



Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ
СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

«УТВЕРЖДАЮ»

И.о. проректора

А.В. Троицкий

«__» _____ 2023 г.

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Б.1.В.04 «ГУМАНИТАРНЫЕ АСПЕКТЫ (ПРОФЕССИОНАЛЬНАЯ
ЭТИКА) ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Соляной В.Н. Рабочая программа дисциплины: «Гуманитарные аспекты (профессиональная этика) информационной безопасности». – Королев МО: «Технологический университет», 2023.

Рецензент: Сухотерин А.И.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переподтверждения)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	№8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП ВО

 Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переподтверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является ознакомление студентов с историей развития информационных технологий, социальными аспектами построения информационного общества, профессиональной ответственностью и морально-этическими нормами поведения при работе с информационными технологиями, вопросами интеллектуальной собственности, вопросами личной безопасности и свободы самовыражения в киберпространстве, влиянием информационных технологий на интернациональность культуры.

Основными **задачами** дисциплины являются формирование у будущих специалистов основ теоретических знаний и приобретение практических навыков работы с информационными технологиями, необходимыми при осуществлении их профессиональной деятельности.

Предмет дисциплины - социальные и этические аспекты, возникающие в обществе в процессе развития информационных технологий и их влияние на характеристики общества, на взаимоотношения между обществом и его членами, а также между отдельными членами общества или его группами.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

Профессиональные компетенции:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС.

Основными задачами дисциплины являются:

1. ознакомление студентов с процессами становления и развития системы защиты информации ее гуманитарными аспектами в России, с государственной политикой и деятельностью органов защиты информации в различные периоды развития государства, с процессами развития и совершенствования нормативной базы по защите информации;

2. формирование у студентов способности самостоятельно анализировать и использовать исторический опыт, основные тенденции, принципы, методы и компоненты системы защиты информации в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам в России.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- описание сути проблемной ситуации
- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;

Необходимые умения:

- выявление составляющих проблемной ситуации и связей между ними
- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;

Трудовые действия:

- выбор способа обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации
- сбор и систематизация информации по проблеме
- оценка адекватности и достоверности информации о проблемной ситуации
- выбор методов критического анализа, адекватных проблемной ситуации
- разработка и обоснование плана действий по решению проблемной ситуации
- анализировать воздействие на защищаемую систему информации, оценивать последствия и выработать предложения по ее совершенствованию;

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Гуманитарные аспекты (профессиональная этика) информационной безопасности» относится к обязательным дисциплинам вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Математическая логика и теория алгоритмов» и компетенциях: ОПК-1,3,5,6,8; ДОПК-1,3.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и очно - заочной формы составляет 2 зачетных единицы, 72 часа.

Таблица 1

Виды занятий	Всего часов	Семестр 6	Семестр 7	Семестр ...	Семестр ...
Общая трудоемкость	72	72			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32	32			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	30	30			
Другие виды контактной работы	6	6			
Практическая подготовка	4	4			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	T1; T2	T1; T2			
Вид итогового контроля	Зачет	Зачет			
ОЧНО - ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	16		16		
Лекции (Л)	8		8		
Практические занятия (ПЗ)	8		8		
Лабораторные работы (ЛР)	-		-		
Самостоятельная работа	56		56		
Другие виды контактной работы	6		6		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+		+		
Практическая подготовка	4		4		
Вид итогового контроля	Зачет		Зачет		

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. очное /очно - заочное	Практические занятия, час. очное/очно-заочное	Занятия в интерактивной форме, час. очное/очно-заочное	Практическая подготовка, час	Код компетенций
1	2	3	4		5
Тема 1. Предмет и задачи курса. Основы информационной этики	2/1	2/1	1/1	-/-	УК-1; ПК-3
Тема 2. История информационных технологий	2/1	2/1	1/1	-/-	УК-1; ПК-3
Тема 3. Влияние информационных технологий на социальные процессы	2/1	2/1	1/1	-/-	УК-1; ПК-3
Тема 4. Анализ этических проблем и норм при формировании глобального информационного общества	2/1	2/1	1/1	-/-	УК-1; ПК-3
Тема 5. Профессиональная ответственность и профессиональная этика при работе с информационными технологиями	2/1	2/1	1/1	1/1	ПК-3
Тема 6. Сущность информационных рисков и управление ими	2/1	2/1	1/1	1/1	ПК-3
Тема 7. Интеллектуальная собственность	2/1	2/1	1/1	1/1	ПК-3
Тема 8. Частная жизнь и гражданские свободы в информационном обществе	2/1	2/1	2/1	1/1	ПК-3
Итого:	16/8	16/8	9/8	4/4	

4.2. Содержание тем дисциплины

Тема 1. Предмет и задачи курса. Основы информационной этики
Этика. Информационная этика. Цель курса. Области информационной этики, предмет ее исследований, необходимость изучения и исследований. Этические кодексы в сфере информационных технологий. Проблемы компьютерной этики. Принципы компьютерной этики. Основные положения кодекса компьютерной этики.

Тема 2. История информационных технологий
Мир в докомпьютерную эру. История развития компьютеров, программного обеспечения, сетевой обработки данных. Пионеры информационных технологий. Необходимость изучения социально-этических вопросов в области информационных технологий в высшей школе.

Тема 3. Влияние информационных технологий на социальные процессы
Влияние информационных технологий и телекоммуникаций на социальные процессы. Сеть Интернет. Организация управления сетью Интернет и доступа к ее ресурсам; Этика информационного общества. Международное сотрудничество и по вопросам этики.

Тема 4. Анализ этических проблем и норм при формировании глобального информационного общества
Этические проблемы формирования глобального информационного общества. Виртуальная (информационная) этика. Оценка аспектов профессиональной деятельности с позиций этики. Понимание социальных аспектов разработки информационных технологий, учет возможных последствий и реальных ценностей. Национальный кодекс деятельности в области информатики и телекоммуникаций.

Тема 5. Профессиональная ответственность и профессиональная этика при работе с информационными технологиями
Общественные ценности и законы этики. Сущность профессионализма. Ступени профессиональной подготовки и их оценка. Роль профессионалов в социальных процессах; уверенность в будущем. Этические кодексы и их осуществление на практике (IEEE, ACM, SE, AITP и др.) Недоверие и дискриминация. Всеобъемлющая информатизация и повсеместное использование информационных технологий. Этика информационной безопасности.

Тема 6. Сущность информационных рисков и управление ими
Риски, связанные с применением компьютерных систем. Анализ и оценка рисков. Управление рисками. Примеры отказов и нарушения безопасности

информационных технологий. Проблемы, связанные со сложностью информационных технологий. Понимание рисков и затрат компании, связанных с использованием нелицензионного программного обеспечения. Управление рисками и оценка рисков. Страхование информационных рисков как метод защиты информации.

Тема 7. Интеллектуальная собственность

Основы интеллектуальной собственности. Права собственности, патенты, коммерческая тайна. Пиратство в использовании программного обеспечения и информационных технологий в целом. Патентование программного обеспечения. Интеллектуальная собственность. Международное право в области информационных технологий.

Тема 8. Частная жизнь и гражданские свободы в информационном обществе

Этические и законодательные основы личной безопасности. Конфиденциальность персональной информации в базах данных. Технологические решения для обеспечения конфиденциальности. Свобода самовыражения в киберпространстве. Влияние информационных технологий на интернациональность культуры.

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

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Гуманитарные аспекты (профессиональная этика) информационной безопасности» приведена в Приложении 1.

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

Основная литература:

1. Гальперин, Михаил Владимирович.

Электротехника и электроника : Учебник. - 1. - Москва ; Москва : Издательство "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2016. - 480 с. - ISBN 9785911347833. - Электронная программа (визуальная).

Электронные данные : электронные.

URL: <http://znanium.com/go.php?id=553180>

2.Куприянов, А.И.

Радиоэлектронная борьба. - 5-е изд. - Москва : Вузовская книга, 2018. - 360 с. : ил. - ISBN 978-5-9502-0833-1. - Текст (визуальный) : непосредственный.

Дополнительная литература:

3.Башлы, П. Н.

Информационная безопасность и защита информации. - Москва :

Издательский Центр РИОР, 2013. - 222 с. - ISBN 9785369011782. -

Электронная программа (визуальная). Электронные данные : электронные.

URL: <http://znanium.com/go.php?id=405000>

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

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
2. <http://informika.ru/> – образовательный портал
3. www.wiklsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. www.biblioclub.ru - Универсальная библиотека онлайн
5. www.rucont.ru - ЭБС «Рукопт».
6. <http://www.academy.it.ru/> – академия АЙТИ.
7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации
8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации.
9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности
10. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному Контролю

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы:

Электронные ресурсы образовательной среды Университета.

Информационно-справочные системы (Консультант+; Гарант).

Ресурсы информационно-образовательной среды МГОТУ:
Рабочая программа и методическое обеспечение по курсу «Гуманитарные аспекты (профессиональная этика) информационной безопасности»

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

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО
ДИСЦИПЛИНЕ**

**«ГУМАНИТАРНЫЕ АСПЕКТЫ (ПРОФЕССИОНАЛЬНАЯ ЭТИКА)
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

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

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Темы 1-4	<ul style="list-style-type: none"> - выбор способа обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации - сбор и систематизация информации по проблеме - оценка адекватности и достоверности информации о проблемной ситуации 	<ul style="list-style-type: none"> - выявление составляющих их проблемной ситуации и связей между ними 	<ul style="list-style-type: none"> - описание сути проблемной ситуации
2.	ПК-3	Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС	<i>Тема 1-8</i>	<ul style="list-style-type: none"> - анализировать воздействие на защищаемую систему информации, оценивать последствия и выработать предложения по ее совершенствованию 	<ul style="list-style-type: none"> - оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ; 	<ul style="list-style-type: none"> - основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;

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

Код компетенции	Инструмент, оценивающий сформированность компетенции	Этапы и показатель оценивания компетенции	Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания
УК-1 ПК-3	<i>Доклад</i>	<p><i>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</i></p> <p><i>Б) частично сформирована:</i></p> <ul style="list-style-type: none"> <i>• компетенция освоена на <u>продвинутом</u> уровне – 4 балла;</i> <i>• компетенция освоена на <u>базовом</u> уровне – 3 балла;</i> <p><i>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</i></p> 	<p><i>Например:</i> <i>Проводится в письменной и/или устной форме.</i> <i>Критерии оценки:</i></p> <ol style="list-style-type: none"> <i>1. Соответствие содержания доклада заявленной тематике (1 балл).</i> <i>2. Качество источников и их количество при подготовке работы (1 балл).</i> <i>3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).</i> <i>4. Качество самой представленной работы (1 балл).</i> <i>5. Оригинальность подхода и всестороннее раскрытие выбранной тематике (1 балл).</i> <p><i>Максимальная сумма баллов - 5 баллов.</i></p>
ПК-3	<i>Выполнение контрольной работы</i>	<p><i>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</i></p> <p><i>Б) частично сформирована:</i></p> <ul style="list-style-type: none"> <i>• компетенция освоена на <u>продвинутом</u> уровне – 4 балла;</i> <i>• компетенция освоена на <u>базовом</u> уровне – 3 балла;</i> <p><i>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</i></p> 	<p><i>При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида</i></p>

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

а) Темы докладов в форме презентации

1. История развития компьютеров, программного обеспечения, Интернет.
2. Основные этапы становления глобальной сети Интернет.
3. Информационное общество.
4. Влияние информационных технологий на социальные процессы.
5. Общественные ценности и законы этики; сущность профессионализма.
6. Этические проблемы формирования глобального информационного общества.
7. Социальные аспекты разработки и внедрения информационных технологий.
8. Виртуальная (информационная) этика: предмет, регулируемые отношения, сферы.
9. Оценка аспектов профессиональной деятельности с позиций этики.
10. Международное право в области информационных технологий.
11. Этические кодексы и их осуществление на практике (IEEE, ACM, SE, AITP и др.)
12. Национальный кодекс деятельности в области информатики и телекоммуникаций: ценностное основание.
13. Этические и законодательные основы личной безопасности в киберпространстве.
14. Основы интеллектуальной собственности.
15. Конфиденциальность персональной информации в базах данных и хранилищах.
16. Свобода самовыражения в киберпространстве.
17. Влияние информационных технологий на интернациональность культуры.
18. Риски, связанные с применением компьютерных систем.
19. Свобода самовыражения в киберпространстве.
20. Киберпространство: содержание, виды, их сходство и различие.
21. Преимущества и недостатки Интернета в сравнении с другими средствами массовой информации и коммуникации.
22. Взаимозависимость важнейших принципов информационной этики: права доступа к информации и необходимости защиты конфиденциальной информации.
23. Этические правила хранения, передачи и распространения информации.
24. Реализация принципа свободы доступа к информации в международных документах по правам человека.
25. Основные направления деятельности ЮНЕСКО по пропаганде информационной этики.

26. Базовые принципы, лежащие в основе правил сетевого этикета.
27. Специфика соблюдения авторских прав в Интернете. Сложности определения интеллектуальной собственности в Интернете.
28. Киберпреступления: их виды и особенности.
29. Пиратство в использовании информационных технологий. Плагиат и копирование: их различие с точки зрения защиты авторских прав и сетевой этики.
30. Права собственности, патенты, коммерческая тайна.
31. Хакерство как вид профессиональной деятельности. Виды хакерства.
32. Понимание рисков и затрат компании, связанных с использованием нелицензионного программного обеспечения.
33. Страхование информационных рисков как метод защиты информации.
34. Понятие об информационных технологиях.
35. Признаки информационного общества.
36. Основные периоды развития информационных технологий.
37. Особенности постиндустриального развития.
38. Какую роль играет информация в современном обществе.
39. Влияние информатизации общества на структуру современных профессий?
40. Производство информации (как товара) и материальные ресурсы.
41. Запасы сырьевых ресурсов и производство компьютерной техники.
42. Какие государства владеют полной технологией производства компьютеров?
43. Ценности и нормы профессиональной этики разработчиков программного обеспечения.
44. Особенности современных информационно-коммуникационных технологий.
45. Основные направления в области развития информационных технологий.
46. Перспективные сферы информатизации.
47. Понятие "информационная этика".
48. Суть и опасность информационного разделения общества.
49. Современное понятие "информационная культура".
50. Принцип "свободы доступа к информации".
51. Новые возможности личности и современные информационные технологии.
52. Специфика соблюдения авторских прав в Интернете.
53. Международные кодексы о свободе доступа к информации: их моральное и социокультурное значение.
54. Компьютерные преступления: виды, причины и возможности противодействия.
55. Виды виртуальной коммуникации; их положительные и отрицательные черты с точки зрения моральной оценки.
56. Основные направления влияния информационных технологий на экономику.

57. Особенности профессионального кодекса специалиста по информационным технологиям.
58. Основные виды взаимодействий, регулируемые профессиональным кодексом специалиста информационным технологиям.
59. Проблемы и особенности глобализации в условиях информационного общества.
60. Основные социальные проблемы применения информационных технологий.
61. Факторы, повышающие риски применения информационных технологий.
62. Как осуществляется права собственности на информационные ресурсы в РФ.
63. Основные методы обеспечения информационной безопасности.
64. Свобода самовыражения в киберпространстве.
65. Основные вредные факторы воздействия на окружающую среду при производстве и эксплуатации компьютерной техники.
66. Современные тенденции в области Green IT.

б) Темы контрольной работы (домашнего задания)

1. Возможности, свойства, функции сети Интернет, которые вызывают наибольший позитивный отклик.

В этом задании студентам предлагается сформулировать, какие 5 (пять) возможностей, свойств, функций сети Интернет, которые вызывают позитивный отклик со следующей дифференциацией ответов:

- a. Самая важная и полезная для меня возможность, предоставляемая Интернет.
- b. Очень важная и полезная для меня возможность, предоставляемая Интернет.
- c. Весьма важная и полезная для меня возможность, предоставляемая Интернет.
- d. Важная и полезная для меня возможность, предоставляемая Интернет.
- e. Как кажется, важная и полезная для меня возможность, предоставляемая Интернет.

Ответы студентов обобщаются преподавателем и используются при обсуждении текущей и следующих тем курса.

2. Возможности, свойства, функции сети Интернет, которые вызывают наибольший позитивный отклик.

В этом задании студентам предлагается сформулировать, какие 5 (пять) возможностей, свойств, функций сети Интернет, которые вызывают позитивный отклик со следующей дифференциацией ответов:

- a. Самая бесполезная и ненужная для меня возможность, предоставляемая Интернет.
- b. В большой степени бесполезная и ненужная для меня возможность, предоставляемая Интернет.

- с. Довольно бесполезная и ненужная для меня возможность, предоставляемая Интернет.
 - d. Бесполезная и ненужная для меня возможность, предоставляемая Интернет.
 - е. Как кажется, бесполезная и ненужная для меня возможность, предоставляемая Интернет.
- Ответы студентов обобщаются преподавателем и используются при обсуждении текущей и следующих тем курса.

3. Ожидания студентов от занятий по дисциплине.

В этом задании студентам предлагается сформулировать в свободной форме, какого результата хотели бы они достичь, закончив занятия по курсу "Социальные и этические вопросы ИТ": Что нового хотели бы узнать и чему научиться? По каким вопросам хотелось больше подробностей и фактов?

Какие проблемы непонятны?

Сформулированный ответ посылается преподавателю по электронной почте. После выполнения задания преподавателем формулируются актуальные темы

курса, на которые должно быть обращено особое внимание. Например: "свобода

взаимоотношений в Интернет", "интеллектуальная собственность", "преступления в сфере ИТ", "профессиональная этика".

Тексты электронных писем анализируются на предмет наличия обратного адреса,

темы, обращения к адресату, подписи, корректного форматирования.

Организуется обсуждение проблем профессионализма, уважения собеседника и

вежливости при сетевой коммуникации.

4. Подготовить реферат на выбранную тему.

Реферат (эссе) должен быть подготовлен в соответствии с требованиями и рекомендациями преподавателя. Темы рефератов приведены в рабочей программе.

По выбору студентов и по согласованию с преподавателем возможно проведение

практических (лабораторных) занятий по следующим дополнительным темам:

5. Проведение оценки аспектов профессиональной деятельности с позиций этики менеджера по информационным технологиям.

6. Выявление информационных рисков и угроз компьютерным системам. Разработка мероприятий по управлению рисками и оценке рисков. Учет возможных последствий рисков.

7. Оценка возможности и определение путей законного использования интеллектуальной собственности.

8. Оценка ответственности за нарушение права частной жизни и гражданских свобод в сфере информационных технологий.

Задания лабораторного практикума готовятся в соответствии с методическими указаниями по выполнению лабораторных работ и могут быть доступны для выполнения.

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

Формой контроля знаний по дисциплине «Гуманитарные аспекты (профессиональная этика) информационной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оцениваемых знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
<i>Проводится в сроки, установленные графиком образовательного процесса</i>	тестирование	УК-1; ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	<i>Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.</i>

<p><i>Проводится в сроки, установленные графиком образовательного процесса</i></p>	<p>тестирование</p>	<p>УК-1; ПК-3</p>	<p>20 вопросов</p>	<p>Компьютерное тестирование; время отведенное на процедуру – 30 минут</p>	<p>Результаты тестирования предоставляются в день проведения процедуры</p>	<p><i>Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением</i></p> <p><i>Неявка – 0.</i> <i>Неудовлетворительно – менее 50% правильных ответов</i> <i>Удовлетворительно - от 51% правильных ответов.</i> <i>Хорошо - от 70%.</i> <i>Отлично – от 90%.</i></p>
<p><i>Проводится в сроки, установленные графиком образовательного процесса</i></p>	<p>Зачет</p>	<p>УК-1; ПК-3</p>	<p>2 теоретических вопроса + практическое задание</p>	<p>Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 15 минут.</p>	<p>Результаты предоставляются в день проведения зачета</p>	<p>Критерии оценки: «Зачтено»:</p> <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на семинарских занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. <p>«Не зачтено»:</p>

						<ul style="list-style-type: none"> • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • не умеет использовать и применять полученные знания на практике; • не работал на семинарских занятиях; не отвечает на вопросы.
--	--	--	--	--	--	--

4.2. Типовые вопросы, выносимые на зачет

1. Могут ли быть переданы другому лицу автором произведения имущественные права и неимущественные права?
2. Какие права НЕ могут быть переданы автором произведения другому лицу?
3. Частью чего является авторское право: гражданского права, уголовного права, административного права, семейного права.
4. Каковы перспективы биометрических процедур?
5. Зачем используется блокирование доступа к различным типам контента семантической сети?
6. В каком году был организован доступ к Интернет в вычислительной системе Тверского государственного университета?
7. В каком году была создана первая вычислительная машина в современном понимании (компьютер)?
8. В каком году Интернет появился в России?
9. Значение государственного контроля посредством управления цифровой идентичностью.
10. На чем основан институциональный подход к ценообразованию информационных продуктов?
11. Сущностью каких рисков является информационная неопределенность?
12. Что такое информационная этика в широком смысле?
13. Какова цель управления информационными рисками?
14. На какой элементной базе работал компьютер ЭНИАК, созданный в

1944 году?

15. Кто изобрел Интернет?

16. Кто первым создал счетную машину - архитектурный прообраз современных компьютеров?

17. Какой статус имеет международная организация Internet Corporation for Assigned Names and Numbers (ICANN)?

18. Являются ли самостоятельными объектами авторского права музыкальные произведения с текстом (например, песни)?

19. Связано ли объективное случайное событие с информационной неопределенностью характеристик объектов или явлений для человека?

20. Основные принципы для создания языков программирования разработала:

21. Какие явления являются предпосылками возникновения информационного рынка?

22. Главное следствие информационных рисков.

23. Какие данные обязательно нужно указывать при цитировании материалов из Интернет?

24. Какие имеются допустимые особенности использования программ для ЭВМ и баз данных?

25. Области применения радиочастотной идентификации (RFID).

26. Какие области, этические вопросы рассматривает информационная этика?

27. Приведите примеры легального использования программного обеспечения.

28. Каковы свойства информации как экономического ресурса?

29. Каковы следствия только информационных рисков?

30. Что такое имущественные права на произведение?

31. Что такое информационные риски?

32. Каковы области современного информационного рынка?

33. Какие Вы знаете показатели качества информации?

34. Какие принципы считаются основными в рамках компьютерной этики?

35. Каковы последствия полной коммерциализации информационной деятельности?

36. Почему этические проблемы возникли с распространением компьютерных технологий и особенно Интернета?

37. Предмет исследований этики?

38. Каковы причины информационного риска?

39. Почему с точки зрения действующего законодательства программы для ЭВМ и базы данных являются объектами интеллектуальной собственности?

40. Какие информационные продукты обладают свойствами неделимости и неисключаемости из потребления?

41. Приведите примеры событий, в котором проявляется риск.

42. О чем говорит закон Мура?

43. Какая задача управления информационными рисками является невыполнимой?
44. С чем связано субъективное случайное событие?
45. Чему может способствовать управление цифровой идентичностью?
46. Каковы факторы информационного риска?
47. Какие произведения подлежат цитированию?
48. Что бы Вы отметили в качестве причин необходимости изучения этических вопросов, оглядываясь на историю развития ИТ?
49. Каковы основные этические понятия?
50. Что такое "службы Интернет"?
51. Что, по Вашему мнению, является наиболее важной задачей для повсеместного распространения этических норм в области ИТ?
52. Что происходит после истечения срока действия авторского права?
53. Что необходимо для получения авторского права?
54. Что такое этика?
55. Ведется ли работа по созданию единого кодекса (свода) правил для унификации понимания норм информационной этики?
56. Верно ли утверждение: "Информационный риск - это предопределенное событие, приводящее к негативным последствиям в информационной системе"?
57. Верно ли утверждение: "Информационный риск - это случайное событие, приводящее к негативным последствиям в информационной системе"?
58. Верно ли утверждение: "Риск - это возможность или вероятность наступления событий с отрицательными последствиями в результате определенных решений или действий"?
59. Верно ли утверждение: "Риск - это неотвратимое наступление события с отрицательными последствиями"?
60. Верно ли утверждение: "Риск - это событие с отрицательными последствиями в результате определенных решений или действий"?
61. Всегда ли является ли случаем правомерного использования произведения его цитирование?
62. Деловой репутации фирмы не может быть дана денежная оценка. Так ли это?
63. Имеют ли переводчики авторское право на выполненный ими перевод чужого произведения?
64. Имеют ли срок действия неимущественные права автора?
65. Как Вы думаете, исследует ли информационная этика информационные мифы?
66. Как Вы думаете, исследует ли информационная этика конфликты в области ИТ?
67. Как Вы думаете, исследует ли информационная этика права на личную жизнь и свободу слова применительно к области ИТ или это только дело общественно-политических организаций?

68. Как Вы думаете, исследует ли информационная этика проблемы защиты прав собственности и авторских прав или это область действия только юридических норм?
69. Как Вы думаете, исследует ли информационная этика проблемы, связанные с проявлениями компьютерных преступлений, или это область действия уголовного права?
70. Как Вы думаете, исследует ли информационная этика скрытые противоречия в информационных теориях и методах?
71. Как Вы думаете, исследует ли информационная этика создание новых структур власти в области ИТ?
72. Может ли быть дана денежная оценка авторскому праву?
73. Может ли иметь отрицательные последствия применение геопространственных и навигационных технологий (например, возможность отслеживания местонахождения)?
74. Может ли информационный риск быть одновременно прямым и косвенными?
75. Относится ли к информационной этике воздействие информационных технологий на общество?
76. Относится ли к информационной этике воздействие информационных технологий на окружающую среду?
77. Относится ли к информационной этике воздействие информационных технологий на решение этических проблем связанных с функционированием цифровых СМИ?
78. Охраняются ли авторским правом идеи, концепции, принципы?
79. Охраняются ли авторским правом методы и способы?
80. Охраняются ли авторским правом составные произведения (сборники)?
81. Очевидно, что деловая информация есть предмет рыночных отношений. А является ли информация для специалистов таким же предметом рыночных отношений?
82. Платность информационных продуктов и услуг - это опасность массового производства дешевых услуг ухудшенного качества. Не согласны?
83. Платность информационных продуктов и услуг - это понимание реальной ценности информации. Не согласны?
84. Согласны ли Вы с утверждением, что авторское право в РФ включает также международные соглашения, в которых участвует РФ?
85. Согласны ли Вы с утверждением, что высокая степень государственного регулирования не является особенностью рынка информации?
86. Согласны ли Вы с утверждением, что информационная деятельность является одним из важнейших элементов рыночной инфраструктуры, но не является самостоятельным сектором рынка?
87. Согласны ли Вы с утверждением, что назначение произведения не влияет на его охраноспособность?
88. Согласны ли Вы с утверждением, что способ выражения произведения

влияет на его охраноспособность?

89. Согласны ли Вы с утверждением, что среди основных тенденций информационного рынка одновременно присутствуют снижение цен и рост спроса?

90. Согласны ли Вы с утверждением, что художественные достоинства произведения влияют на его охраноспособность?

91. Товарному знаку не может быть дана денежная оценка. Так ли это?

92. Экстерналией рынка информации является повышенный конкурс в высшие учебные заведения по направлениям, связанным с информационными технологиями. Так ли это?

93. Является ли информационная деятельность самостоятельным и специализированным сектором рынка?

94. Является ли необходимостью использование экономических характеристик (таких как цена, стоимость, издержки, прибыль) применительно к информационным ресурсам, которые относятся к нематериальным ресурсам?

95. Является ли случаем правомерного использования произведения в качестве иллюстраций в изданиях, звуко- и видеозаписях в объеме, оправданном поставленной целью?

96. Является ли случаем правомерного использования произведения в качестве иллюстраций в изданиях, звуко- и видеозаписях учебного характера в объеме, оправданном поставленной целью?

97. Является ли случаем правомерного использования произведения его репродуцирование в единичном экземпляре без извлечения прибыли в учебных и исследовательских работах, для проведения аудиторных занятий?

98. Является ли случаем правомерного использования произведения его репродуцирование в единичном экземпляре без извлечения прибыли?

99. Является ли случаем правомерного использования произведения его цитирование в объеме, оправданном целью цитирования?

100. Являются ли объектами авторского права государственные символы и знаки (например, флаги, гербы, ордена или денежные знаки)?

101. Являются ли объектами авторского права информационные сообщения о событиях и фактах?

102. Являются ли объектами авторского права официальные документы (например, законы или судебные решения)?

103. Являются ли объектами авторского права произведения народного творчества?

**Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.*

**Методические указания для обучающихся по освоению дисциплины
(модуля)**

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО
ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**«ГУМАНИТАРНЫЕ АСПЕКТЫ (ПРОФЕССИОНАЛЬНАЯ ЭТИКА)
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Общие положения

Целями изучения дисциплины является:

1. Ускоренная адаптация студентов в предметную область информационная безопасность (защита интеллектуальной собственности), опираясь на весь спектр научных воззрений, на развитие и правовую защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации;
2. Повысить уровень правовых знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
3. Изучение правовых основ информационной безопасности и информирование студентов о законодательных источниках, подзаконных и ведомственных правовых актах обеспечивающих информационную безопасность личности, общества и государства;
4. Формирование у студентов специализированной базы знаний по основным понятиям в области правовой защиты информации и охраны интеллектуальной собственности;
5. Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации и охраны интеллектуальной собственности на предприятиях и в организациях.

Задачи дисциплины:

1. Теоретические основы обеспечения защиты интеллектуальной собственности на основе действующего российского законодательства с помощью с помощью современных принципов, методов, сил и средств в различных организационных структурах;
2. Практические аспекты правовой защиты интеллектуальной собственности по базовым направлениям защиты государственной, профессиональной, коммерческой тайны и конфиденциальной информации и формированием у обучающихся системы знаний.

2. Указания по проведению практических занятий

Тема 1. Правовые основы обеспечения информационной безопасности **Практическое занятие 1.**

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области информационной безопасности

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;
2. необходимость правовой защиты продуктов творческой деятельности

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
- б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1. Основные угрозы информационной безопасности РФ.
2. Правовые режимы распространения информации в исключительных ситуациях, представляющих угрозу безопасности РФ.
3. Совершенствование правового регулирования информационной безопасности.

Продолжительность занятия – 2/1 ч.

Тема 2. Понятие и состав информационных систем и прав на них

Практическое занятие 2.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;
2. интеллектуальное право как право на результаты интеллектуальной деятельности

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
- б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1. Законодательная основа защиты государственной тайны.

2. Обеспечение защиты государственной тайны.
3. Нормативное регулирование оборота сведений, составляющих государственную тайну, в системе МВД РФ.
4. Уголовно – правовая защита сведений, составляющих государственную тайну.

Продолжительность занятия – 2/1 ч.

Тема 3. Институт правовой охраны программ для ЭВМ и баз данных

Практическое занятие 3.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;
2. исторические истоки патентного права

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
- б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1. Понятие и состав информационных систем.
2. Территориальные и ведомственные уровни формирования единого информационного пространства.
3. Правовая охрана и защита прав на информационно – телекоммуникационные системы.
4. Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы.

Продолжительность занятия – 2/1 ч.

Тема 4. Институт правовой защиты тайны частной жизни и персональных данных

Практическое занятие 4.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;
2. объекты и субъекты промышленной собственности и патентного права

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
- б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (со доклад).

Учебные вопросы:

- 1.Тенденции усиления борьбы с компьютерными преступлениями на международном уровне.
 2. Основные положения общеевропейской Конвенции о киберпреступности.
 3. Информационные и компьютерные преступления.
 4. Термины и понятия связанные с правоотношениями в компьютерной сфере.
 5. Криминалистическая характеристика компьютерных преступлений.
- Продолжительность занятия – 2/1 ч.

Тема 5. Основные объекты интеллектуальной собственности и их правовая защита

Практическое занятие 5.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;
2. оформление прав патентообладателя

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.

б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1. Понятие и история правовой охраны программ для ЭВМ и баз данных.

2. Основные положения четвертой части Гражданского кодекса РФ, касающейся правовой охраны программ для ЭВМ и баз данных.

3. Выявление контрафакции программного обеспечения.

Продолжительность занятия – 2/1 ч.

Тема 6. Институт правовой защиты авторских и смежных прав Практическое занятие 6.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;

2. оформление прав патентообладателя (заявка на изобретение).

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1. Международные нормативные правовые акты.

2. Российские официальные документы и нормативные правовые акты.

3. Понятие средств индивидуализации юридических лиц, товаров, работ, услуг и предприятий.

4. Современное правовое регулирование отношений в области охраны средств индивидуализации.

5. Действие в России международных правовых актов по охране средств индивидуализации.

Продолжительность занятия – 2/1 ч.

Тема 7. Институт правовой защиты изобретений, полезных моделей и промышленных образцов Практическое занятие 7.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;
2. оформление прав патентообладателя (заявка на полезную модель и на промышленный образец).

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
- б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1. Понятие коммерческой тайны и ее генезис. 2. Действующие нормативно – правовые акты, устанавливающие требования по защите коммерческой тайны.

3. Основные положения Федерального закона « О коммерческой тайне».

4. Основные положения части четвертой Гражданского кодекса РФ, касающейся защиты коммерческой тайны.

5. Ответственность, связанная с нарушением законодательства о коммерческой тайне.

6. Зарубежный опыт правовой защиты коммерческой тайны.

Продолжительность занятия – 2/3 ч.

Тема 8. Институт правовой охраны наименований и товарных знаков (средств индивидуализации юридических лиц, товаров, работ, услуг и предприятий)

Практическое занятие 8.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;
2. объем правовой охраны предоставляемый патентом.

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
- б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1. Понятие результатов интеллектуальной деятельности, средств индивидуализации и иных объектов, созданных в результате деятельности, приравненной к интеллектуальной деятельности.
 2. Защита интеллектуальных прав. Понятие и генезис авторских и смежных прав.
 3. Современное правовое регулирование авторских прав.
 4. Интеллектуальные права авторов произведений литературы, науки и искусства.
 5. Правовая защита смежных прав. Ответственность за нарушение авторских и смежных прав.
 6. Понятие патентного права.
 7. Характеристика объектов патентного права.
 8. Патент как форма охраны объектов патентного права.
 9. Генезис авторских и смежных прав.
 10. Передача исключительного права на изобретения, полезные модели и промышленные образцы.
 11. Защита прав авторов и патентообладателей.
 12. Участие России в работе международных организаций по защите прав авторов и патентообладателей.
- Продолжительность занятия – 2/3 ч.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Тема 5. Профессиональная ответственность и профессиональная этика при работе с информационными технологиями	<i>Подготовка докладов по темам:</i> 1. Интеллектуальная промышленная собственность и патентное право; 2. основные принципы и приемы инженерного творчества; 3. Защита субъекта профессиональной деятельности в процессе его труда.
2.	Тема 6. Сущность информационных рисков и управление ими	<i>Подготовка докладов по темам:</i> 1. Объекты и субъекты промышленной собственности. 2. Оформление прав правообладателя. 3. Объем правовой охраны, представляемый

		патентом.
3	Тема 7. Интеллектуальная собственность	Подготовка докладов по темам: 1. Неалгоритмизированные методы инженерного творчества. 2. Алгоритмизированные методы инженерного творчества. 3. Инженер как субъект труда и жизни.
4	Тема 8. Частная жизнь и гражданские свободы в информационном обществе	Подготовка докладов по темам: 1. Виды и ступени инженерного творчества. 2. Интеллектуальное право на результаты интеллектуальной деятельности.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы «раскрыть», «определить», «установить», «показать», «выявить» и т.д.

3. Основная часть работы включает 2-4 вопроса, каждый из которых посвящается решению задач, сформированных во введении, и заканчивается констатацией итогов.

4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

5. Необходимо давать ссылки на используемую литературу.

6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

7. Вслед за заключением идет список литературы, который должен быть составлен и оформлен с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объем контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4. Примерная тематика контрольных работ:

1. История развития компьютеров, программного обеспечения, Интернет.
2. Основные этапы становления глобальной сети Интернет.
3. Информационное общество.
4. Влияние информационных технологий на социальные процессы.
5. Общественные ценности и законы этики; сущность профессионализма.
6. Этические проблемы формирования глобального информационного общества.
7. Социальные аспекты разработки и внедрения информационных технологий.
8. Виртуальная (информационная) этика: предмет, регулируемые отношения, сферы.
9. Оценка аспектов профессиональной деятельности с позиций этики.
10. Международное право в области информационных технологий.
11. Этические кодексы и их осуществление на практике (IEEE, ACM, SE, AITP и др.)
12. Национальный кодекс деятельности в области информатики и телекоммуникаций: ценностное основание.
13. Этические и законодательные основы личной безопасности в киберпространстве.
14. Основы интеллектуальной собственности.
15. Конфиденциальность персональной информации в базах данных и хранилищах.
16. Свобода самовыражения в киберпространстве.
17. Влияние информационных технологий на интернациональность культуры.
18. Риски, связанные с применением компьютерных систем.
19. Свобода самовыражения в киберпространстве.
20. Киберпространство: содержание, виды, их сходство и различие.
21. Преимущества и недостатки Интернета в сравнении с другими средствами массовой информации и коммуникации.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Гальперин, Михаил Владимирович.

Электротехника и электроника : Учебник. - 1. - Москва ; Москва :

Издательство "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2016. - 480 с. - ISBN 9785911347833. - Электронная программа (визуальная).

Электронные данные : электронные.

URL: <http://znanium.com/go.php?id=553180>

2.Куприянов, А.И.

Радиоэлектронная борьба. - 5-е изд. - Москва : Вузовская книга, 2018. - 360 с. : ил. - ISBN 978-5-9502-0833-1. - Текст (визуальный) : непосредственный.

Дополнительная литература:

3.Башлы, П. Н.

Информационная безопасность и защита информации. - Москва :

Издательский Центр РИОР, 2013. - 222 с. - ISBN 9785369011782. -

Электронная программа (визуальная). Электронные данные : электронные.

URL: <http://znanium.com/go.php?id=405000>

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.

2. <http://informika.ru/> – образовательный портал

3. www.wikIsec.ru - Энциклопедия информационной безопасности.

– Публикации, статьи.

4. www.biblioclub.ru - Универсальная библиотека онлайн

5. www.rucont.ru - ЭБС «Рукопт».

6. <http://www.academy.it.ru/> – академия АЙТИ.

7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации

8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации.

9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности

10. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному Контролю

11. Система ведения учебного процесса по дисциплине через Интернет -<http://elearning.tstu.tver.ru>

12. Общесистемное программное обеспечение Microsoft Windows 7/Windows 8, Microsoft Internet Explorer 10+, Microsoft Office 2007/2010/2013

8. Перечень информационных технологий

Перечень программного обеспечения: *MSoftware, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета.
2. Информационно-справочные системы (Консультант+; Гарант).
3. Рабочая программа и методическое обеспечение по курсу «Гуманитарные аспекты (профессиональная этика) информационной безопасности».