МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра социального и семейного законодательства

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины
Организационное и правовое обеспечение информационной безопасности

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 21 апреля 2023 г., протокол № 5

Программа одобрена НМК
юридического факультета
протокол № 3 от 4 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Дисциплина «Организационное и правовое обеспечение информационной безопасности» призвана обеспечить освоение студентами теоретических и практических навыков работы с нормативными правовыми актами в области обеспечения информационной безопасности компьютерных систем, в том числе нормативными методическими документами ФСБ России и ФСТЭК России, и применения их положений в профессиональной деятельности.

Данная дисциплина раскрывает основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству России, систему защиты государственной тайны, а также основы организационного и правового регулирования отношений в области интеллектуальной собственности и способов ее защиты. Раскрываются понятие и виды компьютерных преступлений, правовые и организационные методы борьбы с ними.

2. Место дисциплины в структуре ОП

«Организационное и правовое обеспечение информационной безопасности» относится к числу дисциплин базовой части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент овладел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин «Основы управленческой деятельности» и «Основы информационной безопасности».

Знания и навыки, полученные в результате изучении дисциплины «Организационное и правовое обеспечение информационной безопасности», используются студентами в дальнейшем при разработке курсовых и дипломных работ.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Универсальные компетенции		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**И_УК-1_3** При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы и точку зрения	**Знать** основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации. **Уметь** применять основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации.

Общепрофессиональные компетенции		
ОПК- 5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	**И-ОПК-5_1.** Знает и понимает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации; **И-ОПК-5_2.** Имеет навык применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации; **И-ОПК-5_3** умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;	**Знать** требования российского законодательства в сфере защиты персональных данных, охраны результатов интеллектуальной деятельности. **Уметь** формулировать основные требования к защите информации и разрабатывать проекты локальных нормативных и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации. формировать политику информационной безопасности организации; контролировать ее исполнение.
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами	**И-ОПК-6_1** знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов	**Знать** методики лицензирования в области обеспечения защиты информации, аттестации объектов информатизации и сертификации средств защиты информации. **Уметь** подготовить необходимые документы для подрядчика по проведению работ в сфере лицензирования в области обеспечения защиты информации, аттестации объектов информатизации

Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях;	и сертификации средств защиты информации.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, **108** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	Самостоятельная работа	
1	Информация как объект правового регулирования.	9	2	1				4	Устный опрос. Подготовка реферата.
2	Законодательство в области информационной безопасности.	9	2	4		1		9	Устный опрос. Подготовка реферата.
3	Правовой режим защиты государственной тайны.	9	4	2		1		5	Устный опрос. Подготовка реферата.
4	Правовые режимы защиты конфиденциальной информации.	9	6	2		1		8	Устный опрос. Подготовка реферата.
5	Организационное обеспечение ИБ	9	6	2		1		8	Устный опрос. Подготовка реферата.
6	Защита интеллектуальной собственности.	9	4	3		2		6	Устный опрос. Подготовка реферата.
7	Международное законодательство в области защиты информации	9	4	1				4	Устный опрос. Подготовка реферата.
8	Компьютерные правонарушения	9	4	1				4	Устный опрос. Подготовка реферата.
							0,3	6,7	зачет
	Всего	**108**	32	16		5	0,3	54,7	

Содержание разделов дисциплины:

Тема 1. Информация как объект правового регулирования.

1. Структура информационной сферы и характеристика ее элементов. Виды информации.

2. Понятие и структура информационной безопасности.

3. Субъекты и объекты правоотношений в области информационной безопасности.

4. Формирование информационных ресурсов и их квалификация.

5. Конституционные гарантии прав на информацию и механизм их реализации.

Тема 2. Законодательство в области информационной безопасности.

1. Понятие и виды защищаемой информации по законодательству России.

2. Отрасли законодательства, регламентирующие деятельность по защите информации.

3. Доктрина информационной безопасности России.

4. Перспективы развития законодательства в области информационной безопасности.

Тема 3. Правовой режим защиты государственной тайны.

1. Понятие правового режима защиты государственной тайны.

2. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну.

3. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания.

4. Органы защиты государственной тайны и их компетенция.

5. Порядок допуска и доступа к государственной тайне.

6. Иные меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны).

7. Перечень и содержание организационных мер, направленных на защиту государственной тайны.

8. Система контроля за состоянием защиты государственной тайны.

9. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

Тема 4. Правовые режимы защиты конфиденциальной информации.

1. Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.

2. Правовые режимы конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации.

3. Юридическая ответственность за нарушения правового режима конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).

Тема 5. Организационное обеспечение информационной безопасности.

1. Понятия организационной защиты информации.

2. Виды представления информации.

3. Пути прохождения информации.

4. Основные каналы утечки информации при обработке на компьютерах.

5. Защита компьютерной информации.

6. Понятие «режим защиты информации».

7. Политика информационной безопасности.

8. Методы обеспечения физической безопасности.

9. Технологические меры поддержания безопасности.

10. Подразделения, обеспечивающие информационную безопасность предприятия, организации.

11. Обзор российских национальных стандартов в сфере информационной безопасности

Тема 6. Защита интеллектуальной собственности.

1. Законодательство РФ об интеллектуальная собственности.
2. Понятие интеллектуальной собственности. Объекты и субъекты авторского права. Исключительные авторские права. Смежные права.
3. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем.
4. Защита авторских и смежных прав.
5. Основы патентных правоотношений. Условия патентоспособности.
6. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями. Авторы изобретений и патентообладатели.
7. Механизм патентования.
8. Защита прав патентообладателей и авторов.
9. Особенности договорных отношений в области информационной безопасности.
10. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности. Особенности трудовых отношений.
11. Обзор положений ГОСТ Р ИСО/МЭК 56824-2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет».

Тема 7. Международное законодательство в области защиты информации

1. Правовой режим участия в международном обмене.
2. Субъекты и объекты международного информационного обмена.
3. Национальные законодательства о компьютерных правонарушениях и защите информации. (Беларусь, США, ЕС, Китай)
4. Международное сотрудничество в области борьбы с компьютерной преступностью.

Тема 8. Компьютерные правонарушения

1. Преступления в сфере компьютерной информации.
2. Признаки и элементы состава преступления.
3. Основы расследования преступлений в сфере компьютерной информации.
4. Административная ответственность за правонарушения в сфере информационных технологий.
5. Обзор положений ГОСТ Р ИСО/МЭК 18044-2007 «Менеджмент инцидентов информационной безопасности» для решения задач расследования инцидентов безопасности.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине (или ее разделе) и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки специалиста. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках курса, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины,

активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний по предложенному алгоритму.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

Электронный учебный курс «Организационное и правовое обеспечение информационной безопасности» в LMS Электронный университет Moodle ЯрГУ, в котором:

- представлены задания для самостоятельной работы обучающихся по темам дисциплины;
- осуществляется проведение отдельных мероприятий текущего контроля успеваемости студентов;
- представлены тексты лекций по отдельным темам дисциплины;
- представлены правила прохождения промежуточной аттестации по дисциплине;
- представлен список учебной литературы, рекомендуемой для освоения дисциплины;
- представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;

посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- Adobe Acrobat Reader;
- Интернет-версия справочной системы Гарант.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

Автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993).
2. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).
3. Федеральный закон от 27.07.2006 № 149 – ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.
5. Федеральный закон ««О коммерческой тайне» от 29.07.2004 N 98-ФЗ.
6. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне».
7. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года №187-ФЗ.
8. Часть четвертая Гражданского кодекса Российской Федерации от 18 декабря 2006 г. № 230-ФЗ.
9. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ (ред. от 30.12.2021).
10. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 30.12.2021).
11. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844 (дата обращения: 29.01.2022).
12. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277 (дата обращения: 29.01.2022).
13. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) : учебное пособие. / В. К. Новиков - Москва : Горячая линия - Телеком, 2015. - 176 с. - ISBN 978-5-9912-0525-2. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991205252.html (дата обращения: 29.01.2022). - Режим доступа : по подписке.
14. ГОСТ Р ИСО/МЭК 56824-2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет» Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2017. - 27с.
15. ГОСТ Р ИСО/МЭК 18044-2007г., «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2009. - 46с.

б) дополнительная литература:

1. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах№ (Зарегистрировано в Минюсте России 31.05.2013 № 28608).
2. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375).

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год. http://fstec.ru/component/attachments/download/289 .

4. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.).

5. Банк данных угроз безопасности информации ФСТЭК России. https://bdu.fstec.ru/threat

6. Некоммерческая (бесплатная) Интернет-версия справочной системы Гарант. http://ivo.garant.ru/#/startpage:0

7. Коваленко, Ю. И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Коваленко Ю. И. - Москва : Горячая линия - Телеком, 2012. - 140 с. - ISBN 978-5-9912-0261-9. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991202619.html (дата обращения: 29.01.2022). - Режим доступа : по подписке.

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор:

старший преподаватель кафедры КБ и ММОИ		А.В. Саханда
должность, ученая степень	*подпись*	*И.О. Фамилия*

Приложение №1 к рабочей программе дисциплины
«Организационное и правовое обеспечение информационной безопасности»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1. Контрольные задания и иные материалы, используемые в процессе текущей аттестации.

В течение семестра каждому студенту необходимо подготовить реферат по одной из выбранных тем из нижеуказанного списка. Сдача реферата является необходимым условием для допуска к зачету.

Перечень тем для подготовки рефератов:

1. Принципы государственной политики обеспечения информационной безопасности.
2. Ключевые проблемы информационной безопасности государства.
3. Основные обязанности органов законодательной власти в сфере информационной безопасности.
4. Основные обязанности органов исполнительной власти в сфере информационной безопасности.
5. Основные обязанности органов судебной власти в сфере информационной безопасности.
6. Информационные войны: проблемы правового регулирования.
7. Право на доступ к информации в России: проблемы теории и законодательства.
8. Проблема практического применения ФЗ «Об информации, информационных технологиях и о защите информации».
9. Понятие и роль информации в жизни современного общества.
10. Гарантии информационных прав граждан.
11. Права граждан в информационной сфере.
12. Организация защиты государственной тайны в России.
13. Ответственность за шпионаж и разглашение государственной тайны.
14. Состояние и эффективность законодательства о коммерческой тайне.
15. Изменения в правовом регулировании института коммерческой тайны в связи с введением в действие четвертой части Гражданского кодекса РФ.
16. Требования к обработке персональных данных и ответственность за нарушение работы с ними.
17. Международное и национальное законодательство зарубежных стран о защите персональных данных.
18. Персональные данные в системе документооборота предприятия.
19. Персональные данные в Интернете.
20. Правовое регулирование борьбы с киберпреступностью в США (Италии, Китае, Японии, Великобритании).
21. Выявление технических каналов утечки информации.
22. История развития криптографии.
23. Криптография как средство защиты информации.
24. Расследование компьютерных преступлений в РФ и за рубежом.

25. Роль положений ГОСТ Р ИСО/МЭК 18044-2007г., «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», в расследовании инцидентов компьютерной безопасности.

26. Роль положений ГОСТ Р ИСО/МЭК 56824-2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет» в защите интеллектуальной собственности российских государственных и коммерческих структур при ее попадании в Интернет.

1.2. Список вопросов для опроса на практических занятиях

1. Какие в настоящее время отмечаются особенности структуры информационной сферы и характеристики ее элементов?
2. В чем заключаются парадоксы понятия и структура информационной безопасности?
3. На каких принципах строятся правоотношения в области информационной безопасности?
4. В чем заключаются конституционные гарантии прав на доступ к информации и обеспечение сохранности различных видов тайны?
5. Чем обеспечиваются гарантии защиты информации по законодательству Российской федерации и исключения из предусмотренных законом правил?
6. В чем суть и основные направления реализации национальных интересов России в сфере ИБ, отраженные в Доктрине информационной безопасности Российской Федерации?
7. Каковы перспективы развития законодательства в области информационной безопасности в настоящий исторический период?
8. Каковы составляющие российской системы обеспечения безопасности критических информационных систем от компьютерных атак?
9. Каковы функции участников реализации системы обеспечения безопасности критических информационных систем от компьютерных атак?
10. На что направлено введение правового режима защиты государственной тайны?
11. Назовите состав принципов, механизмов и процедур отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
12. Какие организации и структуры непосредственно осуществляют защиту государственной тайны, регулируют и контролируют?
13. Назовите и опишите порядок допуска и доступа к государственной тайне.
14. Опишите предназначение и составляющие режима секретности, как основного порядка деятельности в сфере защиты государственной тайны, организационных и технических мер, направленных на защиту государственной тайны.
15. Какими органами и в каком порядке реализуется система контроля за состоянием защиты государственной тайны?
16. Опишите составляющие условий наступления юридической ответственности за нарушения правового режима защиты государственной тайны (уголовной, административной, дисциплинарной).
17. Что общего и в чем различия в характере конфиденциальной информации различных видов: персональных данных, служебной тайны, коммерческой и банковской тайны, тайны следствия и судопроизводства, других профессиональных видов тайны?
18. Каковы основные требования, предъявляемые к организации защиты конфиденциальной информации?
19. Опишите составляющие условий наступления юридической ответственности за нарушения правового режима конфиденциальной информации (уголовной, административной, гражданско-правовой и дисциплинарной).

20. В чем отличия организационной от технической защиты информации?
21. Как определяются основные каналы утечки информации при обработке на компьютерах?
22. Как формируется и на что направлена политика информационной безопасности?
23. Опишите и дайте характеристику методов обеспечения физической безопасности.
24. Для чего вводятся и из чего состоят технологические меры поддержания безопасности?
25. Поясните на примере состав и функции подразделения, обеспечивающего информационную безопасность предприятия.
26. В чем особенности настоящего состава законодательства России об интеллектуальная собственности?
27. Поясните различие и связь исключительных авторских и смежных прав в сфере интеллектуальной собственности.
28. Какая предусмотрена в Российской Федерации правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем?
29. Поясните сложности в защите авторских и смежных прав.
30. Какие в настоящее время условия патентоспособности действуют в настоящее время в России? В мировом сообществе?
31. Какие выделяются объекты изобретения, полезной модели и промышленного образца, связанные с электронно-вычислительной техникой и информационными технологиями?
32. Как осуществляется защита прав патентообладателей и авторов полезных моделей?
33. Каковы особенности договорных отношений России со странами ближнего и дальнего зарубежья в области информационной безопасности?
34. В чем суть и содержание правового регулирования трудовых отношений администрации и персонала в области обеспечения информационной безопасности?
35. Назовите и охарактеризуй те основные составляющие правового режима участия российских предприятий организаций и учреждений различных форм собственности в международном информационном обмене.
36. Назовите субъекты и объекты международного информационного обмена.
37. Приведите примеры положительных результатов международного сотрудничества в области борьбы с компьютерной преступностью.
38. Назовите и поясните признаки и элементы состава преступлений в сфере компьютерной информации (ст. 272, 273, 274 УК России).
39. Какие необходимо знать основы расследования преступлений в сфере компьютерной информации?
40. Каковы условия наступления административной ответственности за правонарушения в сфере информационных технологий?
41. Какие положения ГОСТ Р ИСО/МЭК 18044-2007г., «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» применимы в расследовании инцидентов компьютерной безопасности?
42. Какие положения ГОСТ Р ИСО/МЭК 56824-2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет» применимы в защите интеллектуальной собственности российских государственных и коммерческих структур при ее попадании в Интернет?

1.3 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету

1. Информация как объект правового регулирования. Структура информационной сферы и характеристика ее элементов. Виды информации. Формирование

информационных ресурсов и их квалификация. Конституционные гарантии прав на информацию и механизм их реализации.

2. Понятие и структура информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ.

3. Отрасли законодательства, регламентирующие деятельность по защите информации. Перспективы развития законодательства в области информационной безопасности.

4. Понятие правового режима защиты государственной тайны. Государственная тайна как особый вид защищаемой информации и её характерные признаки.

5. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания.

6. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Иные меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны).

7. Перечень и содержание организационных мер, направленных на защиту государственной тайны. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

8. Правовые режимы защиты конфиденциальной информации. Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.

9. Правовые режимы конфиденциальной информации в России: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Юридическая ответственность за нарушения правового режима конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).

10. Правовая регламентация охранной деятельности. Лицензирование и сертификация в информационной сфере. Понятия лицензирования по российскому законодательству. Виды деятельности в информационной сфере, подлежащие лицензированию.

11. Правовые основы защиты информации с использованием технических средств (защиты от технических разведок, применения и разработки шифровальных средств, применения электронно-цифровой подписи и т.д.).

12. Защита интеллектуальной собственности. Законодательство РФ об интеллектуальная собственности. Понятие интеллектуальной собственности.

13. Объекты и субъекты авторского права. Исключительные авторские права. Смежные права.

14. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем.

15. Защита авторских и смежных прав. Основы патентных правоотношений. Условия патентоспособности.

16. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями. Авторы изобретений и патентообладатели. Механизм патентования. Защита прав патентообладателей и авторов.

17. Особенности договорных отношений в области информационной безопасности. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности. Особенности трудовых отношений.

18. Компьютерные правонарушения. Преступления в сфере компьютерной информации. Признаки и элементы состава преступления. Административная ответственность за преступления в информационной сфере.

19. Международное законодательство в области защиты информации. Правовой режим участия в международном обмене. Субъекты и объекты международного информационного обмена.

20. Национальные законодательства о компьютерных правонарушениях и защите информации.

21. Международное сотрудничество в области борьбы с компьютерной преступностью.

22. Положения ГОСТ Р ИСО/МЭК 18044-2007г., «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», имеющие значение для расследования инцидентов компьютерной безопасности.

23. Положения ГОСТ Р ИСО/МЭК 56824-2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет», имеющие значение для защиты интеллектуальной собственности российских государственных и коммерческих структур при ее попадании в Интернет.

24. Основные положения федерального закона от 26 июля 2017 года №187 – ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» для укрепления национальной системы защиты критической информационной инфраструктуры страны.

2. Правила приема зачета.

Оценка знаний по итогу прохождения курса проводится в форме принятия зачета.

На зачете проверяется сформированность всех указанных в учебной программе компетенций (ОПК-1, ОПК-5, ОПК-6, ОПК-10).

В билет для зачета включаются два теоретических вопроса. На подготовку к ответу дается не менее 1 академического часа.

Также есть возможность ответить на контрольные вопросы в электронном курсе «Организационное и правовое обеспечение информационной безопасности» в LMS Электронный университет Moodle ЯрГУ.

По итогам ответов студенту выставляется одна из оценок: «зачтено», «не зачтено».

Оценка «зачтено» выставляется студенту, если: он знает основные определения, последователен в изложении материала, демонстрирует базовые знания дисциплины, владеет необходимыми умениями и навыками при выполнении практических заданий.

Оценка «не зачтено» выставляется студенту, если: он не знает основных определений, непоследователен и сбивчив в изложении материала, не обладает определенной системой знаний по дисциплине, не в полной мере владеет необходимыми умениями и навыками при выполнении практических заданий.

Оценка «не зачтено» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

Приложение №2 к рабочей программе дисциплины
«Организационное и правовое обеспечение информационной безопасности»

Методические указания для студентов по освоению дисциплины

Изучение дисциплины предполагает уверенное владение компьютером, умение осуществлять поиск и оценку достоверности необходимой информации в сети Интернет, но студенту достаточно сложно самостоятельно освоить вопросы дисциплины «Организационное и правовое обеспечение информационной безопасности». Посещение всех предусмотренных аудиторных занятий является совершенно необходимым в силу обучения на них учащихся сравнительным оценкам знаний из различных источников, критической их оценки. Также без упорных и регулярных самостоятельных занятий в течение семестра, желательно с «упреждающим знакомством» с содержанием предстоящего занятия, крайне сложно усвоить логику и аргументацию упомянутых сравнительных оценок и критического анализа знаний из различных источников, что не позволит студентам развить продвинутого и высокого уровня компетенций.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы рекомендуется использовать учебную литературу, интернет-источники, указанные в разделе 7 настоящей Рабочей программы и электронный курс «Организационное и правовое обеспечение информационной безопасности» в LMS Электронный университет Moodle ЯрГУ.