



Государственное бюджетное образовательное учреждение высшего образования  
Московской области

# ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



«УТВЕРЖДАЮ»

Проректор по учебно-методической работе

Н.В. Бабина

«28» апреля 2020 г.

**ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ**

**ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ  
И ТЕХНОЛОГИЙ**

**КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**РАБОЧАЯ ПРОГРАММА**

**ДИСЦИПЛИНЫ**

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

**Направление подготовки: 10.03.01 Информационная безопасность**

**Профиль: Информационно-аналитические системы  
финансового мониторинга**

**Квалификация (степень) выпускника: бакалавр**

**Форма обучения: очная**

Королев  
2020

**Автор:** к.в.н., доцент Сухотерин А.И. Рабочая программа дисциплины: «Гуманитарные аспекты (профессиональная этика) информационной безопасности». – Королев МО: «Технологический университет», 2020.

**Рецензент:** к.в.н., доцент Соляной В.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 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 (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания кафедры	Протокол № 8 от 26.03. 2020			

**Рабочая программа согласована:**

**Руководитель ОПОП ВО**



к.в.н., доцент Воронов А.Н.

**Рабочая программа рекомендована на заседании УМС:**

Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания УМС	№ 7 от 28.04.2020			

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

**Целью** освоения 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.

**Задачами** освоения 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:

### **Общепрофессиональные компетенции:**

- ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;
- ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

### **Профессиональные компетенции:**

- ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
- ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

После завершения освоения данной дисциплины студент должен:

### **Знать:**

- основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ;
- характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ РФ, ФСКЭК в данной области;
- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;
- правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;
- правовые нормы и стандарты по лицензированию в области обеспечения государственной тайны и сертификации средств защиты информации;
- правовые основы деятельности подразделений защиты информации;
- основы правового регулирования взаимоотношений администрации и персонала предприятия любой формы собственности в области защиты информации;
- меры гражданско – правовой, уголовной, административной и дисциплинарной ответственности за разглашение защищаемой информации и нарушение правил ее защиты и условия применения этих мер.
- назначение и место правовой защиты информации в реализации комплексной системы защиты информации;
- отрасли права, обеспечивающие правовое регулирование в сфере защиты информации и охраны интеллектуальной собственности;
- институты правовой защиты государственной служебной, коммерческой тайны и информации персонального характера;
- правовые основы федерального информационного ресурса, отнесенного к государственной тайне, ресурса субъектов федерации, юридических и физических лиц;
- роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ.

### **Уметь:**

- использовать в практической деятельности правовые знания;
- анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в

профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав;

- пользоваться нормативными документами по защите информации.

#### **Владеть:**

- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- навыками поиска нормативной правовой информации для профессиональной деятельности;
- правовыми основами защиты государственной, коммерческой, служебной, процессуальной, профессиональной тайны и информации персонального характера;
- методами гражданско-правового регулирования отношений, возникающих в связи с созданием и использованием объектов интеллектуальной собственности;
- содержанием законодательных и иных нормативно-правовых актов, регулирующих деятельность государственных органов, должностных лиц, общественных организаций и граждан в сфере обеспечения защиты информации и охраны интеллектуальной собственности;
- мерами гражданско-правовой, уголовной, административной и дисциплинарной ответственности за разглашение защищаемой информации и нарушение правил ее защиты и условия применения этих мер;
- порядком разрешения гражданско-правовых споров, возникающих в связи с нарушением исключительных прав владельцев объектов интеллектуальной собственности;
- законодательными основами организации защиты государственной тайны, правовыми нормами и стандартами по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;
- методами правового обеспечения информационной безопасности РФ и основными направлениями его совершенствования.

## **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», профиль: «Информационно-аналитические системы финансового мониторинга».



Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Основы управления в корпорациях», «Системный анализ в области информационной безопасности» и компетенциях: ОК-4,5,8, ОПК-2,4,5 и ПК-2,6,8,9,10,15.

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

### 3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 2 зачетные единицы, 72 часа.

Таблица 1

Виды занятий	Всего часов	Семестр 6	Семестр 7	Семестр ...	Семестр ...
<b>Общая трудоемкость</b>	72	72			
<b>ОЧНАЯ ФОРМА ОБУЧЕНИЯ</b>					
<b>Аудиторные занятия</b>	32	32			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	-	-			
<b>Самостоятельная работа</b>	40	40			
<b>КСР</b>	-	-			
<b>Курсовые работы (проекты)</b>	-	-			
<b>Расчетно-графические работы</b>	-	-			
<b>Контрольная работа, домашнее задание</b>	+	+			
<b>Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.</b>	T1; T2	T1; T2			
<b>Вид итогового контроля</b>	Зачет	Зачет			

## 4. Содержание дисциплины

### 4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. очное	Практические занятия, час. очное	Занятия в интерактивной форме, час. очное	Код компетенций
1	2	3	4	5
Тема 1. Предмет и задачи курса. Основы информационной этики	2	2	1	ОПК-5,7; ПК-4,10.
Тема 2. История информационных технологий	2	2	1	ОПК-5,7; ПК-4,10.
Тема 3. Влияние информационных технологий на социальные процессы	2	2	1	ОПК-5,7; ПК-4,10.
Тема 4. Анализ этических проблем и норм при формировании глобального информационного общества	2	2	1	ОПК-5,7; ПК-4,10.
Тема 5. Профессиональная ответственность и профессиональная этика при работе с информационными технологиями	2	2	1	ОПК-5,7; ПК-4,10.
Тема 6. Сущность информационных рисков и управление ими	2	2	1	ОПК-5,7; ПК-4,10.
Тема 7. Интеллектуальная собственность	2	2	1	ОПК-5,7; ПК-4,10.
Тема 8. Частная жизнь и гражданские свободы в информационном обществе	2	2	2	ОПК-5,7; ПК-4,10.
<b>Итого:</b>	16	16	9	

### 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. Чубукова С.Г., Элькин В.Д. Основы правовой информатики (юридические и математические вопросы информатики: Учебное пособие. Изд. Второе, исправленное, дополненное. – М.: Юридическая фирма «КОНТРАКТ», ИНФРА – М, 2010, - 287 с. – (Высшее образование).
2. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. Технические средства и методы защиты информации. Учебное пособие для вузов. -4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.
3. Коваленко Ю.Ю. Правовой режим лицензирования и сертификации в сфере информационной безопасности. Учебное пособие. – М. Горячая линия – Телеком, 2012.

### **Дополнительная литература:**

1. В.А. Тихонов, В.В. Райх. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. - М.: Гелиос АРВ, 2006.
2. Афанасьев А.А., Веденньев Л.Т. и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009.
3. Демущкин А.С. Документы и тайна. – М., ООО «Городец-издат», 2003. – 400 с.
4. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
5. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.
6. Тихонов В.А., Райх В.В., Информационная безопасность: концептуальные, правовые. Организационные и технические аспекты.: Учебное пособие. -М.: Гелиос АРВ, 2006. -528 с., ил. с.171.
7. Ищейнов В.Я., Мещатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).

### **Рекомендуемая литература:**

1. Ищейнов В.Я., Мещатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009.
2. А.Ф. Чепига. Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010.
3. Яковец Е. Н.. Правовые основы информационной безопасности Российской Федерации: учебное пособие. – М.: Юрлитинформ, 2010. – 336 с.
4. Яковец Е. Н.. Основы правовой защиты информации и интеллектуальной собственности: учебное пособие. – М.: Юрлитинформ, 2010. – 400 с.
5. Федеральный закон от 27 июля 2006 г. №149 «Об информации, информационных технологиях и о защите информации».
6. Федеральный закон от 29 июля 2004 г. № 98-ФЗ (с изменениями и дополнениями от 2 февраля 2006 года № 19-ФЗ; от 24 июля 2007 года № 244 – ФЗ) « О Коммерческой тайне».
7. Федеральный закон от 27 июля 2006 г. № 152 – ФЗ «О персональных данных».
8. Указ Президента РФ от 09 сентября 2000 г. «Доктрина информационной безопасности Российской Федерации».
9. Указ Президента РФ от 16 августа 2004 г. № 1085 « Вопросы Федеральной Службы по техническому и экспортному контролю».
10. Указ Президента РФ от 06 марта 1997 г. № 188 « Об утверждении перечня сведений конфиденциального характера».

11. Постановление Правительства РФ от 17 ноября 2007 г. №781 « Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

12. Постановление Правительства РФ от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»

13. Постановление Правительства РФ от 15 августа 2006 г. № 532 « О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

14. РД «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» 2002 г.

15. РД «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР - К)» 2002 г.

#### **Электронные книги:**

1. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. Технические средства и методы защиты информации. Учебное пособие для вузов.: -4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.

<http://biblioclub.ru/index.php?page=book&id=253208&sr=1>

2. Минаев В.А. и др. Правовое обеспечение информационной безопасности. -М.: Маросейка, 2008.

<http://biblioclub.ru/index.php?page=book&id=96249&sr=1>

3. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности. Учебное пособие. – М. Горячая линия – Телеком, 2012.

<http://biblioclub.ru/index.php?page=book&id=253538&sr=1>

4. Курило А.П. Обеспечение информационной безопасности бизнеса. М.: Альпина Паблишерз, 2011

[http://biblioclub.ru/index.php?page=book\\_view&book\\_id=235577](http://biblioclub.ru/index.php?page=book_view&book_id=235577)

5. Организационная защита информации: учебное пособие для вузов. М.: Флинта, 2011

[http://biblioclub.ru/index.php?page=book\\_view&book\\_id=93343](http://biblioclub.ru/index.php?page=book_view&book_id=93343)

#### **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.wikIsec.ru](http://www.wikIsec.ru) - Энциклопедия информационной безопасности. – Публикации, статьи.

4. [www.biblioclub.ru](http://www.biblioclub.ru) - Универсальная библиотека онлайн
5. [www.rucont.ru](http://www.rucont.ru) - ЭБС «Руконт».
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:**
  1. Ресурсы информационно-образовательной среды МГОТУ.
  2. Рабочая программа и методическое обеспечение по дисциплине: «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.

***ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ***

***ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ  
И ТЕХНОЛОГИЙ***

***КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ***

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

**«ГУМАНИТАРНЫЕ АСПЕКТЫ (ПРОФЕССИОНАЛЬНАЯ ЭТИКА)  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»  
(Приложение 1 к рабочей программе)**

**Направление подготовки: 10.03.01 Информационная безопасность**

**Профиль: Информационно-аналитические системы  
финансового мониторинга**

**Квалификация (степень) выпускника: бакалавр**

**Форма обучения: очная**

Королев  
2020

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

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности	Темы 1,2,5,6,7		определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам	профессиональной терминологией в области информационной безопасности
2.	ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Темы 1,2,3,4,5,6,7		пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет	
3.	ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности	Темы 1,2,3,4,7		использовать в практической деятельности правовые знания;	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;



		объекта защиты				
4.	ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартам в области информационной безопасности	Темы 1,4,5,6,7		реализовывать и контролировать выполнение требований по охране труда и технике безопасности в профессиональной деятельности;	навыками безопасного использования технических средств в профессиональной деятельности

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

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-5	Доклад в форме презентации	<p>А) полностью сформирована <b>5 баллов</b></p> <p>В) частично сформирована <b>3-4 балла</b></p> <p>С) не сформирована <b>2 балла</b></p>	<p>Проводится устно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <ol style="list-style-type: none"> <li>1.Соответствие представленной презентации заявленной тематике (1 балл).</li> <li>2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл).</li> <li>3.Владение информацией и способность отвечать на вопросы аудитории (1 балл).</li> <li>4.Качество самой представленной презентации (1 балл).</li> <li>5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).</li> </ol> <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.</p>
ОПК-7	Доклад в форме презентации	<p>А) полностью сформирована <b>5 баллов</b></p> <p>В) частично сформирована <b>3-4 балла</b></p> <p>С) не сформирована <b>2 балла</b></p>	<p>Проводится устно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <ol style="list-style-type: none"> <li>1.Соответствие представленной презентации заявленной тематике (1 балл).</li> <li>2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл).</li> <li>3.Владение информацией и способность отвечать на вопросы аудитории (1 балл).</li> </ol>

			<p>4.Качество самой представленной презентации (1 балл).</p> <p>5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).</p> <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.</p>
ПК-4	Доклад в форме презентации	<p>А) полностью сформирована <b>5 баллов</b></p> <p>В) частично сформирована <b>3-4 балла</b></p> <p>С) не сформирована <b>2 балла</b></p>	<p>Проводится устно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <p>1.Соответствие представленной презентации заявленной тематике (1 балл).</p> <p>2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл).</p> <p>3.Владение информацией и способность отвечать на вопросы аудитории (1 балл).</p> <p>4.Качество самой представленной презентации (1 балл).</p> <p>5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).</p> <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.</p>
ПК-10	Контрольная работа (домашнее задание)	<p>А) полностью сформирована <b>5 баллов</b></p> <p>В) частично сформирована <b>3-4 балла</b></p> <p>С) не сформирована <b>2 балла</b></p>	<p>1. Проводится устно в форме защиты отчета</p> <p>2.Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <p>1.Соответствие оформлению требованиям (1 балл).</p> <p>2. Соответствие разработанного устройства</p>

			<p>техническому заданию ( 1 балл)</p> <p>3. Моделирование работы разработанного устройства ( 1 балл)</p> <p>4. Качество и количество используемых источников ( 1 балл)</p> <p>5. Правильность и полнота ответов на контрольные вопросы ( 1 балл)</p> <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.</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:

- а. Самая важная и полезная для меня возможность, предоставляемая Интернет.
- б. Очень важная и полезная для меня возможность, предоставляемая Интернет.
- с. 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.
- c. Довольно бесполезная и ненужная для меня возможность, предоставляемая Интернет.
- d. Бесполезная и ненужная для меня возможность, предоставляемая Интернет.
- e. 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, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	ОПК-5 ОПК-7 ПК-4 ПК-10	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов.

						Хорошо - от 70%. Отлично – от 90%.
Согласно учебному плану	тестирование	ОПК-5 ОПК-7 ПК-4 ПК-10	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно учебному плану	Зачет	ОПК-5 ОПК-7 ПК-4 ПК-10	2 теоретических вопроса + практическое задание	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 15 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: <b>«Зачтено»:</b> <ul style="list-style-type: none"> <li>• знание основных понятий предмета;</li> <li>• умение использовать и применять полученные знания на практике;</li> <li>• работа на семинарских занятиях;</li> <li>• знание основных научных теорий, изучаемых предметов;</li> <li>• ответ на вопросы</li> </ul>

					билета. <b>«Не зачтено»:</b> <ul style="list-style-type: none"> <li>• демонстрирует частичные знания по темам дисциплин;</li> <li>• незнание основных понятий предмета;</li> <li>• не умеет использовать и применять полученные знания на практике;</li> <li>• не работал на семинарских занятиях;</li> </ul> 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?

***ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ***

***ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ  
И ТЕХНОЛОГИЙ***

***КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ***

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

**«ГУМАНИТАРНЫЕ АСПЕКТЫ (ПРОФЕССИОНАЛЬНАЯ ЭТИКА)  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»  
(Приложение 2 к рабочей программе)**

**Направление подготовки: 10.03.01 Информационная безопасность**

**Профиль: Информационно-аналитические системы  
финансового мониторинга**

**Квалификация (степень) выпускника: бакалавр**

**Форма обучения: очная**

## 1. Общие положения

**Целью изучения дисциплины является** 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;

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;

Изучение правовых основ информационной безопасности и информирование студентов о законодательных источниках, подзаконных и ведомственных правовых актах обеспечивающих информационную безопасность личности, общества и государства;

Формирование у студентов специализированной базы знаний по основным понятиям в области правовой защиты информации и охраны интеллектуальной собственности;

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:**

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;

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: *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 ч.

## **Тема 2. Понятие и состав информационных систем и прав на них** **Практическое занятие 2.**

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 ч.

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

#### **Практическое занятие 3.**

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 ч.

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

#### **Практическое занятие 4.**

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 (содоклад).

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 ч.

### **Тема 5. Основные объекты интеллектуальной собственности и их правовая защита** **Практическое занятие 5.**

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 ч.

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

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 ч.

## **Тема 7. Институт правовой защиты изобретений, полезных моделей и промышленных образцов**

### **Практическое занятие 7.**

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 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: *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 ч.

#### 4. Указания по проведению самостоятельной работы студентов

*Цель самостоятельной работы:* подготовить студентов к самостоятельному научному творчеству.

*Задачи самостоятельной работы:*

1) расширить представление в области существующих методов защиты интеллектуальной собственности;

2) привить навыки самостоятельного решения нестандартных задач в области нормативно-правового обеспечения защиты профессиональной тайны и интеллектуальной собственности в деятельности инженеров.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

#### Объем времени и виды самостоятельной работы

Виды самостоятельной работы	Очная форма обучения
	Всего академических часов
Всего часов на самостоятельную работу	40
Вопросы, выносимые на самостоятельное изучение	8
Подготовка к практическим занятиям	16
Подготовка докладов	8
Выполнение практических заданий	8

#### Вопросы, выносимые на самостоятельное изучение:

**для очной формы обучения:**

1. Интеллектуальная промышленная собственность и патентное право;
2. основные принципы и приемы инженерного творчества;
3. Защита субъекта профессиональной деятельности в процессе его труда.

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

#### Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
-------	-----------------------------	------------------	------------------

1.	Вопросы, выносимые на самостоятельное изучение	8	Изучение открытых источников
2.	Подготовка к практическим занятиям	16	Изучение открытых источников при подготовке доклада на выбранную тему.
4.	Тематика докладов	8	См. п.1-8
5.	Выполнение практических заданий	8	Выполнение расследования инцидента информационной безопасности в соответствии с нормативно-правовой базой документов

### **Примерные темы докладов**

1. Объекты и субъекты промышленной собственности.
2. Оформление прав правообладателя.
3. Объем правовой охраны, представляемый патентом.
4. Неалгоритмизированные методы инженерного творчества.
5. Алгоритмизированные методы инженерного творчества.
6. Инженер как субъект труда и жизни.
7. Виды и ступени инженерного творчества.
8. 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. Основная часть работы раскрывает процесс анализа заданной электрической цепи и должна содержать промежуточные и окончательные результаты расчетов, а также соответствующие временные или частотные диаграммы, поясняющие работу электрической цепи.
3. В процессе изложения материала необходимо давать ссылки на используемую литературу.
4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

### **5.3. Требования к оформлению**

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

### **6. Перечень основной и дополнительной учебной литературы**

#### **Основная литература:**

1 Чубукова С.Г., Элькин В.Д. Основы правовой информатики (юридические и математические вопросы информатики: Учебное пособие. Изд. Второе, исправленное, дополненное. – М.: Юридическая фирма «КОНТРАКТ», ИНФРА – М, 2010, - 287 с. – (Высшее образование).

2 А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. Технические средства и методы защиты информации. Учебное пособие для вузов.: -4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.

3 Коваленко Ю.Ю. Правовой режим лицензирования и сертификации в сфере информационной безопасности. Учебное пособие. – М. Горячая линия – Телеком, 2012.

#### **Дополнительная литература:**

1. В.А. Тихонов, В.В. Райх. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. - М.: Гелиос АРВ, 2006.

2. Афанасьев А.А., Веденньев Л.Т. и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009.

3. Демущкин А.С. Документы и тайна. – М., ООО «Городец-издат», 2003. – 400 с.

4. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.

5. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.

6. Тихонов В.А., Райх В.В., Информационная безопасность: концептуальные, правовые. Организационные и технические аспекты.: Учебное пособие. -М.: Гелиос АРВ, 2006. -528 с., ил. с.171.

7. Ищейнов В.Я., Мещатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).

8. Гражданский кодекс Российской Федерации: части первая, вторая, третья и четвертая : [офиц. текст : по состоянию на 5 сент. 2007 г.]. - Москва : Омега-Л, 2012. - 669 с.;

9. Этика и права человека в информационном обществе. Материалы Европейской региональной конференции. (Организована Комиссией

Франции по делам ЮНЕСКО и Советом Европы Страсбург), 13–14 сентября 2012 г.;

10. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – М.: Изд-во «Омега-Л», 2013;

11. Стратегия развития информационного общества в РФ (на период до 2015 года) (утверждена 7 февраля 2008 № пр-212) // Российская газета.– 2013. – 16 февраля. – № 4591;

12. Бабкин, Б.А. Интеллектуальная собственность в Интернет / Б.А. Бабкин. – М.: ЮрИнфоР, 2013. – 512 с.

13. Белл, Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / Перевод с английского. Изд. 2-ое, испр. и доп. – М.: Academia, 2014. - 788 с.

14. Дмитрик, Н.А. Осуществление субъективных гражданских прав с использованием сети Интернет/ Н.А. Дмитрик. – М.: Волтерс Клувер, 2006. – 200 с.;

15. Кибанов, А.Я. Этика деловых отношений: Учебник / А.Я. Кибанов, Д.К. Захаров, В.Г. Коновалова. – М.: Инфра-М, 2014. – 432 с.;

16. Землянова, Л.М. Коммуникативистика и средства информации: Англо-русский толковый словарь концепций и терминов / Л. М. Землянова. – М.: Изд-во Моск. ун-та, 2014. – 416 с.

#### **Рекомендуемая литература:**

1. Ищейнов В.Я., Мещатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009.

2. А.Ф. Чепига. Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010.

3. Яковец Е. Н.. Правовые основы информационной безопасности Российской Федерации: учебное пособие. – М.: Юрлитинформ, 2010. – 336 с.

4. Яковец Е. Н.. Основы правовой защиты информации и интеллектуальной собственности: учебное пособие. – М.: Юрлитинформ, 2010. – 400 с.

5. Федеральный закон от 27 июля 2006 г. №149 «Об информации, информационных технологиях и о защите информации».

6. Федеральный закон от 29 июля 2004 г. № 98-ФЗ (с изменениями и дополнениями от 2 февраля 2006 года № 19-ФЗ; от 24 июля 2007 года № 244 – ФЗ) « О Коммерческой тайне».

7. Федеральный закон от 27 июля 2006 г. № 152 – ФЗ «О персональных данных».

8. Указ Президента РФ от 09 сентября 2000 г. «Доктрина информационной безопасности Российской Федерации».

9. Указ Президента РФ от 16 августа 2004 г. № 1085 « Вопросы Федеральной Службы по техническому и экспортному контролю».

10. Указ Президента РФ от 06 марта 1997 г. № 188 « Об утверждении перечня сведений конфиденциального характера».

11. Постановление Правительства РФ от 17 ноября 2007 г. №781 « Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

12. Постановление Правительства РФ от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»

13. Постановление Правительства РФ от 15 августа 2006 г. № 532 « О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

14. РД «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» 2002 г.

15. РД «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР - К)» 2002 г.

## **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](http://www.wikIsec.ru) - Энциклопедия информационной безопасности.  
– Публикации, статьи.

4. [www.biblioclub.ru](http://www.biblioclub.ru) - Универсальная библиотека онлайн

5. [www.rucont.ru](http://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:** *MSOffice, Multisim.*

**Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине «Гуманитарные аспекты (профессиональная этика) информационной безопасности».