МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета
математики и компьютерных
наук имени профессора Н.И. Червякова
Гробова Т.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Организационное и правовое обеспечение информационной безопасности»

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	8-9

Разработано
Лапина М.А. - доцент кафедры вычислительной математики и кибернетики.

Ставрополь 2026 г.

1.Цель и задачи освоения дисциплины

Целью освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» системных знаний и практических навыков в области организационного управления и правового регулирования информационной безопасности, необходимых для профессиональной деятельности

Задачи дисциплины:

- изучение нормативно-правовой базы Российской Федерации и международных стандартов в области информационной безопасности;
- освоение принципов организационного обеспечения защиты информации на предприятиях и в учреждениях;
- формирование навыков разработки организационно-распорядительных документов по информационной безопасности;
- изучение методов правового регулирования отношений в информационной сфере;
- приобретение компетенций в области лицензирования, сертификации и аттестации объектов информатизации;
- развитие умений проводить правовую экспертизу документов и действий в сфере информационной безопасности;
- освоение методик расследования инцидентов информационной безопасности с правовой точки зрения.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к части, формируемой участниками образовательных отношений дисциплинам (модулям) обязательной части. Ее освоение происходит в 8-9 семестрах.

3. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ИД-1ОПК-5 Знаком с действующим законодательством Российской Федерации в области информационной безопасности и защиты информации; системами защиты государственной тайны; определяет перечень сведений, относящихся к конфиденциальной информации и способы ее защиты; знаком с понятием и принципами электронной подписи (ЭП); определяет виды компьютерных вирусов; классифицирует компьютерные преступления; использует понятие и способы защиты интеллектуальной собственности; Знаком с действующим законодательством в области международного и российского права в области	Предоставляет детально проработанный план по использованию Законодательства Российской Федерации в области информационной безопасности и защиты информации; систем защиты государственной тайны с перечнем сведений относящихся к конфиденциально й информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуальной собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации.

	защиты информации; знаком со способами совершения преступлений в сфере компьютерной информации; знаком с правовыми режимами защиты информации.	
	ИД-2ОПК-5 Определяет рациональные меры по обеспечению организационной защите на объекте; организует работу персонала с конфиденциальной информацией; разрабатывает проекты нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.	Предоставляет детально проработанный план по организации защиты на объекте; организации работы персонала с конфиденциальной информацией; разработке проектов нормативных документов, регламентирующи х работу по защите информации, а также положений, инструкций и других организационно- распорядительны х документов
	ИД-3ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	Предоставляет детальный отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующи е деятельность по защите информации
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД-1ОПК-6 Знаком с нормативно-правовыми механизмами лицензирования, сертификации и аттестации; принципами организационного обеспечения информационной безопасности; основными угрозами информационной безопасности на объекте (в организации); порядком организации службы безопасности на объекте; типовыми структурами службы безопасности, ее основными задачами и функциями должностных лиц; роль персонала в обеспечении информационной безопасности на объекте; основами организационной защиты информации, ее современные проблемы и терминологию; основными руководящими документами по обеспечению режима и конфиденциальности на объекте; основными документами, регламентирующими организационную безопасность на объекте.	определяет критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
	ИД-2ОПК-6 Эффективно применяет знания теории и методики курса при раскрытии компьютерных преступлений, при	разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет

	работе с конфиденциальной информацией и государственной тайной, при работе с организационно- правовым обеспечением, при работе с ЭП, при защите авторского и международного права, при проведении экспертизы преступлений в сфере компьютерной информации; применять нормативно-правовые акты при защите информации; оценивать состояние организационной защиты информации на объекте.	политику контроля доступа работников к информации ограниченного доступа
	ИД-ЗОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей

4. Объем учебной дисциплины и формы контроля *

Объем занятий: всего: **7** з.е. 252 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	32/0 36/0
Лабораторных работ/из них практическая подготовка	0
Практических занятий/из них практическая подготовка	48/0 54/0
Самостоятельная работа	46
Формы контроля	
Экзамен **9 семестр**	36
Зачет **8 семестр**	+
Зачет с оценкой	-
Курсовая работа	нет

* Дисциплина предусматривает применение электронного обучения, дистанционных образовательных технологий

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества часов и видов занятий

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	очная форма				Формы текущего контроля успеваемости
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов	
			Лекции	Практические занятия	Лабораторные работы		
	8 СЕМЕСТР						
1.	**Анализ структуры и нормативной базы компании в сфере информационной безопасности** Изучение внутренней системы компании и её соответствия требованиям ИБ. В данной теме студентам предстоит изучить внутреннюю организацию компании и её нормативные документы в сфере информационной безопасности. Особое внимание будет уделено анализу соответствия внутренней документации требованиям законодательства и стандартов ИБ. В конце изучения темы студент будет уметь оценивать структуру ИБ компании и выявлять несоответствия.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование

2.	**Законодательство РФ в области информационной безопасности** Анализ действующих законов, регулирующих сферу ИБ в России. В данной теме студентам предстоит ознакомиться с основными законами РФ, регулирующими сферу информационной безопасности. Особое внимание будет уделено таким актам, как ФЗ-152, ФЗ-149 и другим нормативным источникам. В конце изучения темы студент будет знать законодательную базу и уметь ориентироваться в применении соответствующих норм.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование
3.	**Нормативно-правовые акты. ФЗ «О техническом регулировании» в сфере информационной безопасности** Работа с федеральными законами и техническими нормами в ИБ. В данной теме студентам предстоит изучить положения ФЗ «О техническом регулировании» в контексте информационной безопасности. Особое внимание будет уделено роли стандартов и нормативов в обеспечении технической защиты информации. В конце изучения темы студент будет понимать механизм технического регулирования в ИБ.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	4	4	-	4	Собеседование
4.	**Правовое регулирование отдельных видов информации в сфере информационной безопасности** Изучение правовых аспектов защиты служебной и иной информации. В данной теме студентам предстоит изучить правовое регулирование отдельных видов информации — коммерческой, служебной, профессиональной. Особое внимание будет уделено условиям допуска, хранения и передачи таких данных. В конце изучения темы студент будет знать правовые основания охраны специальных видов информации.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование

5.	**Правовое обеспечение защиты банковской, профессиональной и служебной тайны** Разбор правовых механизмов охраны конфиденциальной информации. В данной теме студентам предстоит разобраться в правовых нормах, регулирующих защиту конфиденциальной информации в банковской, профессиональной и служебной сферах. Особое внимание будет уделено требованиям к хранению, доступу и передаче данных. В конце изучения темы студент будет уметь применять правовые нормы для защиты тайн.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование
6.	**Анализ аспектов обеспечения правовой защиты конфиденциальной информации** Проверка соответствия процессов требованиям по защите тайн. В данной теме студентам предстоит провести анализ соответствия процессов компании требованиям по защите конфиденциальной информации. Особое внимание будет уделено выявлению нарушений и разработке корректирующих мер. В конце изучения темы студент будет уметь оценивать правовую защищенность информации в организации.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	4	4	-	4	Собеседование
7.	**Правовое обеспечение защиты персональных данных** Работа с законом о персональных данных и практиками их защиты. В данной теме студентам предстоит изучить закон «О персональных данных» и практические аспекты их обработки и защиты. Особое внимание будет уделено согласию на обработку, правам субъектов данных и требованиям к операторам. В конце изучения темы студент будет знать, как юридически правильно обеспечивать защиту персональных данных.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование

8.	**Правовая охрана и защита патентного и авторского права** Разбор основ прав интеллектуальной собственности в ИБ. В данной теме студентам предстоит изучить правовые основы охраны патентов, авторских прав и других объектов интеллектуальной собственности в контексте информационной безопасности. Особое внимание будет уделено защите программного обеспечения, баз данных и технических решений. В конце изучения темы студент будет уметь применять правовые меры защиты ИС.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование
9.	**Структура органов. Общие функции органов госвласти в области ИБ** Изучение ролей ФСТЭК, ФСБ и других органов в обеспечении ИБ. В данной теме студентам предстоит ознакомиться со структурой государственных органов, участвующих в обеспечении информационной безопасности. Особое внимание будет уделено функциям ФСБ, ФСТЭК, Минцифры и другим ведомствам. В конце изучения темы студент будет знать распределение полномочий между органами власти в сфере ИБ.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	4	4	-	2	Собеседование
10.	**Интеллектуальная собственность и патенты в сфере информационной безопасности** Разбор механизмов патентной защиты технологий ИБ. В данной теме студентам предстоит рассмотреть вопросы патентования и авторской охраны технологий, применяемых в сфере информационной безопасности. Особое внимание будет уделено механизму получения патентов и регистрации прав. В конце изучения темы студент будет знать, как осуществляется охрана интеллектуальной собственности в ИБ.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование

11.	**Министерство обороны РФ и ФСТЭК России в системе информационной безопасности** Анализ функций ведомств в оборонной и гражданской сферах ИБ. В данной теме студентам предстоит проанализировать роль Министерства обороны и ФСТЭК России в обеспечении ИБ как в оборонной, так и гражданской сферах. Особое внимание будет уделено функциям по сертификации, контролю и регламентированию. В конце изучения темы студент будет понимать различия между ведомственными подходами к ИБ.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	4	4	-	2	Собеседование
12.	**Лицензирование и сертификация в области информационной безопасности** Порядок получения лицензий на деятельность в сфере защиты информации. В данной теме студентам предстоит изучить процесс лицензирования и сертификации деятельности в области защиты информации. Особое внимание будет уделено порядку получения лицензий, требованиям к соискателям и особенностям сертификации средств защиты. В конце изучения темы студент будет знать, как осуществляется допуск к работам в сфере ИБ.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование
	ИТОГО за 8 семестр		**32**	**48**	**-**	**28**	
	9 СЕМЕСТР						
13.	**Уголовная ответственность в сфере ИБ** Анализ статей УК РФ, связанных с преступлениями в ИБ. В данной теме студентам предстоит проанализировать статьи Уголовного кодекса РФ, предусматривающие ответственность за преступления в сфере информационной безопасности. Особое внимание будет уделено статьям 272–274. В конце изучения темы студент будет уметь распознавать уголовно наказуемые деяния, связанные с ИБ.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	2	-	2	Собеседование

14.	**Основы работы с российскими и международными стандартами в области информационной безопасности** Ознакомление с ISO, ГОСТ и другими стандартами. В данной теме студентам предстоит ознакомиться с основными российскими и международными стандартами в области ИБ, включая ISO/IEC 27001, ГОСТ Р 57580 и другие. Особое внимание будет уделено структуре, целям и применению этих стандартов. В конце изучения темы студент будет знать классификацию и назначение стандартов.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-		Собеседование
15.	**Анализ стандартов информационной безопасности** Сравнение отечественных и международных стандартов ИБ. В данной теме студентам предстоит провести сравнительный анализ стандартов информационной безопасности, применяемых в России и за рубежом. Особое внимание будет уделено различиям в подходах, терминологии и требованиях. В конце изучения темы студент будет уметь выбирать подходящий стандарт под задачи организации.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование
16.	**Анализ структуры и нормативной базы компании** Повторное исследование структуры ИБ в конкретной организации. В данной теме студентам предстоит повторно проанализировать структуру ИБ в конкретной компании. Особое внимание будет уделено выявлению соответствия внутренних процессов актуальным требованиям ИБ. В конце изучения темы студент будет способен представить структурную карту системы ИБ организации.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	4	4	-		Собеседование

17.	**Разработка политики безопасности компании** Создание документа, определяющего стратегию ИБ. В данной теме студентам предстоит разработать политику информационной безопасности компании. Особое внимание будет уделено целям политики, принципам, зонам ответственности и методам контроля. В конце изучения темы студент будет уметь создавать ИБ-документ, определяющий стратегию компании в этой области.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование
18.	**Разработка модели угроз компании** Идентификация и классификация возможных угроз. В данной теме студентам предстоит разработать модель угроз, характерных для конкретной организации. Особое внимание будет уделено систематизации угроз по источникам и последствиям. В конце изучения темы студент будет уметь составлять обоснованную и структурированную модель угроз.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование
19.	**Разработка модели нарушителя** Описание типов потенциальных нарушителей и их возможностей. В данной теме студентам предстоит разработать модель нарушителя — возможного злоумышленника. Особое внимание будет уделено классификации нарушителей по уровню доступа, мотивации и технической оснащённости. В конце изучения темы студент будет уметь описывать типы угроз и средства их реализации.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	4	4	-	2	Собеседование
20.	**Организация службы безопасности компании** Построение системы управления безопасностью в компании. В данной теме студентам предстоит изучить принципы организации службы информационной безопасности компании. Особое внимание будет уделено распределению ролей, определению зон ответственности и взаимодействию с другими подразделениями. В конце изучения темы студент будет понимать структуру и задачи службы ИБ.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-		Собеседование

21.	**Организация внутриобъектного режима компании** Разработка мер ограничения доступа внутри объекта. В данной теме студентам предстоит разработать меры по организации внутриобъектового режима предприятия. Особое внимание будет уделено физической охране, контролю доступа и защите ИТ-инфраструктуры. В конце изучения темы студент будет уметь разрабатывать комплекс организационных мер по обеспечению безопасности.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование
22.	**Организация видеонаблюдения компании** Проектирование системы видеоконтроля для охраны. В данной теме студентам предстоит изучить вопросы проектирования системы видеонаблюдения для обеспечения охраны. Особое внимание будет уделено техническим требованиям, зонам наблюдения и вопросам хранения видеоданных. В конце изучения темы студент будет способен предложить проект видеонаблюдения для объекта.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	4	4	-	2	Собеседование
23.	**Организация пропускного режима** Создание системы учета и допуска сотрудников и посетителей. В данной теме студентам предстоит разработать систему пропускного режима на предприятии. Особое внимание будет уделено процедурам идентификации, регистрации и доступа сотрудников и посетителей. В конце изучения темы студент будет уметь создавать регламент пропускного режима.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-		Собеседование
24.	**Аудит информационной безопасности** Проверка соблюдения стандартов ИБ в компании. В данной теме студентам предстоит изучить методы и процедуры проведения аудита информационной безопасности. Особое внимание будет уделено планированию, сбору доказательств, оформлению результатов и рекомендациям. В конце изучения темы студент будет уметь проводить оценку соответствия системы ИБ стандартам.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование

25.	**Лицензирование деятельности в области защиты информации** Изучение порядка лицензирования и сертификации в ИБ. В данной теме студентам предстоит изучить процедуру лицензирования деятельности в сфере защиты информации. Особое внимание будет уделено требованиям к организациям, этапам получения лицензии и видам сертификаций. В конце изучения темы студент будет знать порядок получения разрешительных документов.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	4	4	-		Собеседование
26.	**Анализ требований ГОСТ Р 56939-2024** Изучение ключевого государственного стандарта по ИБ. В данной теме студентам предстоит провести анализ требований ГОСТ Р 56939-2024, который определяет ключевые положения обеспечения информационной безопасности. Особое внимание будет уделено структуре стандарта, его применению и обязательным требованиям. В конце изучения темы студент будет уметь использовать данный ГОСТ в практике ИБ.	ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5 ОПК-6 ИД-1ОПК-6 ИД-2ОПК-6 ИД-3ОПК-6	2	4	-	2	Собеседование
	ИТОГО за 9 семестр		**36**	**54**	**-**	**18**	
	ИТОГО		**68**	**102**	**-**	**46**	

6. Фонд оценочных средств по дисциплине

Фонд оценочных средств (ФОС) по дисциплине базируется на перечне осваиваемых компетенций с указанием индикаторов. ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций (включаются в методические указания по тем видам работ, которые предусмотрены учебным планом и предусматривают оценку сформированности компетенций);
- типовые оценочные средства, необходимые для оценки знаний, умений и уровня сформированности компетенций.

ФОС является приложением к данной программе дисциплины.

7. Методические указания для обучающихся по освоению дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения.

Дисциплина «Организационное и правовое обеспечение информационной безопасности» построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

Теоретический материал посвящен рассмотрению ключевых, базовых положений курсов и разъяснению учебных заданий, выносимых на самостоятельную работу студентов.

Практические работы направлены на приобретение опыта практической работы в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим и лабораторным занятиям, а также выполнения всех видов самостоятельной работы.

Для успешного освоения дисциплины, необходимо выполнить все виды самостоятельной работы, используя рекомендуемые источники информации.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

8.1.1. Перечень основной литературы:

1. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0.
2. Шибаев, Д. В. Организационно-правовое обеспечение информационной безопасности : учебное пособие / Д. В. Шибаев ; Северо-Западный институт (филиал) Университета имени О. Е. Кутафина (МГЮА). – Вологда : Северо-Западный ин-т (филиал) Ун-та им. О. Е. Кутафина (МГЮА), 2024. - 178 с.- Текст: электронный.
3. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности - Санкт-Петербург: НИУ ИТМО, 2014. - 173 с. - 100 экз.

8.1.2. Перечень дополнительной литературы:

1. Организационное и правовое обеспечение информационной безопасности : учебно-методическое пособие / Сибирский федеральный университет, Институт космических и информационных технологий ; сост. В. И. Вайнштейн [и др.]. -

Красноярск : СФУ, 2021 (2021-06-09). - 84 с., 4.0 усл. печ. л. : табл. - Библиогр.: с. 72-73. - 100 экз. - Изд. № 2021-13952
2. Пушкин, П. Ю. Организационно-правовое обеспечение информационной безопасности : учебно-методическое пособие / П. Ю. Пушкин, Д. А. Головченко, Е. О. Карамышева. — Москва : РТУ МИРЭА, 2023. — 32 с. — ISBN 978-5-7339-1916-4. — Текст : электронный // Лань : электронно-библиотечная система

8.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по выполнению практических работ по дисциплине " Организационное и правовое обеспечение информационной безопасности (электронный ресурс)

2. Методические указания по организации и проведению самостоятельной работы по дисциплине " Организационное и правовое обеспечение информационной безопасности " (электронный ресурс)

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

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Организационное и правовое обеспечение информационной безопасности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При чтении лекций используется компьютерная техника, демонстрации презентационных мультимедийных материалов. На практических занятиях студенты защищают отчеты по работам, которые они выполняют самостоятельно или в команде с применением компьютерной техники и Интернет-технологий

Информационные справочные системы:

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1	https://www.garant.ru/
2	http://www.consultant.ru/

Программное обеспечение:

1.	Альт Рабочая станция 10
2.	Альт Рабочая станция К
3.	Альт «Сервер»
4.	Пакет офисных программ - Р7-Офис

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

Лекционные занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.

Практические занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.
Самостоятельная работа	Помещение для самостоятельной работы обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и возможностью доступа к электронной информационно-образовательной среде университета

11. Особенности освоения дисциплины лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,
- специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),
- индивидуальное равномерное освещение не менее 300 люкс,
- при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;
- обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента задания могут выполняться в устной форме.

12. Особенности реализации дисциплины с применением дистанционных образовательных технологий и электронного обучения

Согласно части 1 статьи 16 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» под *электронным обучением* понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. Под *дистанционными образовательными технологиями* понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Реализация дисциплины может быть осуществлена с применением дистанционных образовательных технологий и электронного обучения полностью или частично. Компоненты УМК дисциплины (рабочая программа дисциплины, оценочные и методические материалы, формы аттестации), реализуемой с применением дистанционных образовательных технологий и электронного обучения, содержат указание на их использование.

При организации образовательной деятельности с применением дистанционных образовательных технологий и электронного обучения могут предусматриваться асинхронный и синхронный способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет».

При применении дистанционных образовательных технологий и электронного обучения в расписании по дисциплине указываются:

способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет» (ВКС-видеоконференцсвязь, ЭТ – электронное тестирование);

ссылки на электронную информационно-образовательную среду СКФУ, на образовательные платформы и ресурсы иных организаций, к которым предоставляется открытый доступ через информационно-телекоммуникационную сеть «Интернет»;

для синхронного обучения - время проведения онлайн-занятий и преподаватели;

для асинхронного обучения - авторы онлайн-курсов.

При организации промежуточной аттестации с применением дистанционных образовательных технологий и электронного обучения используются Методические рекомендации по применению технических средств, обеспечивающих объективность результатов при проведении промежуточной и государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры с применением дистанционных образовательных технологий (Письмо Минобрнауки России от 07.12.2020 г. № МН-19/1573-АН "О направлении методических рекомендаций").

Реализация дисциплины с применением электронного обучения и дистанционных образовательных технологий осуществляется с использованием электронной информационно-образовательной среды СКФУ, к которой обеспечен доступ обучающихся через информационно-телекоммуникационную сеть «Интернет», или с использованием ресурсов иных организаций, в том числе платформ, предоставляющих сервисы для проведения видеоконференций, онлайн-встреч и дистанционного обучения (МТС-Линк), а также с использованием возможностей социальных сетей для осуществления коммуникации обучающихся и преподавателей.

Учебно-методическое обеспечение дисциплины, реализуемой с применением электронного обучения и дистанционных образовательных технологий, включает представленные в электронном виде рабочую программу, учебно-методические пособия или курс лекций, методические указания к выполнению различных видов учебной

деятельности обучающихся, предусмотренных дисциплиной, и прочие учебно-методические материалы, размещенные в информационно-образовательной среде СКФУ.