных Содержание темы дисциплины Федеральный закон № 152-ФЗ «О персональных данных»: понятия, принципы и условия обработки, категории персональных данных, согласие субъекта. Права субъекта персональных данных и обязанности оператора. Уведомление Роскомнадзора об обработке персональных данных. Требования к защите персональных данных при их обработке в информационных системах (Постановление Правительства РФ № 1119), уровни защищенности. Состав и содержание мер по обеспечению безопасности персональных данных	5 / 4				Устный опрос, тест

	(Приказ ФСТЭК России № 21). Трансграничная передача персональных данных.					
	Практическое занятие № 4. Разработка комплекта документов оператора персональных данных (политика обработки ПДн, согласие, уведомление в Роскомнадзор); определение уровня защищенности ПДн			5 / 4		практическое задание,
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-5 ИОПК-5.1, ОПК-10 ИОПК-10.1	Тема 5. Государственная система защиты информации. Лицензирование и сертификация Содержание темы дисциплины Структура государственной системы защиты информации. Полномочия ФСТЭК России, ФСБ России, Роскомнадзора, Минцифры России. Лицензирование деятельности по технической защите конфиденциальной информации и деятельности, связанной с шифровальными (криптографическими) средствами. Сертификация средств защиты информации, аттестация объектов информатизации. Безопасность значимых объектов критической информационной инфраструктуры (Федеральный закон № 187-ФЗ).	5 / 4-				Устный опрос,
	Практическое занятие № 5. Работа с реестрами ФСТЭК России: сертифицированные СЗИ, лицензиаты; анализ требований 187-ФЗ			5 / 4		доклад
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-10 ИОПК-10.1 ИОПК-10.2 ИОПК-10.3	Тема 6. Политика информационной безопасности и организационно-распорядительная документация Содержание темы дисциплины Политика информационной безопасности организации: назначение, структура, порядок разработки, утверждения и пересмотра. Частные политики. Требования ГОСТ Р ИСО/МЭК 27001 и ГОСТ Р ИСО/МЭК 27002 к документированию системы менеджмента информационной безопасности. Состав организационно-распорядительной документации по	5 / 4				устный опрос

	защите информации: приказы, положения, перечни, инструкции, журналы. Перечень сведений, составляющих коммерческую тайну, положение о конфиденциальной информации					
	Практическое занятие № 6. Разработка политики информационной безопасности организации			5 / 4		Практическое задание,
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-10 ИОПК-10.2 ИОПК-10.3	Тема 7. Организационные меры защиты информации. Служба защиты информации Содержание темы дисциплины Работа с персоналом: подбор, проверка, обучение, оформление обязательств о неразглашении, контроль, увольнение. Разграничение доступа сотрудников к информации ограниченного доступа. Пропускной и внутриобъектовый режим. Организация охраны помещений. Служба защиты информации (подразделение ИБ): задачи, функции, структура, права и обязанности, взаимодействие с другими подразделениями. Планирование и контроль мероприятий по защите информации.	5 / 4				тест
	Практическое занятие № 7. Разработка положения о службе защиты информации, инструкции пользователя и обязательства о неразглашении			5 / 4		Практическое задание,
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
ОПК-5 ИОПК-5.2, ОПК-10 ИОПК-10.2	Тема 8. Ответственность за правонарушения в информационной сфере. Реагирование на инциденты Содержание темы дисциплины Дисциплинарная, гражданско-правовая, административная и уголовная ответственность за нарушения в информационной сфере. Составы преступлений в сфере компьютерной информации (гл. 28 УК РФ). Административные правонарушения в области связи и информации (ст. 13.11–13.14 КоАП РФ). Порядок служебного расследования. Инциденты	5 / 4				Устный опрос,

	информационной безопасности: выявление, регистрация, реагирование, взаимодействие с ГосСОПКА.					
	Практическое занятие № 8. Решение ситуационных задач по квалификации правонарушений; составление акта служебного расследования			5 / 4		решение ситуационных задач
	Самостоятельная работа. Изучение лекционного материала, основной и дополнительной литературы				8 / 11	
	ИТОГО	**24/12**	**- / -**	**36/24**	**48/68**	

Примечание: *-/- объем часов соответственно для очной, очно-заочной форм обучения*

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов **образовательных технологий:**

-балльно-рейтинговая технология оценивания;

- электронное обучение;

- проблемное обучение;

- разбор конкретных ситуаций;

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в поточной аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

В ходе лекционных занятий рекомендуется конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

Отдельные темы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям / лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.4. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа/ на практических занятиях

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;

- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;

- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Практические занятия организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предусматривает: *выполнение всех заданий на практических занятиях.*

4.5. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

Самостоятельная работа студентов включает:

1. Изучение учебной литературы по курсу.

2. Решение практических ситуаций и задач

Подготовка рефератов

3. Работу с ресурсами Интернет

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Нормативные правовые акты и нормативно-методические документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). - Текст : электронный // КонсультантПлюс : сайт. – URL: http://www.consultant.ru (дата обращения: 09.11.2023).

2. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 N 149-ФЗ (последняя ред.) : [принят Гос. Думой 8 декабря 2006 г. : одобрен Советом Федерации 14 июля 2006 г.]. – Текст : электронный // КонсультантПлюс : сайт. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 09.11.2023).

3. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (последняя ред.) : [принят Гос. Думой 08 июля 2006 г. : одобрен Советом Федерации 15 июля 2006 г.]. - Текст : электронный // КонсультантПлюс : сайт. - URL: http://www.consultant.ru (дата обращения: 09.11.2023).

4. О коммерческой тайне : Федеральный закон от 29.07.2004 №98-ФЗ (последняя ред.) : [принят Гос. Думой 9 июля 2004 г. : одобрен Советом Федерации 15 июля 2004 г.]. – Текст : электронный // КонсультантПлюс : сайт. – URL: https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 09.11.2023).

5. О государственной тайне : Федеральный закон от 21.07.1993 №5485-1 (последняя ред.) : [принят Гос. Думой 1 июля 1993 г. : одобрен Советом Федерации 13 июля 1993 г.]. – Текст : электронный // КонсультантПлюс : сайт. – URL: https://www.consultant.ru/document/cons_doc_LAW_1406/ (дата обращения: 05.02.2025).

6. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 № 646. – Текст : электронный // Консорциум Кодекс. Электрон. фонд правовой и нормативно-техн. документации : [сайт]. - URL: http://docs.cntd.ru (дата обращения: 09.11.2023).

7. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : Указ Президента РФ от 01.05.2022 № 250 (с изменениями на 13 июня 2024 года). – Текст : электронный // Консорциум Кодекс. Электрон. фонд правовой и нормативно-техн. документации : [сайт]. - URL: http://docs.cntd.ru (дата обращения: 09.11.2023).

8. Об электронной подписи : Федеральный закон от 06.04.2011 №63-ФЗ (последняя ред.) : [принят Гос. Думой 25 марта 2011 г. : одобрен Советом Федерации 30 марта 2011 г.]. – Текст : электронный // КонсультантПлюс : сайт. – URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 09.11.2023).

9. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения : дата введения 2008-02-01. – Текст : электронный // Консорциум Кодекс. Электрон. фонд правовой и нормативно-техн. документации : [сайт]. - URL: http://docs.cntd.ru (дата обращения: 09.11.2023).

10. ГОСТ Р ИСО/МЭК 27011-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной

безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002 : нац. стандарт Российской Федерации : утв. и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. N 424-ст : дата введения 2014-01-01. – Текст : электронный // Консорциум Кодекс. Электрон. фонд правовой и нормативно-техн. документации : [сайт]. - URL: http://docs.cntd.ru (дата обращения: 09.11.2023).

Основная литература

11. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения [в области информационной безопасности (защиты информации)] : учеб. пособие для студентов (слушателей) по доп. проф. прогр. в обл. информ. безопасности / В. К. Новиков. - Москва : Горячая линия -Телеком, 2017. - 176 с. : ил. - Прил. - ISBN 978-5-9912-0525-2 : 400-18. - Текст : непосредственный.

12. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник по направлению подгот. "Информ. безопасность" / М. В. Тумбинская, М. В. Петровский. - Изд. 2-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 344 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/256133 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-45046-6 : 0-00. - Текст : электронный.

13. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учеб. пособие для вузов по направлению 09.03.01 "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ read. - Москва : ФОРУМ [и др.], 2022. - 592 с. : ил. - (Высшее образование - Бакалавриат) (Высшее образование - Бакалавриат). - Предм. указ. - URL: https://znanium.ru/read?id=389857 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8199-0730-6. - 978-5-16-106148-0. - Текст : электронный.

14. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учеб. пособие для студентов высш. учеб. заведений по укрупн. группе специальностей 10.05.00. "Информационная безопасность" / Ю. Н. Сычев. - 2-е изд., перераб. и доп. - Документ read. - Москва : ИНФРА-М, 2024. - 602 с. - (Высшее образование - специалитет). - Прил. - URL: https://znanium.ru/read?id=443671 (дата обращения: 30.09.2025). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-112445-1. - Текст : электронные.

15. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие по направлению "Приклад. информатика" / Е. К. Баранова, А. В. Бабаш. - 5-е изд., перераб. и доп. - Документ read. - Москва : РИОР [и др.], 2026. - 384 с. - (Высшее образование). - Прил. - URL: https://znanium.ru/read?id=477891 (дата обращения: 26.05.2026). - Режим доступа: для авториз. пользователей. - ISBN 78-5-369-02005-0. - 978-5-16-114639-2. - Текст : электронный.

Дополнительная литература

14. Башлы, П. Н. Информационная безопасность : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Документ read. - Москва : РИОР, 2013. - 222 с. : ил. - Слов. терминов. - URL: https://znanium.ru/read?id=213488 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-001178-2. - Текст : электронный.

15. Борисов, М. А. Основы организационно-правовой защиты информации : [учеб. пособие] / М. А. Борисов, О. А. Романов. - Изд. 2-е. - Москва : Кн. дом "ЛИБРОКОМ", 2013. - 208 с. - (Основы защиты информации). - Прил. - ISBN 978-5-397-03361-9 : 200-00. - Текст : непосредственный.

16. Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере : монография / Н. Н. Куняев. – Документ read. – Москва : Логос, 2020. – 348 с. – URL: https://znanium.com/read?id=367507 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-98704-513-8. – Текст : электронный.

17. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учеб. пособие для студентов вузов по направлению подгот. 090900 "Информ. безопасность" (уровни - бакалавр, магистр) / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - Москва : Горячая линия -Телеком, 2018. - 214 с. : ил. - (Вопросы управления информационной безопасностью. Кн. 4). - Прил. - ISBN 978-5-9912-0364-7 : 377-74. - Текст : непосредственный.

18. Организационно-правовое обеспечение информационной безопасности : учеб. пособие для вузов по специальностям "Компьютер. безопасность", "Комплекс. обеспеч. информ. безопасности автоматизир. систем", "Информ. безопасность телекоммуникац. систем" / А. А. Стрельцов, В. С. Горбатов, Т. А. Полякова [и др.] ; под ред. А. А. Стрельцова. - Москва : Академия, 2008. - 249 с. : табл. - (Высшее профессиональное образование. Информационная безопасность). - ISBN 978-5-7695-4240-4 : 255-20. - Текст : непосредственный.

19. Основы управления информационной безопасностью : учеб. пособие для вузов по направлениям подгот. (специальностям) укрупн. группы специальностей "Информ. безопасность" / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - Москва : Горячая линия -Телеком, 2016. - 244 с. : ил. - (Вопросы управления информационной безопасностью. Книга 1). - Прил. - ISBN 978-5-9912-0361-6 : 400-18. - Текст : непосредственный.

20. Чепурнова, Н. М. Правовые основы прикладной информатики : учеб. пособие / Н. М. Чепурнова, Л. Л. Ефимова. – Документ read. – Москва : Курс [и др.], 2019. – 192 с. – URL: https://znanium.com/read?id=354636 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-906818-01-0. - 978-5-16-102928-2. – Текст : электронный.

21. Противодействие преступлениям, совершаемым в сфере информационных технологий : учеб. по специальностям 40.05.01 "Правовое обеспечение нац. безопасности", 40.05.02 "Правоохранит. деятельность" (квалификация "юрист"), 40.05.03 "Судебная экспертиза" (квалификация судебный эксперт), 10.05.01 "Компьютер. безопасность", 10.05.05 "Безопасность информ. технологий в правоохранит. сфере" (квалификация "специалист по зпщите информации") / И. А. Калиниченко, А. В. Андреев, В. В. Гончар [и др.] ; под ред. И. А. Калиниченко. - Документ read. - Москва : ИНФРА-М, 2024. - 642 с. - (Высшее образование - Специалитет). - Прил. - URL: https://znanium.ru/read?id=438959 (дата обращения: 11.04.2025). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-110845-1. - Текст : электронный.

22. Русскевич, Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : учеб. пособие / Е. А. Русскевич. - 2-е изд., доп. - Документ read. - Москва : ИНФРА-М, 2024. - 188 с. - (Высшее образование - Магистратура). - Прил. - URL: https://znanium.ru/read?id=444124 (дата обращения: 03.04.2025). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-106903-5. - Текст : электронный.

23. Противодействие преступлениям в сфере информационных технологий : учебник / И. А. Калиниченко, А. В. Андреев, Д. В. Галиев [и др.] ; под ред. И. А. Калиниченко ; тех. ред. В. В. Гончар. - Документ read. - Москва : ИНФРА-М, 2025. - 806 с. с. - (Высшее образование). - Прил. - URL: https://znanium.ru/read?id=452569 (дата обращения: 03.04.2025). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-112340-9. - Текст : электронный.

24. Вершинин, А. П. Доступ к цифровой информации: правовое регулирование : учеб. пособие / А. П. Вершинин. - 2-е изд., перераб. и доп. - Москва : ИНФРА-М, 2026. - 265 с. - (Высшее образование). - Прил. - URL: https://znanium.ru/read?id=482858 (дата обращения: 10.09.2026). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-114768-9. - Текст : электронные.

25. Защита информации : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 3-е изд. - Документ read. - Москва : РИОР [и др.], 2024. - 400 с. - (Высшее образование). - URL: https://znanium.ru/read?id=443251 (дата обращения: 29.04.2025). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01759-3. - 978-5-16-106478-8. - Текст : электронный.

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. 3DNEWS.RU : Электронное периодическое издание : сайт. – Москва, 1997 - . - URL: https://3dnews.ru/ (дата обращения: 09.11.2023). – Текст: электронный.

2. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 - . - URL: https://elibrary.ru (дата обращения: 09.11.2023). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

3. Консорциум Кодекс. Электрон. фонд правовой и нормативно-техн. документации : [сайт]. – URL: http://docs.cntd.ru (дата обращения: 09.11.2023). – Текст электронный.

4. КонсультантПлюс : справочная правовая система : сайт / ЗАО «КонсультантПлюс». – Москва, 1992 - . - URL: http://www.consultant.ru (дата обращения: 09.11.2023). - Текст : электронный.

5. Электронная библиотека. Техническая литература : сайт. - URL : http://techliter.ru/ (дата обращения: 09.11.2023). - Текст : электронный.

6. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти, 2010 - . - URL. : http://elib.tolgas.ru (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный.

7. Электронно-библиотечная система Znanium.com : сайт / ООО "ЗНАНИУМ". – Москва, 2011 - . - URL: https://znanium.com/ (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный.

8. Электронно-библиотечная система Лань : сайт / ООО "ЭБС ЛАНЬ". - Москва, 2011 - . - URL: https://e.lanbook.com/ (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

компьютерные классы университета;

библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
	Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
зачет	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
	пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
			70-85,9	«хорошо» / 4	зачтено
	повышенный	86-100	86-100	«отлично» / 5	зачтено

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

***Результат обучения считается сформированным (повышенный уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.*

***Результат обучения считается сформированным (пороговый уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.*

***Результат обучения считается несформированным**, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует*

необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.

Формы текущего контроля успеваемости

Формы текущего контроля	Количество контрольных точек	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Доклад/сообщение	5	4	20
Тестирование по темам лекционных занятий	4	10	40
Устный опрос, практическое задание	5	4	20
Творческий рейтинг (участие в конференциях, олимпиадах и т.п.) *Дополнительные баллы за активное изучение дисциплины и др.*	2	10	20
Итого по дисциплине			**100 баллов**

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (семинарским) занятиям

3.1. Вопросы для устного опроса

Тема 1. Информационная безопасность как объект организационного и правового регулирования

1. Раскройте содержание понятий «информационная безопасность» и «защита информации» по ГОСТ Р 50922-2006.

2. Каковы национальные интересы РФ в информационной сфере согласно Доктрине информационной безопасности?

3. Назовите основные угрозы информационной безопасности, выделяемые в Доктрине.

4. Как соотносятся правовые, организационные и технические меры защиты информации?

Тема 2. Система законодательства Российской Федерации в области информационной безопасности

1. Какие положения Конституции РФ являются основой правового регулирования информационных отношений?

2. Охарактеризуйте иерархию нормативных правовых актов в области защиты информации.

3. Как классифицируется информация по категориям доступа в Федеральном законе № 149-ФЗ?

4. Какие обязанности обладателя информации установлены законом № 149-ФЗ?

5. Какова роль национальных стандартов в обеспечении информационной безопасности?

Тема 3. Правовые режимы информации ограниченного доступа

1. Перечислите виды сведений конфиденциального характера по Указу Президента РФ № 188.

2. Какие степени секретности сведений, составляющих государственную тайну, установлены законом?

3. Какие меры обязан принять обладатель информации для установления режима коммерческой тайны?

4. Какие сведения не могут составлять коммерческую тайну?

5. Чем режим служебной информации ограниченного распространения отличается от режима коммерческой тайны?

Тема 4. Правовое регулирование обработки и защиты персональных данных

1. Назовите принципы обработки персональных данных.

2. Какие категории персональных данных выделяет закон № 152-ФЗ?

3. Какие сведения должно содержать согласие субъекта на обработку персональных данных?

4. Как определяется уровень защищенности персональных данных в ИСПДн?

5. Какие обязанности возникают у оператора при утечке персональных данных?

Тема 5. Государственная система защиты информации. Лицензирование и сертификация

1. Каковы полномочия ФСТЭК России в области защиты информации?

2. Какие виды деятельности в области защиты информации подлежат лицензированию?

3. Чем сертификация средств защиты информации отличается от аттестации объекта информатизации?

4. Что относится к объектам критической информационной инфраструктуры?

Тема 6. Политика информационной безопасности и организационно-распорядительная документация

1. Какова структура политики информационной безопасности организации?

2. Кто утверждает политику ИБ и как часто она пересматривается?

3. Назовите основные организационно-распорядительные документы по защите информации.

4. Какие требования к документированию СМИБ предъявляет ГОСТ Р ИСО/МЭК 27001?

Тема 7. Организационные меры защиты информации. Служба защиты информации

1. Какие мероприятия проводятся при приеме сотрудника на работу, связанную с конфиденциальной информацией?

2. Что включает организация пропускного и внутриобъектового режима?

3. Каковы задачи и функции службы защиты информации?

4. Как организуется контроль выполнения мероприятий по защите информации?

Тема 8. Ответственность за правонарушения в информационной сфере. Реагирование на инциденты

1. Какие виды юридической ответственности предусмотрены за нарушения в информационной сфере?

2. Перечислите составы преступлений гл. 28 УК РФ.

3. Какая ответственность установлена ст. 13.11 КоАП РФ?

4. Каков порядок проведения служебного расследования по факту разглашения конфиденциальной информации?

5. Какие этапы включает процесс реагирования на инцидент ИБ?

3.2. Тестовые задания закрытого типа

Примечание: правильные варианты ответов выделены ***полужирным шрифтом с подчеркиванием****. В варианте ФОС, предъявляемом обучающимся, выделение снимается.*

1. Основным федеральным законом, регулирующим отношения при осуществлении права на поиск, получение, передачу, производство и распространение информации, является: (ИОПК-5.1)

а) Федеральный закон № 152-ФЗ

б) Федеральный закон № 149-ФЗ

в) Федеральный закон № 98-ФЗ

г) Федеральный закон № 63-ФЗ

2. В зависимости от категории доступа информация подразделяется на: (ИОПК-5.1)

а) открытую и секретную

б) общедоступную и информацию ограниченного доступа

в) документированную и недокументированную

г) государственную и коммерческую

3. Перечень сведений конфиденциального характера утвержден: (ИОПК-5.1)

а) Федеральным законом № 149-ФЗ

б) Указом Президента РФ № 188

в) Постановлением Правительства РФ № 1119

г) Приказом ФСТЭК России № 17

4. Степени секретности сведений, составляющих государственную тайну: (ИОПК-5.1)

а) «конфиденциально», «секретно», «совершенно секретно»

б) «для служебного пользования», «секретно», «особой важности»

в) «секретно», «совершенно секретно», «особой важности»

г) «секретно» и «строго секретно»

5. Режим коммерческой тайны считается установленным после принятия обладателем информации мер, предусмотренных: (ИОПК-5.2)

а) ст. 10 Федерального закона № 98-ФЗ

б) ст. 19 Федерального закона № 152-ФЗ

в) ст. 16 Федерального закона № 149-ФЗ

г) ст. 272 УК РФ

6. На документах, содержащих коммерческую тайну, проставляется гриф: (ИОПК-5.2)

а) «Для служебного пользования»

б) «Коммерческая тайна» с указанием обладателя информации

в) «Секретно»

г) «Конфиденциально» без указания обладателя

7. Федеральный орган исполнительной власти, уполномоченный в области защиты прав субъектов персональных данных: (ИОПК-5.1)

а) ФСТЭК России

б) ФСБ России

в) Роскомнадзор

г) Минцифры России

8. Количество уровней защищенности персональных данных, установленных Постановлением Правительства РФ № 1119: (ИОПК-5.2)

а) два

б) три

в) четыре

г) шесть

9. К специальным категориям персональных данных относятся сведения о (выберите все верные): (ИОПК-5.2)

а) состоянии здоровья

б) политических взглядах

в) фамилии, имени, отчестве

г) религиозных убеждениях

10. Лицензирование деятельности по технической защите конфиденциальной информации осуществляет: (ИОПК-5.1)

а) ФСБ России

б) ФСТЭК России

в) Роскомнадзор

г) Минобороны России

11. Лицензирование деятельности, связанной с шифровальными (криптографическими) средствами, осуществляет: (ИОПК-5.1)

а) ФСТЭК России

б) ФСБ России

в) Минцифры России

г) Роскомнадзор

12. Документ, определяющий цели, принципы и правила обеспечения информационной безопасности организации на высшем уровне, – это: (ИОПК-10.1)

а) инструкция пользователя

б) политика информационной безопасности

в) журнал учета носителей

г) акт классификации

13. Неправомерный доступ к охраняемой законом компьютерной информации квалифицируется по статье: (ИОПК-5.2)

а) 272 УК РФ

б) 273 УК РФ

в) 274 УК РФ

г) 183 УК РФ

14. Создание, использование и распространение вредоносных компьютерных программ квалифицируется по статье: (ИОПК-5.2)

а) 272 УК РФ

б) 273 УК РФ

в) 274.1 УК РФ

г) 137 УК РФ

15. Незаконное получение и разглашение сведений, составляющих коммерческую тайну, квалифицируется по статье: (ИОПК-5.2)

а) 183 УК РФ

б) 272 УК РФ

в) 283 УК РФ

г) 138 УК РФ

16. Национальный стандарт, устанавливающий требования к системам менеджмента информационной безопасности: (ИОПК-10.1)

а) ГОСТ Р 50922-2006

б) ГОСТ Р ИСО/МЭК 27001-2021

в) ГОСТ Р 7.0.97-2016

г) ГОСТ 34.602-2020

17. Обязательство о неразглашении конфиденциальной информации оформляется: (ИОПК-10.2)

а) только при увольнении работника

б) при приеме на работу или допуске к конфиденциальной информации

в) только по требованию работника

г) по решению суда

18. Федеральный закон № 187-ФЗ регулирует отношения в области обеспечения безопасности: (ИОПК-5.1)

а) персональных данных

б) критической информационной инфраструктуры

в) электронной подписи

г) коммерческой тайны

19. Пропускной режим – это: (ИОПК-10.2)

а) совокупность правил, регламентирующих порядок входа (выхода) лиц, въезда (выезда) транспорта, вноса (выноса) материальных ценностей

б) порядок хранения документов

в) система паролей пользователей

г) перечень сведений, составляющих тайну

20. Нарушение законодательства РФ в области персональных данных влечет административную ответственность по статье КоАП РФ: (ИОПК-5.2)

а) 13.11

б) 13.14

в) 19.7

г) 5.39

Типовые задания к практическим занятиям

1. Составьте схему иерархии нормативных правовых актов РФ в области защиты информации с примерами документов каждого уровня.

2. Для предприятия торговли (условные исходные данные) разработайте перечень сведений, составляющих коммерческую тайну, и обоснуйте каждый пункт.

3. Определите уровень защищенности персональных данных для ИСПДн «Кадры» (сотрудники оператора, 250 субъектов, угрозы 3-го типа) и перечислите требуемые меры защиты.

4. Подготовьте проект политики обработки персональных данных оператора в соответствии со ст. 18.1 Федерального закона № 152-ФЗ.

5. Разработайте проект политики информационной безопасности организации (разделы: цели, область действия, принципы, роли и ответственность, порядок пересмотра).

6. Разработайте положение о службе защиты информации и должностную инструкцию администратора безопасности.

7. По материалам кейса квалифицируйте правонарушение (дисциплинарное, административное, уголовное) и составьте акт служебного расследования.

8. С использованием реестра ФСТЭК России подберите сертифицированные средства защиты информации для заданного класса ИС и оформьте обоснование.

3.5. Темы докладов (рефератов)

1. Эволюция законодательства РФ о защите информации.

2. Доктрина информационной безопасности РФ 2016 г.: новеллы и приоритеты.

3. Правовой режим коммерческой тайны: судебная практика.

4. Ответственность операторов за утечки персональных данных: изменения законодательства 2022–2025 гг.

5. Трансграничная передача персональных данных.

6. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

7. Категорирование объектов КИИ: порядок и практика.

8. Организация работы службы информационной безопасности на предприятии.

9. Социальная инженерия и организационные меры противодействия.

10. Сертификация средств защиты информации в РФ.

11. Международные стандарты серии ISO/IEC 27000 и их применение в России.

12. Расследование инцидентов информационной безопасности.

8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: *зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования).*

Устно-письменная форма по экзаменационным билетам предполагается, как правило, для сдачи академической задолженности.

Перечень вопросов к зачету

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

1. Понятия информации, информационной безопасности и защиты информации.
2. Доктрина информационной безопасности РФ: национальные интересы и угрозы.
3. Соотношение правовых, организационных и технических мер защиты информации.
4. Структура законодательства РФ в области информационной безопасности.
5. Федеральный закон № 149-ФЗ: основные понятия и принципы.
6. Классификация информации по категориям доступа.
7. Перечень сведений конфиденциального характера (Указ Президента РФ № 188).
8. Государственная тайна: понятие, степени секретности, грифы.
9. Допуск и доступ к государственной тайне.
10. Коммерческая тайна: понятие и режим коммерческой тайны.
11. Охрана конфиденциальности информации в рамках трудовых и гражданско-правовых отношений.
12. Служебная информация ограниченного распространения.
13. Профессиональные тайны: виды и правовое регулирование.
14. Федеральный закон № 152-ФЗ: принципы и условия обработки персональных данных.
15. Права субъекта персональных данных и обязанности оператора.
16. Уровни защищенности персональных данных и требования к их обеспечению.
17. Состав мер по обеспечению безопасности персональных данных (Приказ ФСТЭК России № 21).

ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

18. Государственная система защиты информации: органы и их полномочия.
19. Лицензирование деятельности в области защиты информации.
20. Сертификация средств защиты информации и аттестация объектов информатизации.
21. Правовое регулирование безопасности КИИ (Федеральный закон № 187-ФЗ).
22. Политика информационной безопасности: структура и порядок разработки.
23. Организационно-распорядительная документация по защите информации.
24. Требования ГОСТ Р ИСО/МЭК 27001 к СМИБ.
25. Работа с персоналом в целях защиты информации.

26. Пропускной и внутриобъектовый режим.

27. Служба защиты информации: задачи, функции, структура.

28. Виды юридической ответственности за правонарушения в информационной сфере.

29. Преступления в сфере компьютерной информации (гл. 28 УК РФ).

30. Административная ответственность в области связи и информации.

31. Служебное расследование по факту нарушения режима конфиденциальности.

32. Управление инцидентами информационной безопасности.