Аннотация к рабочей программе дисциплины «Организационное и правовое обеспечение информационной безопасности»

Цель преподавания дисциплины

Формирование у студентов знаний в области организационного и правового обеспечения информационной безопасности.

Задачи изучения дисциплины

- изучение основ организационно-правового обеспечения информационной безопасности;
- изучение российского законодательства в области информационной безопасности;
- изучение организационных методов и мероприятий защиты информации.

Индикаторы клмпетенций, формируемые в результате освоения дисциплины

УК-10.1 - Анализирует правовые последствия коррупционной деятельности, в том числе собственных действий или бездействий;

ОПК-5.1 разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;

ОПК-5.2 формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;

ОПК-5.3 формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации;

ОПК-6.1; разрабатывает модели угроз и модели нарушителя объекта информатизации;

ОПК-6.4; разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации;

ОПК-8.1 составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов;

ОПК-8.2 систематизирует научную информацию в области информационной безопасности;

ОПК-8.3 использует информационно-справочные системы при поиске информации в области профессиональной деятельности;

ОПК-4.1.2 Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе;

ОПК-4.1.3 Организует работу персонала автоматизированной системы с учетом требований по защите информации;

ОПК-4.1.4 Готовит документы, определяющие правила и процедуры,

реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.

Разделы дисциплины

Информационная безопасность в системе национальной безопасности России. Информация, информационные системы как объект правового регулирования информационной безопасности. Правовая основа допуска и доступа персонала к защищаемым сведениям. Правовые проблемы, связанные с защитой прав обладателей собственности на информацию и распоряжением информацией. Правовые основы защиты коммерческой тайны. Компьютерная информация – как объект информатизации. Лицензирование в области защиты информации. Сертификация в области защиты информации. Система правовой ответственности за утечку информации и утрату носителей информации. Правовые основы деятельности подразделений защиты информации. Правовые основы защиты личной тайны. Правовые основы защиты персональных данных.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)

_____М.О. Таныгин
(подпись, инициалы, фамилия)

«30» июня 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организационное и правовое обеспечение информационной безопасности

(наименование дисциплины)

ОПОП ВО 10.03.01 Информационная безопасность
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий)»
наименование направленности (профиля, специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета (протокол № 7 «28» февраля 2022 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий» на заседании кафедры информационной безопасности №11 «30» 06 2022 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы _____ Кулешова Е.А.

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол №___«__»_____20___г., на заседании кафедры_____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол №___«__»_____20___г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1. Цель и задачи дисциплины, планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения основной профессиональной образовательной программы

1.1. Цель дисциплины

Формирование у студентов знаний в области организационного и правового обеспечения информационной безопасности.

1.2. Задачи дисциплины

- изучение основ организационно-правового обеспечения информационной безопасности;
- изучение российского законодательства в области информационной безопасности;
- изучение организационных методов и мероприятий защиты информации.

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательный программы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1 Анализирует правовые последствия коррупционной деятельности, в том числе собственных действий или бездействий	***Знать:*** Основные термины и понятия гражданского права, используемые антикоррупционном законодательстве, действующее антикоррупционное законодательство и практику его применения ***Уметь:*** Правильно толковать гражданско-правовые термины, используемые антикоррупционном законодательстве; давать оценку коррупционному поведению и применять практике антикоррупционное законодательство. ***Владеть (****или* ***Иметь опыт деятельности):*** Навыками правильного толкования гражданско-правовых терминов, используемых в

			антикоррупционном законодательстве, а так же навыками применения на практике антикоррупционного законодательства, правовой квалификацией коррупционного поведения и его пресечения.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1 разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	***Знать:*** Правовые основы организации защиты конфиденциальной информации, задачи органов защиты информации; ***Уметь:*** применять действующую законодательную базу в области обеспечения информационной безопасности; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации ***Владеть (или Иметь опыт деятельности):*** навыками работы с нормативными правовыми актами; навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.
		ОПК-5.2 формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	***Знать:*** Правовые нормы и стандарты по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; принципы формирования политики информационной безопасности в автоматизированных системах ***Уметь:*** применять действующую законодательную базу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; разрабатывать проекты локальных правовых актов, инструкций,

			регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации ***Владеть (или Иметь опыт деятельности):*** навыками работы с нормативными правовыми актами; навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.
		ОПК-5.3 формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	***Знать:*** Правовые нормы и стандарты по лицензированию в области обеспечения защиты информации и сертификации средств защиты; основные отечественные и зарубежные стандарты в области информационной безопасности; терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем. ***Уметь:*** применять действующую законодательную базу в области обеспечения информационной безопасности при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; разрабатывать проекты локальных правовых актов, инструкций, регламентов при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации. ***Владеть (или Иметь опыт деятельности):*** навыками работы с нормативными правовыми актами; навыками работы с технической документацией на ЭВМ и вычислительные системы; навыками работы с технической документацией на компоненты автоматизированных

			систем на русском и иностранном языках.
ОПК-6.	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1; разрабатывает модели угроз и модели нарушителя объекта информатизации	***Знать*** основные угрозы безопасности и модели нарушителя объекта информатизации ***Уметь:*** разрабатывать модели угроз и модели нарушителя объекта информатизации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки угроз для объекта информатизации
		ОПК-6.4; разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	***Знать*** правовые нормы и стандарты для разработки инструкций, регламентов, положений и приказов, регламентирующих защиту информации ***Уметь:*** составлять проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками организации документооборота в области защиты информации.
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1 составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов	***Знать:*** структуру, особенности, методы и средства составления рефератов по результатам обзора научно-технической литературы, нормативных и методических документов ***Уметь:*** составлять рефераты по результатам обзора научно-технической литературы, нормативных и методических документов ***Владеть (****или* ***Иметь опыт деятельности):*** навыками реферирования научно-технической литературы, нормативных и методических документов.
		ОПК-8.2 систематизирует научную информацию в области информационной безопасности	***Знать:*** методы систематизации информации; принципы поиска научной информации в области информационной безопасности; критерии группировки. ***Уметь:*** группировать научную информацию по определенным признакам. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с системами поиска и систематизации

			научной информации.
		ОПК-8.3 использует информационно-справочные системы при поиске информации в области профессиональной деятельности	***Знать*** основные функции и возможности информационно-справочных систем. ***Уметь:*** формулировать запросы к информационно-справочной системе ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с информационно-справочными системами при поиске информации в области защиты информации.
ОПК - 4.1.	Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.2 Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	***Знать*** организационные основы информационной безопасности ***Уметь:*** анализировать и оценивать угрозы информационной безопасности объекта ***Владеть:*** навыками оценки состояния организационной защиты информации на объекте и разработки рациональных мер по обеспечению организационной защиты
		ОПК-4.1.3 Организует работу персонала автоматизированной системы с учетом требований по защите информации	***Знать*** основные нормативно-правовые акты в области информационной безопасности и защиты информации. ***Уметь:*** формулировать задачи для организации работы персонала автоматизированной системы; оценивать итоги исполнения поставленных задач перед персоналом. ***Владеть (****или* ***Иметь опыт деятельности):*** организационно-управленческой работы.
		ОПК-4.1.4 Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	***Знать*** основные требования по защите информационной системы. ***Уметь:*** определять правила и процедуры, реализуемые оператором, для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками разработки организационно-распорядительной документации по защите информации.

2. Указание места дисциплины в структуре образовательной программы

Дисциплина «Организационное и правовое обеспечение информационной безопасности» входит в обязательную часть блока 1 «Дисциплины (модули»)) основной профессиональной образовательной программы – программы бакалавриата 10.03.01 Информационная безопасность профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий». Дисциплина изучается на 3 курсе в 5 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 4 зачётных единиц (з.е.), 144 академических часов.

Таблица 3 – Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	72
в том числе:	
лекции	36
лабораторные занятия	0
практические занятия	36
Самостоятельная работа обучающихся (всего)	43,85
Контроль (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрен
экзамен (включая консультацию перед экзаменом)	1,15

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Информационная безопасность в системе национальной безопасности России	Место информационной безопасности в системе. национальной безопасности России. Понятие, структура и содержание правового обеспечения защиты информации. Правовые основы защиты государственной, служебной, профессиональной тайны, персональных данных
2	Информация, информационные системы как объект правового регулирования информационной безопасности	Информация и информационные системы как объект правоотношений в сфере обеспечения информационной безопасности. Понятие и виды защищаемой информации по законодательству Российской Федерации. Анализ и оценка угроз информационной безопасности объекта. Оценка ущерба.
3	Правовая основа допуска и доступа персонала к защищаемым сведениям	Понятие о доступе к государственным информационным ресурсам. Правовая защита информации и информационных ресурсов. Правовые режимы конфиденциальной информации. Правовая защита государственных информационных ресурсов. Система защиты государственной тайны.
4	Правовые проблемы, связанные с защитой прав обладателей собственности на информацию и распоряжением информацией	Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты. Основы авторского права. Основные положения патентного права. Законодательство о ноу-хау.
5	Правовые основы защиты коммерческой тайны	Понятие коммерческой тайны как правовой категории. Определение сведений, составляющих коммерческую тайну. Объекты защиты коммерческой тайны. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации
6	Компьютерная информация – как объект информатизации	Понятие и классификация видов компьютерных правонарушений. Криминалистические характеристики компьютерных преступлений. Криминалистические аспекты проведения расследования преступлений в сфере компьютерной информации. Особенности проведения экспертизы в области компьютерной информации.
7	Лицензирование в области защиты информации	Основные понятия и организационная структура системы государственного лицензирования. Порядок лицензирования. Проведение специальной экспертизы предприятия. Порядок приостановления или аннулирования действия лицензии
8	Сертификация в области защиты информации	Система сертификации средств защиты информации. Особенности сертификации средств защиты информации по требованиям безопасности
9	Система правовой ответственности за утечку информации и утрату носителей информации	Понятие, виды норм и условия применения юридической ответственности за нарушение правовых норм в области защиты информации. Уголовная ответственность за нарушение правовых норм в сфере защищаемой информации. Административная ответственность за нарушения правовых норм в сфере защищаемой

		информации. Особенности юридической ответственности за нарушение норм информационной безопасности в области трудовых и гражданскоправовых отношений
10	Правовые основы деятельности подразделений защиты информации	Правовая регламентация охранной деятельности. Служба безопасности объекта. Формы, средства и методы защиты объекта. Организация и обеспечение режима секретности. Организация пропускного и внутриобъектового режима
11	Правовые основы защиты личной тайны	Конституционные гарантии прав граждан на информацию и механизм их регулирования. Концепция правовой информатизации как инструмент правового регулирования информационной безопасности личности, общества и государства
12	Правовые основы защиты персональных данных	Понятие и виды персональных данных. Государственное регулирование и правовой режим персональных данных3. Права и обязанности субъектов в области защиты персональных данных. Классификация информационных систем персональных данных. Принципы и особенности обработки персональных данных. Требования по обеспечению безопасности персональных данных. Ответственность за нарушение законодательства в области персональных данных

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра)	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Информационная безопасность в системе национальной безопасности России	3	-		У-1-5 МУ-2	УО - 1	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1
2	Информация, информационные системы как объект правового регулирования информационной безопасности	3	-	1,2	У-1-5 МУ- 1,2	УО, ЗПР – 2-3	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1
3	Правовая основа допуска и доступа персонала к защищаемым сведениям	3	-		У-1-5 МУ-2	УО - 4	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1
4	Правовые проблемы,	3	-		У-1-5	УО, ЗПР – 5-	УК-10

	связанные с защитой прав обладателей собственности на информацию и распоряжением информацией			3,4	МУ- 1,2	6	ОПК-5 ОПК-6 ОПК-8 ОПК-4.1
5	Правовые основы защиты коммерческой тайны	3	-		У-1-5 МУ-2	УО - 7	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1
6	Компьютерная информация – как объект информатизации	3	-	5,6	У-1-5 МУ- 1,2	УО, ЗПР – 8-9	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1
7	Лицензирование в области защиты информации	3	-		У-1-5 МУ-2	УО - 10	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1
8	Сертификация в области защиты информации	3	-	7	У-1-5 МУ- 1,2	УО, ЗПР – 11-12	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1
9	Система правовой ответственности за утечку информации и утрату носителей информации	3	-		У-1-5 МУ-2	УО - 13	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1
10	Правовые основы деятельности подразделений защиты информации	3	-		У-1-5 МУ-2	УО – 14	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1
11	Правовые основы защиты личной тайны	3	-	8	У-1-5 МУ- 1,2	УО, ЗПР – 15-17	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1
12	Правовые основы защиты персональных данных	3	-		У-1-5 МУ-2	УО –18	УК-10 ОПК-5 ОПК-6 ОПК-8

							ОПК-4.1
	Итого	36	-	-			

УО – устный опрос, ЗПР – защита практической работы.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 – Практические занятия

№	Наименование практического занятия	Объем, час.
1	2	3
1	Организационно-правовые механизмы обеспечения информационной безопасности	4
2	Технические средства защиты информации	4
3	Защита персональных данных	4
4	Разработка организационно-распорядительной документации для объекта информатизации	4
5	Анализ эффективности применения средств защиты информации на объекте информатизации	4
6	Организация внутриобъектового режима	4
7	Организация пропускного режима	6
8	Разработка модели угроз информационной безопасности	6
	Итого	36

4.3 Самостоятельная работы студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Информационная безопасность в системе национальной безопасности России	1 неделя	3
2	Информация, информационные системы как объект правового регулирования информационной безопасности	2-3 недели	4
3	Правовая основа допуска и доступа персонала к защищаемым сведениям	4 неделя	3
4	Правовые проблемы, связанные с защитой прав обладателей собственности на информацию и распоряжением информацией	5-6 недели	4
5	Правовые основы защиты коммерческой тайны	7 неделя	3
6	Компьютерная информация – как объект информатизации	8-9 недели	4
7	Лицензирование в области защиты информации	10 неделя	3
8	Сертификация в области защиты информации	11-12 недели	4

9	Система правовой ответственности за утечку информации и утрату носителей информации	13 неделя	4
10	Правовые основы деятельности подразделений защиты информации	14 неделя	4
11	Правовые основы защиты личной тайны	15-17 недели	4
12	Правовые основы защиты персональных данных	18 неделя	3,85
	Итого		43,85

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

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;

– вопросов к экзамену;

–методических указаний к выполнению практических работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных и общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
1	Организационно-правовые механизмы обеспечения информационной безопасности (практическое занятие)	Разбор конкретных ситуаций	4
4	Разработка организационно-распорядительной документации для объекта информатизации (практическое занятие)	Разбор конкретных ситуаций	4
Итого			8

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики,

культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

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

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модуле), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
Способен формировать нетерпимое отношение к коррупционному поведению (УК-10)	Правоведение	Организационное и правовое обеспечение информационной безопасности	
Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности (ОПК-5)	Организационное и правовое обеспечение информационной безопасности.		Производственная эксплуатационная практика. Основы управления информационной безопасностью.
Способен при решении профессиональных задач	Организационное и правовое обеспечение информационной		Основы управления информационной

организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ОПК – 6);	безопасности	безопасностью.
Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности (ОПК-8)	Учебная ознакомительная практика	Организационное и правовое обеспечение информационной безопасности
Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах (ОПК-4.1.)	Организационное и правовое обеспечение информационной безопасности	Основы управления информационной безопасностью

7.2 Описание показателей и критериев оценивания компетенций на различных этапах формирования, описание шкал оценивания

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
УК-10/ основной	УК-10.1 Анализирует правовые последствия коррупционной деятельности, в том числе собственных действий или бездействий	Знать: Основные термины и понятия гражданского права, используемые антикоррупционном законодательстве, Уметь: Правильно толковать гражданско-правовые	Знать: Основные термины и понятия гражданского права, используемые антикоррупционном законодательстве, Уметь: Правильно толковать гражданско-правовые	Знать: Основные термины и понятия гражданского права, используемые антикоррупционном законодательстве, действующее антикоррупционное законодательство и практику его применения Уметь: Правильно толковать

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		термины, используемые антикоррупционном законодательстве.	термины, используемые антикоррупционном законодательстве. Владеть (или Иметь опыт деятельности): Навыками правильного толкования гражданско-правовых терминов, используемых в антикоррупционном законодательстве.	гражданско-правовые термины, используемые антикоррупционном законодательстве; давать оценку коррупционному поведению и применять практике антикоррупционное законодательство. Владеть (или Иметь опыт деятельности): Навыками правильного толкования гражданско-правовых терминов, используемых в антикоррупционном законодательстве, а так же навыками применения на практике антикоррупционного законодательства, правовой квалификацией коррупционного поведения и его пресечения.
ОПК-5/ основной	ОПК-5.1 Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационн	Знать: -стандарты в области информационной безопасности; Уметь: - сопоставлять характеристики правового	Знать: - методологические подходы применения нормативных документов при оценке защищённости	Знать: - принципы формирования комплексных отчётов по аудиту информационной безопасности; Уметь: - вырабатывать

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	о-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	обеспечения действующим стандартам, Владеть: - комплексной оценкой защищённости систем документооборота	правового обеспечения; Уметь: - выявлять не декларируемые угрозы; Владеть: - способностью к критическому анализу используемых методов аудита информационной безопасности	методические рекомендации по формированию политик безопасности; Владеть: -организационными формами и методами проведения научных исследований
	ОПК-5.2 Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	Знать: - основные нормативные правовые документы. Уметь: - ориентироваться в системе законодательства и нормативных правовых актов в области защиты информации. Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в профессиональной деятельности	Знать: - нормативно правовые документы. Уметь: - использовать нормативно правовые акты в задачах защиты информации Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками анализа результатов их применения.	Знать: - Российские и международные нормативно правовые документы в области защиты информации. Уметь: - разрабатывать рекомендации по применению нормативно правовых документов в области защиты информации. Владеть: - навыками разработки организационно-распорядительной документации на объекте информатизации

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	ОПК-5.3 Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	Знать: - основные нормативные правовые документы. Уметь: - ориентироваться в системе законодательства и нормативных правовых актов в области защиты информации. Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в профессиональной деятельности	Знать: - нормативно правовые документы. Уметь: - использовать нормативно правовые акты в задачах защиты информации Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками анализа результатов их применения.	Знать: - Российские и международные нормативно правовые документы в области защиты информации. Уметь: - разрабатывать рекомендации по применению нормативно правовых документов в области защиты информации. Владеть: - навыками разработки организационно-распорядительной документации на объекте информатизации
ОПК – 6/ основной	ОПК – 6.1 Разрабатывает модели угроз и модели нарушителя объекта информатизации	Знать: - основные нормативные правовые документы по разработке модели нарушителя и угроз. Уметь: - ориентироваться в системе законодательства и нормативных правовых актов в	Знать: - нормативно правовые документы. Уметь: - использовать нормативно правовые акты при разработке моделей угроз и нарушителей. Владеть: - навыками поиска необходимых	Знать: - Российские и международные нормативно правовые документы в области защиты информации. Уметь: - разрабатывать модели угроз и модели нарушителя объекта информатизации. Владеть: - навыками анализа

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		области защиты информации. Владеть: - навыками поиска необходимых нормативных и законодательных документов для разработки модели угроз и нарушителя	нормативных и законодательных документов и навыками анализа результатов их применения.	защищенности модели угроз и нарушителей.
	ОПК-6.4 Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	Знать: - основные нормативные правовые документы по разработке инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации. Уметь: - ориентироваться в системе законодательства и нормативных правовых актов в области защиты информации. Владеть: - навыками поиска необходимых	Знать: - нормативно правовые документы по разработке инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации. Уметь: - использовать нормативно правовые акты при разработке инструкций, регламентов, положений и приказов. Владеть: - навыками поиска необходимых	Знать: - Российские и международные нормативно правовые документы в области защиты информации. Уметь: - разрабатывать инструкции, регламенты, положения и приказы, регламентирующие защиту информации ограниченного доступа в организации. Владеть: - навыками анализа уязвимостей инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		нормативных и законодательных документов для разработки инструкций, регламентов, положений и приказов.	нормативных и законодательных документов и навыками анализа результатов их применения.	доступа в организации.
ОПК-8/ основной	ОПК-8.1 Составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов	***Знать:*** структуру, особенности, составления рефератов по результатам обзора научно-технической литературы, нормативных и методических документов ***Уметь:*** составлять рефераты по результатам обзора научно-технической литературы, нормативных и методических документов ***Владеть (****или* ***Иметь опыт деятельности):*** навыками реферирования научно-технической литературы, нормативных и методических	***Знать:*** структуру, особенности и методы составления рефератов по результатам обзора научно-технической литературы, нормативных и методических документов ***Уметь:*** составлять рефераты по результатам обзора научно-технической литературы, нормативных и методических документов ***Владеть (****или* ***Иметь опыт деятельности):*** навыками реферирования научно-технической литературы, нормативных и	***Знать:*** структуру, особенности, методы и средства составления рефератов по результатам обзора научно-технической литературы, нормативных и методических документов ***Уметь:*** составлять рефераты по результатам обзора научно-технической литературы, нормативных и методических документов ***Владеть (****или* ***Иметь опыт деятельности):*** навыками реферирования научно-технической литературы, нормативных и методических документов.

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		документов.	методических документов.	
	ОПК-8.2 Систематизирует научную информацию в области информационной безопасности	***Знать:*** основы систематизации информации; принципы поиска научной информации в области информационной безопасности; критерии группировки. ***Уметь:*** группировать научную информацию по определенным шаблонам. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с системами поиска и систематизации научной информации.	***Знать:*** методы систематизации информации; принципы поиска научной информации в области информационной безопасности; критерии группировки. ***Уметь:*** группировать научную информацию по определенным шаблонам. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с системами поиска и систематизации научной информации.	***Знать:*** методы систематизации информации; принципы поиска научной информации в области информационной безопасности; критерии группировки. ***Уметь:*** группировать научную информацию по определенным признакам. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с системами поиска и систематизации научной информации.
	ОПК-8.3 Использует информационно-справочные системы при поиске информации в области профессиональной деятельности	***Знать*** основные функции и возможности информационно-справочных систем. ***Уметь:*** формулировать запросы к информационно-справочной системе	***Знать*** расширенный список функций и возможностей информационно-справочных систем. ***Уметь:*** формулировать запросы к информационно-справочной	***Знать*** расширенный список функций и возможностей информационно-справочных систем. ***Уметь:*** создавать сложные запросы к информационно-справочной системе ***Владеть (****или* ***Иметь опыт***

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		Владеть (*или* ***Иметь опыт деятельности):*** навыками работы с информационно-справочными системами при поиске информации в области защиты информации.	системе ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с информационно-справочными системами при поиске информации в области защиты информации.	***деятельности):*** навыками работы с информационно-справочными системами при поиске информации в области защиты информации.
ОПК-4.1/основной	ОПК-4.1.2 Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	***Знать*** организационные основы информационной безопасности; основы составления комплексов правил, процедур, практических приемов, принципов и методов обеспечения защиты информации в автоматизированной системе составления ***Уметь:*** формулировать основные требования для составления правил, процедур, практических приемов,	***Знать*** организационные мероприятия информационной безопасности; методы составления комплексов правил, процедур, практических приемов, принципов и методов обеспечения защиты информации в автоматизированной системе составления ***Уметь:*** формулировать основные требования для составления правил, процедур, практических приемов,	***Знать*** организационные мероприятия информационной безопасности; методы составления комплексов правил, процедур, практических приемов, принципов и методов обеспечения защиты информации в автоматизированной системе составления ***Уметь:*** формулировать требования для составления правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		принципов и методов, средств обеспечения защиты информации в автоматизированной системе ***Владеть:*** навыками конфиденциального документооборота, разработки организационно-распорядительной документации	принципов и методов, средств обеспечения защиты информации в автоматизированной системе ***Владеть:*** навыками конфиденциального документооборота, разработки организационно-распорядительной документации	***Владеть:*** навыками конфиденциального документооборота, разработки организационно-распорядительной документации, навыками анализа правильности разработанной документации
	ОПК-4.1.3 Организует работу персонала автоматизированной системы с учетом требований по защите информации.	***Знать*** основные принципы организации работы персонала автоматизированной системы с учетом требований по защите информации. ***Уметь:*** формулировать задачи для организации работы персонала автоматизированной системы; ***Владеть (или Иметь опыт деятельности):*** организационно-управленческой работы.	***Знать*** нормативно-правовые акты в области информационной безопасности и защиты информации. принципы организации работы персонала автоматизированной системы с учетом требований по защите информации. ***Уметь:*** формулировать задачи для организации работы персонала автоматизированной системы;	***Знать*** нормативно-правовые акты в области информационной безопасности и защиты информации РФ и др. стран. принципы организации работы персонала автоматизированной системы с учетом требований по защите информации. ***Уметь:*** формулировать задачи для организации работы персонала автоматизированной системы; оценивать итоги исполнения поставленных задач перед персоналом.

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
			Владеть (*или* ***Иметь опыт деятельности):*** организационно-управленческой работы.	***Владеть (****или* ***Иметь опыт деятельности):*** организационно-управленческой работы.
	ОПК-4.1.4 Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.	***Знать*** основные требования по защите информационной системы. ***Уметь:*** определять правила и процедуры, реализуемые оператором, для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками разработки организационно-распорядительной документации по защите информации.	***Знать*** основные требования по защите информационной системы. Методы контроля исполнения правил и процедур для обеспечения защиты информации. ***Уметь:*** определять правила и процедуры, реализуемые оператором, для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками разработки организационно-распорядительной документации по защите информации.	***Знать*** основные требования по защите информационной системы. Методы контроля исполнения правил и процедур для обеспечения защиты информации. ***Уметь:*** определять правила и процедуры, реализуемые оператором, для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками разработки организационно-распорядительной документации по защите информации; навыками экспертизы документации, определяющие правила и

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
				процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1	Информационная безопасность в системе национальной безопасности России	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1	Лекция СРС	Вопросы для УО	1-11	Согласно табл. 7.2
2	Информация, информационные системы как объект правового регулирования информационной безопасности	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1	Лекция СРС Практическое занятие	Вопросы для УО КВЗПР	1-12 1-5	Согласно табл. 7.2
3	Правовая основа допуска и доступа персонала к	УК-10 ОПК-5	Лекция СРС	Вопросы для УО	1-11	Согласно табл. 7.2

	защищаемым сведениям	ОПК-6 ОПК-8 ОПК-4.1				
4	Правовые проблемы, связанные с защитой прав обладателей собственности на информацию и распоряжением информацией	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1	Лекция СРС Практическое занятие	Вопросы для УО КВЗПР	1-13 1-10	Согласно табл. 7.2
5	Правовые основы защиты коммерческой тайны	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1	Лекция СРС	Вопросы для УО	1-12	Согласно табл. 7.2
6	Компьютерная информация – как объект информатизации	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1	Лекция СРС Практическое занятие	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл. 7.2
7	Лицензирование в области защиты информации	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1	Лекция СРС	Вопросы для УО	1-10	Согласно табл. 7.2
8	Сертификация в области защиты информации	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1	Лекция СРС Практическое занятие	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл. 7.2
9	Система правовой ответственности за утечку информации и утрату носителей информации	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1	Лекция СРС	Вопросы для УО	1-10	Согласно табл. 7.2
10	Правовые основы деятельности подразделений защиты информации	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1	Лекция СРС	Вопросы для УО	1-10	Согласно табл. 7.2
11	Правовые основы защиты личной тайны	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1	Лекция СРС Практическое занятие	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл. 7.2

12	Правовые основы защиты персональных данных	УК-10 ОПК-5 ОПК-6 ОПК-8 ОПК-4.1	Лекция СРС	Вопросы для УО	1-10	Согласно табл. 7.2

КВЗПР – контрольные вопросы к защите практических работ

Примеры типовых контрольных заданий для текущего контроля

Вопросы для устного опроса по теме 1 «Информационная безопасность в системе национальной безопасности России»

1. Какие качественные изменения в военно-политической и научно-технической сфере обусловливают государственную политику в национальной безопасности страны?
2. Раскрыть содержание задач обеспечения информационной безопасности страны.
3. Дать определение понятия информационной безопасности России.
4. Каково содержание методов правовой защиты информации.
5. Какие отрасли права регулируют отношения в сфере защиты информации?

Контрольные вопросы для защиты практической работы 1 «Организационные источники и каналы утечки информации»

1) Понятие, проблемы и структура экономической безопасность предпринимательской деятельности.

2) Классификация информационных ресурсов ограниченного доступа к ним персонала фирмы, характеристика каждой группы.

3) Информационная безопасность, история формирования.

Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Типовые задания для промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Что включают в себя системы управления ИБ?

A. Политика, планирование, должностные обязанности, процедуры, процессы и ресурсы.

B. Организационную структуру, политики, планирование, должностные обязанности, практики,

C. Организационную структуру, политики, планирование, должностные обязанности, практики.

D. Организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.

E. Организационную структуру, политики, должностные обязанности, практики, процессы и ресурсы.

Задание в открытой форме:

1. Основными принципами политики безопасности являются…
2. Политика безопасности верхнего уровня включает…
3. Удаленный доступ к сервису организован…

Задание на установление правильной последовательности.

Установить действия этапа анализа рисков:

1. Оценка вероятности того, что угроза будет реализована на практике
2. Оценка рисков технологических и информационных активов
3. Идентификация и оценка стоимости технологических и информационных активов
4. Анализ угроз, для которых технологические и информационные активы являются целевым объектом

Задание на установление соответствия:

Установить соответствие типа организации его характеристике:

1) Аттестация	a) Проверка, выполняемая компетентным органом (лицом) с целью обеспечения независимой оценки степени соответствия программных продуктов или процессов установленным требованиям
2) Аудит	b) Объединение нескольких рисков в один риск, направленное на более глубокое понимание совокупного риска
3) Аккредитация	c) Официальное признание правомочий осуществлять какую-либо деятельность
	d) Подтверждение экспертизой и представлением объективных доказательств того, что конкретные требования к конкретным объектам полностью реализован

Компетентностно-ориентированная задача:

В Курской области создается Комитет Курской области по контролю успеваемости учащихся образовательных организациях Курской области (выделяется часть функций из комитета образования и науки).

В рамках комитета создается автоматизированная система внутренней работы. Необходимо подготовить частную модель угроз персональным данным, исходя из «Базовой модели угроз персональным данным ФСТЭК».

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016–2018 Обалльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно - рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Практическая работа №1 (Организационно-правовые механизмы обеспечения информационной безопасности)	2	Выполнил, доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Практическая работа №2 (Технические средства защиты информации)	2	Выполнил, доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Практическая работа №3 (Защита персональных данных)	2	Выполнил, доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Практическая работа №4 (Разработка организационно-распорядительной документации для объекта информатизации)	2	Выполнил, доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Практическая работа №5 (Анализ эффективности применения средств защиты информации на объекте информатизации)	2	Выполнил, доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Практическая работа №6 Организация внутриобъектового режима	2	Выполнил, доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Практическая работа №7 Организация пропускного режима	2	Выполнил, доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%

Практическая работа №8 Разработка модели угроз информационной безопасности	2	Выполнил, доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по темам 1-12	8	Доля правильных ответов от 50% до 90%	16	Доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

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

8.1 Основная учебная литература

1. Корнилова, А. А. Защита персональных данных : учебное пособие : [16+] / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2020. – 119 с. : ил., табл. – Режим доступа:– URL: https://biblioclub.ru/index.php?page=book&id=611314 . – Библиогр. в кн. – Текст : электронный.

2. Информационная безопасность в цифровом обществе : учебное пособие : [16+] / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. : табл., ил. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=611084. – Библиогр. в кн. – Текст : электронный.

3. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=576726. – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный.

4. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие : [16+] / А. Б. Арзуманян ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 140 с. – Режим доступа:– URL: https://biblioclub.ru/index.php?page=book&id=612162. – Библиогр.: с. 129-133. – ISBN 978-5-9275-3546-0. – Текст : электронный.

5. Информационная безопасность в цифровом обществе : учебное пособие : [16+] / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. : табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=611084 (дата обращения: 17.09.2021). – Библиогр. в кн. – Текст : электронный.

8.2 Дополнительная учебная литература

6. Спеваков А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Текст : непосредственный. Ч. 1. - 150 с. : ил., табл. - Имеется электрон. аналог. - Библиогр.: с. 137-149. - ISBN 978-5-7681-08 57-1

7. Спеваков А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Текст : непосредственный. Ч. 2. - 303 с. : ил., табл. - Библиогр.: с. 290-302. - Имеется электрон. аналог. - ISBN 978-5-7681-08 58-8

8.3 Перечень методических указаний

1. Организационно-правовое обеспечение информации [Текст] : методические рекомендации по выполнению практических работ/ Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. – Курск, 2022. – 14 с. – Библиогр.: с.13.

2. Организационно-правовое обеспечение информационной безопасности [Текст] : методические рекомендации по выполнению самостоятельных работ/ Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. – Курск, 2022. – 19 с. – Библиогр.: с.19.

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

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Организационное и правовое обеспечение информационной безопасности» являются лекции и практические занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования и результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Организационное и правовое обеспечение информационной безопасности»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Организационное и правовое обеспечение информационной безопасности» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Организационное и правовое обеспечение информационной безопасности» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

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

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Проекционный экран на штативе; Мультимедиацентр: ноут-букASUSX50VLPMD-T2330/14"/1024Mb/ 160Gb/сумка/проектор inFocusIN24+

13. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	изменённых	заменённых	аннулированных	новых			