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

Цель преподавания дисциплины

Дисциплина «Организационное и правовое обеспечение информационной безопасности» изучается с целью формирования 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 компетенций, формируемые в результате освоения дисциплины

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-5.4 Формулирует основные требования информационной безопасности при эксплуатации телекоммуникационной системы

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

ОПК-6.2 формулирует основные требования, предъявляемые к организации защиты информации ограниченного доступа

ОПК-6.3 анализирует состав и функциональные возможности средств защиты информации телекоммуникационной системы в целях его совершенствования

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

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 10.05.02 Информационная безопасность
(шифр согласно ФГОС и наименование направления подготовки (специальности))
телекоммуникационных систем

направленность (профиль, специализация) «Управление безопасностью
наименование направленности (профиля, специализации)
телекоммуникационных систем и сетей»

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

Курск – 2022

Рабочая программа дисциплины составлена в соответствии составлена в соответствии с ФГОС ВО – специалитет по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, направленность Управление безопасностью телекоммуникационных систем и сетей, 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 10.05.02 Информационная безопасность телекоммуникационных систем, направленность Управление безопасностью телекоммуникационных систем и сетей на заседании кафедры информационной безопасности Протокол № 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 10.05.02 Информационная безопасность телекоммуникационных систем, направленность Управление безопасностью телекоммуникационных систем и сетей, 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 10.05.02 Информационная безопасность телекоммуникационных систем, направленность Управление безопасностью телекоммуникационных систем и сетей, одобренного Ученым советом университета Протокол № « » _____ 20 г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1. Цель дисциплины

Дисциплина «Организационное и правовое обеспечение информационной безопасности» изучается с целью формирования 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 образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

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*		
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	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	***Знать:*** Правовые нормы и стандарты по лицензированию в области обеспечения защиты информации и сертификации средств защиты; основные отечественные и зарубежные

		деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	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-5.4 Формулирует основные требования информационной безопасности при эксплуатации телекоммуникационной системы	***Знать:*** Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. ***Уметь:*** применять действующую законодательную базу по защите конфиденциальной информации, при эксплуатации телекоммуникационной системы ***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 при эксплуатации телекоммуникационной системы

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-6.2 формулирует основные требования, предъявляемые к организации защиты информации ограниченного доступа	***Знать*** основные требования, предъявляемые к организации защиты информации ограниченного доступа угрозы безопасности и модели нарушителя объекта информатизации ***Уметь:*** разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа ***Владеть (или Иметь опыт деятельности):*** навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа
		ОПК-6.3 анализирует состав и функциональные возможности средств защиты информации телекоммуникационной системы в целях его совершенствования	***Знать*** состав и функциональные возможности средств защиты информации телекоммуникационной системы. ***Уметь:*** совершенствовать состав и функциональные возможности средств защиты информации телекоммуникационной системы ***Владеть (или Иметь опыт деятельности):*** навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы
		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.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Организационное и правовое обеспечение информационной безопасности», входит в обязательную часть блока 1 «Дисциплины (модули») основной профессиональной образовательной программы – программы специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, направленность «Управление безопасностью телекоммуникационных систем и сетей». 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 единицы (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)	34.85
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	1.15
в том числе:	
зачет	1.15
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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, темы 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	ОПК-5 ОПК-6
2	Информация, информационные системы как объект правового регулирования информационной безопасности	3	-	1,2	У-1-5 МУ- 1,2	УО, ЗПР – 2-3	ОПК-5 ОПК-6
3	Правовая основа допуска и доступа персонала к	3	-		У-1-5 МУ-2	УО - 4	ОПК-5 ОПК-6

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

4.3Самостоятельная работы студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Информационная безопасность в системе национальной безопасности России	1 неделя	2
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	2
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	2
6	Компьютерная информация – как объект информатизации	8-9 недели	4
7	Лицензирование в области защиты информации	10 неделя	2
8	Сертификация в области защиты информации	11-12 недели	4
9	Система правовой ответственности за утечку информации и утрату носителей информации	13 неделя	2
10	Правовые основы деятельности подразделений защиты информации	14 неделя	2

11	Правовые основы защиты личной тайны	15-17 недели	4
12	Правовые основы защиты персональных данных	18 неделя	2,85
	Итого		34,85

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 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 вопросов к экзамену, методических указаний к выполнению практических работ.

типографией университета:

− путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

− путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных 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)	Блиц опрос	1
2	Технические средства защиты информации (практическое занятие)	Блиц опрос	1
3	Защита персональных данных (практическое занятие)	Блиц опрос	1
4	Разработка организационно-распорядительной документации для объекта информатизации (практическое занятие)	Блиц опрос	2
5	Анализ эффективности применения средств защиты информации на объекте информатизации (практическое занятие)	Блиц опрос	2
6	Организация внутриобъектового режима (практическое занятие)	Блиц опрос	2
7	Организация пропускного режима (практическое занятие)	Блиц опрос	1
8	Разработка модели угроз информационной безопасности (практическое занятие)	Блиц опрос	2
	Итого		12

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 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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модуле), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации (ОПК-5)	Организационное и правовое обеспечение информационной безопасности		Производственная эксплуатационная практика

Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ОПК-6)	Организационное и правовое обеспечение информационной безопасности Управление информационной безопасностью телекоммуникационных систем	Производственная эксплуатационная практика

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

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала 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»)
ОПК-5/ основной	ОПК-5.1 Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	Знать: -стандарты в области информационной безопасности; Уметь: - сопоставлять характеристики правового обеспечения действующим стандартам, Владеть: - комплексной оценкой защищённости систем документооборота	Знать: - методологические подходы применения нормативных документов при оценке защищённости правового обеспечения; Уметь: - выявлять не декларируемые угрозы; Владеть: - способностью к критическому анализу используемых	Знать: - принципы формирования комплексных отчётов по аудиту информационной безопасности; Уметь: - вырабатывать методические рекомендации по формированию политик безопасности; Владеть: -организационными формами и методами проведения научных исследований

			методов аудита информационной безопасности	
	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
	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-5.4 Формулирует основные требования информационной безопасности при эксплуатации телекоммуникационной системы	Знать*:* Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. Уметь: применять действующую законодательную базу по защите конфиденциальной информации, при эксплуатации телекоммуникационной системы Владеть (или Иметь опыт деятельности): навыками работы с нормативными правовыми актами;	Знать*:* Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. Уметь: применять действующую законодательную базу по защите конфиденциальной информации, при эксплуатации телекоммуникационной системы 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 при эксплуатации телекоммуникационной системы	Знать*:* Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. Уметь: применять действующую законодательную базу по защите конфиденциальной информации, при эксплуатации телекоммуникационной системы 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 при эксплуатации телекоммуникационной системы; навыками анализа качества разработанных документов.
ОПК-6/ основной	ОПК-6.1 Разрабатывает модели угроз и модели нарушителя объекта	***Знать*** основные угрозы безопасности нарушителя объекта информатизации	***Знать*** основные угрозы безопасности объекта информатизации ***Уметь:*** разрабатывать	***Знать*** основные угрозы безопасности и модели нарушителя объекта информатизации ***Уметь:*** разрабатывать

	информатизации	***Уметь:*** разрабатывать модели угроз и модели нарушителя объекта информатизации ***Владеть (или Иметь опыт деятельности):*** навыками использования моделей угроз и нарушителя	модели угроз и модели нарушителя объекта информатизации ***Владеть (или Иметь опыт деятельности):*** навыками оценки угроз для объекта информатизации	модели угроз и модели нарушителя объекта информатизации ***Владеть (или Иметь опыт деятельности):*** навыками оценки угроз для объекта информатизации
	ОПК-6.2 Формулирует основные требования, предъявляемые к организации защиты информации ограниченного доступа	***Знать*** основные требования, предъявляемые к организации защиты информации ограниченного доступа ***Уметь:*** формулировать требования, предъявляемые к организации защиты информации ограниченного доступа ***Владеть (или Иметь опыт деятельности):*** навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа	***Знать*** требования, предъявляемые к организации защиты информации ограниченного доступа объекта информатизации ***Уметь:*** разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа ***Владеть (или Иметь опыт деятельности):*** навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа	***Знать*** требования, предъявляемые к организации защиты информации ограниченного доступа угрозы безопасности и модели нарушителя объекта информатизации ***Уметь:*** разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа ***Владеть (или Иметь опыт деятельности):*** навыками формулирования требований, предъявляемых к организации защиты информации ограниченного доступа
	ОПК-6.3 Анализирует состав и функциональные возможности средств защиты	***Знать*** основной состав и функциональные возможности средств защиты информации	***Знать*** состав и функциональные возможности средств защиты информации телекоммуникационной системы.	***Знать*** состав и функциональные возможности средств защиты информации телекоммуникационной системы.

	информации телекоммуникационной системы в целях его совершенствования	телекоммуникационной системы. ***Уметь:*** совершенствовать состав и функциональные возможности средств защиты информации телекоммуникационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы	***Уметь:*** совершенствовать состав и функциональные возможности средств защиты информации телекоммуникационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы	***Уметь:*** совершенствовать состав и функциональные возможности средств защиты информации телекоммуникационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы
	ОПК-6.4 Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	***Знать*** основные 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	***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	***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; навыками оценки качества

		защиты информации.	защиты информации.	разработанных документов.

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

№ 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	ОПК-5 ОПК-6	Лекция СРС	Вопросы для УО	1-11	Согласно табл. 7.2
2	Информация, информационные системы как объект правового регулирования информационной безопасности	ОПК-5 ОПК-6	Лекция СРС Практическое занятие	Вопросы для УО КВЗПР	1-12 1-10	Согласно табл. 7.2
3	Правовая основа допуска и доступа персонала к защищаемым сведениям	ОПК-5 ОПК-6	Лекция СРС	Вопросы для УО	1-11	Согласно табл. 7.2
4	Правовые проблемы, связанные с защитой прав обладателей собственности на информацию и распоряжением информацией	ОПК-5 ОПК-6	Лекция СРС Практическое занятие	Вопросы для УО КВЗПР	1-13 1-10	Согласно табл. 7.2
5	Правовые основы защиты коммерческой тайны	ОПК-5 ОПК-6	Лекция СРС	Вопросы для УО	1-12	Согласно табл. 7.2
6	Компьютерная информация – как объект информатизации	ОПК-5 ОПК-6	Лекция СРС Практическое занятие	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл. 7.2
7	Лицензирование в области защиты информации	ОПК-5 ОПК-6	Лекция СРС	Вопросы для УО	1-10	Согласно табл. 7.2

8	Сертификация в области защиты информации	ОПК-5 ОПК-6	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	ОПК-5 ОПК-6	Лекция СРС	Вопросы для УО	1-10	Согласно табл. 7.2
10	Правовые основы деятельности подразделений защиты информации	ОПК-5 ОПК-6	Лекция СРС	Вопросы для УО	1-10	Согласно табл. 7.2
11	Правовые основы защиты личной тайны	ОПК-5 ОПК-6	Лекция СРС Практическое занятие	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл. 7.2
12	Правовые основы защиты персональных данных	ОПК-5 ОПК-6	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…

4.Системный подход к защите информации базируется на принципах…

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:

между средствами и функциями

1	Человек, информация, технические средства	А	Информационное оружие
2	Целенаправленное производство и распространение специальной информации, оказывающей непосредственное влияние на функционирование и развитие психологической среды общества, психику и поведение населения, руководства страны, военнослужащих	Б	Информационное воздействие
3	Комплекс технических средств и технологий, предназначенных для получения контроля над информационными ресурсами потенциального противника в целях выведения их из строя, получения или модификации содержащихся в них	В	Элементы информационного пространства

	данных, целенаправленного продвижения выгодной информации (или дезинформации)		
		Г	Психологическое воздействие

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

1. 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

2. 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

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/
3. Электронно-библиотечная система «Лань» - http://e.lanbook.com/
4. Электронно-библиотечная система IQLib – http://www.iqlib.ru
5. Электронная библиотека «Единое окно доступа к образовательным ресурсам» - http://window.edu.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 перечь программного обеспечения и информационных справочных систем(при необходимости)

1) Libreoffice (Бесплатная, GNU General Public License) - https://ru.libreoffice.org/ ;
2) Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. С ООО «АйТи46», лицензионный договор №К0000000117 от 21.12.2015 г. с ООО «СМСКанал»,
3) Операционная система Windows, договор IT000012385;
4) Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234.

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.

Для проведения промежуточной аттестации необходимо следующее материально-техническое оборудование:

1. Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24

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	заме-нённых	анну-лирован-ных	новых			