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**

**«ЗАЩИТА ОБЩЕСТВА ОТ ИНФОРМАЦИИ, ЗАПРЕЩЕННОЙ К РАСПРОСТРАНЕНИЮ»**

**Направление подготовки: 10.03.01 Информационная безопасность**

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

**Квалификация (степень) выпускника: бакалавр**

**Форма обучения: очная**

Королев
2020

**Автор: к.т.н. Журавлев С.И. Рабочая программа дисциплины: «Защита общества от информации, запрещенной к распространению». – 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 28.04.2020года.

**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 | | | |



2

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

**Целями изучения дисциплины является:**

1. обучение студентов принципам и средствам обеспечения информационной безопасности личности (сотрудников), коллективов (организационных структур предприятий) и в целом общества (предприятий);
2. получение студентами фундаментальных основ по формированию научного мировоззрения, развитию системного мышления и интеграции полученных ранее знаний по обеспечению информационной безопасности.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

**Профессиональные компетенции**:

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.

**Профессионально - специализированные компетенции:**

ПСК-3: способность участвовать в разработке информационно-аналитических систем финансового мониторинга.

**Основные задачи дисциплины** – дать основные знания, умения и навыки по вопросам обеспечения информационной безопасности личности (сотрудника), коллектива сотрудников (отделов, служб) и, в целом, всего коллектива предприятия как общества.

После завершения освоения данной дисциплины студент должен:

- ***Иметь представление:***

о целях, задачах, принципах, и основных направлениях обеспечения информационно-психологической безопасности;

о методологии организации обеспечения информационно-психологической безопасности предприятии;

о средствах и методах защиты человека и общества от противоправного информационно-психологического воздействия;

- ***Знать:***

роль и место информационно-психологической безопасности в системе информационной безопасности предприятия;

угрозы информационно-психологической безопасности коллектива и отдельных сотрудников предприятий;

содержание информационно-психологической войны, методы и средства ее ведения;

правовые основы обеспечения информационно-психологической безопасности;
информационные средства и технологии (информационно-психологическое оружие), негативно влияющие на здоровье;
способы и системы защиты от деструктивных воздействий;
средства и способы обеспечения информационно-психологической безопасности;

- ***Владеть (уметь):***

выбирать методы и средства защиты от негативных информационно-психологических воздействий;
пользоваться современными средствами защиты от негативных информационно-психологических воздействий;
применять полученные знания в сферах профессиональной деятельности;
выявлять попытки противоправного информационно-психологического воздействия, манипулирования и противодействовать им;
соблюдать правила информационно-психологической безопасности в быту и в служебной обстановке.

## 2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Защита общества от информации, запрещенной к распространению» относится к дисциплинам по выбору 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», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6, ОПК-2,4,6 и ПК-4,14.

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

## 3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетных единицы, 108 часов.

**Таблица1**

| Виды занятий | Всего часов | Семестр 6 | Семестр … | Семестр | Семестр |
|---|---|---|---|---|---|
| **Общая трудоемкость** | **108** | **108** | | | |
| **ОЧНАЯ ФОРМА ОБУЧЕНИЯ** | | | | | |
| **Аудиторные занятия** | 48 | 48 | | | |
| Лекции (Л) | 16 | 16 | | | |
| Практические занятия (ПЗ) | 16 | 16 | | | |
| Лабораторные работы (ЛР) | 16 | 16 | | | |
| **Самостоятельная работа** | 60 | 60 | | | |
| **КСР** | - | - | | | |
| **Курсовые работы (проекты)** | - | - | | | |
| **Расчетно-графические работы** | - | - | | | |
| **Контрольная работа, домашнее задание** | + | + | | | |
| **Текущий контроль знаний (7 - 8, 15 - 16 недели)** | Т1; Т2 | Т1; Т2 | | | |
| **Вид итогового контроля** | **Зачет с оценкой** | **Зачет с оценкой** | | | |

# 4. Содержание дисциплины

## 4.1.Темы дисциплины и виды занятий

**Таблица 2**

| Наименование тем | Лекции, час. Очное | Практические занятия, час. Очное | Лабораторные занятия, час. Очное | Занятия в интерактивной форме, час. Очное | Код компетенций |
|---|---|---|---|---|---|
| Тема 1. О стратегии государственной информационной политики России в условиях развития информационного общества. Ограничения на распространение информации запрещенной к распространению | **3** | **3** | **3** | **2** | ПК-4, ПСК-3 |
| Тема 2. Интернет - информация и ее правовое регулирование. Защита чести, достоинства и деловой репутации персонала предприятий | **3** | **3** | **3** | **2** | ПК-4, ПСК-3 |
| Тема 3. Неприкосновенность частной жизни граждан. Запрещенная информация и ее место в системе информационных отношений | **3** | **3** | **3** | **2** | ПК-4, ПСК-3 |
| Тема 4. Ограничение свободы распространения информации в целях противодействия экстремистской деятельности | **3** | **3** | **3** | **3** | ПК-4, ПСК-3 |
| Тема 5. Проблемы реализации конституционного права граждан на доступ к информации | **4** | **4** | **4** | **3** | ПК-4, ПСК-3 |
| **Итого:** | **16** | **16** | **16** | **12** | |

## 4.2. Содержание тем дисциплины

### Тема 1. О стратегии государственной информационной политики России в условиях развития информационного общества. Ограничения на распространение в СМИ информации запрещенной к распространению

Роль информации в социально-экономическом развитии страны. Цели и принципы государственной информационной политики. Стратегические приоритеты государственной информационной политики. Доступность информации. Содержательное разнообразие информации. Качество информации. Государственная информация и информационные ресурсы. Информационные ресурсы местного самоуправления. Информационная безопасность. Основные направления государственной информационной политики. Законодательная база. Экономическая политика. Социальная политика. Технологическая политика. Международное сотрудничество. Первоочередные меры по реализации государственной информационной политики. Принятие федеральных законов: «О государственной информационной политике», «О государственных информационных ресурсах, реестрах и регистрах», «Об обеспечении доступа граждан и организаций к информации о деятельности государственных органов и органов местного самоуправления», «Об электронном документообороте», «О персональных данных».

Нормы действующего федерального законодательства. Законодательство субъектов РФ. Проект федерального закона о защите нравственности. Правовое регулирование порнографии в США.

### Тема 2. Интернет информация и ее правовое регулирован Защита чести, достоинства и деловой репутации персонала предприятий.

Является ли Интернет средством массовой информации? Статья об «иных СМИ». Информационная безопасность. Правовое регулирование содержания сообщений. Нарушения авторского права. Нормативное регулирование. Обеспечение доказательств. Принудительное саморегулирование

Основные принципы и понятия. Опровержение. Право на ответ. Моральный вред

Деловая репутация. Извинение. Презумпция невиновности. Факт и мнение. Клевета и оскорбление. Освобождение от ответственности. Дело «"Нью-Йорк Таймс" против Салливана». Решения Европейского суда по правам человека

### Тема 3. Неприкосновенность частной жизни граждан. Запрещенная информация и ее место в системе информационных отношений.

Защита от несанкционированного проникновения в личную жизнь в КОСТИТУЦИОННОМ ПРАВЕ РФ. Реализация конституционных принципов

на защиту личной жизни в УГОЛОВНОМ ПРАВЕ РФ. Гарантии неприкосновенности частной жизни. Защита общественных интересов. Различия прав на личную жизнь и на честь и достоинство. Скрытая запись. Согласие на распространение сведений. Защита частной жизни в США.

Клевета: способы защиты. Свобода политической дискуссии. Факты и оценки. Защита рекламы. Различные типы СМИ. Лицензирование. Ограничение государственных монополий. Стадии информационного процесса. Доступ к информации.

### Тема 4. Ограничение свободы распространения информации в целях противодействия экстремистской деятельности

Право на защиту чести, достоинства и деловой репутации в системе субъективных гражданских прав. Компенсация морального вреда как способ защиты чести, достоинства и деловой репутации. Судебная защита чести, достоинства, деловой репутации. Судебная защита чести, достоинства, деловой репутации. Судебная защита чести, достоинства, деловой репутации.

Виды информации, причиняющей вред здоровью и развитию детей. Возрастные ограничения, зависящие, от характера допускаемой к обороту информации. Знаки, обозначающие категорию информационной продукции, в зависимости от возраста детей.

### Тема 5. Проблемы реализации конституционного права граждан на доступ к информации

Конституционные гарантии права граждан РФ на информацию. Конституционно - правовые гарантии свободы распространения информации в РФ. Международный опыт конституционно-правового регулирования доступа граждан к информации. Право граждан на доступ к правовой информации. Правовая информация: понятие, виды, социальная потребность. Гарантии прав граждан на доступ к информации о деятельности органов государственной власти. Право на информацию о деятельности органов государственной власти как фактор обеспечения участия в управлении государством. Правовое регулирование порядка распространения информации о деятельности органов государственной власти в РФ. Обеспечение открытости информации о деятельности органов государственной власти в рамках административной реформы.

## 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 «Защита общества от информации,

запрещенной к распространению» 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

4 Государственная информационная политика в условиях информационно-психологической войны. – 3-у издание, стереотип. Манойло А.М., Петренко А.И., Фролов Д.Б., - М.: Горячая линия – Телеком, 2013. – 542с.

5 Теория защиты информации. Малюк А.А. – М. Горячая линия – Телеком, 2013 -184с.

6 Концептуальные основы создания и применение системы защиты объектов. Ворона В.А., Тихонов В.А. –М.: Горячая линия – Телеком, 2013.-196с.


**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. Демушкин 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., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).

**Рекомендуемая литература:**

1. Ищейнов В.Я., Мецатунян 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**
5. Организационная защита информации: учебное пособие для вузов. М.: Флинта,2011
**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 - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн
5. **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. Методичские 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: «Защита общества от информации, запрещенной к распространению».

## 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.

**Приложение 1**

*ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ*

*ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ*

*КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

# «ЗАЩИТА ОБЩЕСТВА ОТ ИНФОРМАЦИИ, ЗАПРЕЩЕННОЙ К РАСПРОСТРАНЕНИЮ»

**(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. | ПК-4 | способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты. | Тема:1,3,4,5 | роль и место информационно-психологической безопасности в системе информационной безопасности предприятия, угрозы информационно-психологической безопасности коллектива и отдельных сотрудников предприятий | выбирать методы и средства защиты от негативных информационно-психологических воздействий; применять полученные знания в сферах профессиональной деятельности | пользоваться современными средствами защиты от негативных информационно-психологических воздействий |
| 2. | ПСК-3 | способность участвовать в разработке информационно-аналитических систем финансового мониторинга. | Тема:1,2,3,4 | содержание информационно-психологической войны, методы и средства ее ведения; информационные средства и технологии (информационно-психологическое оружие), негативно влияющие на здоровье; способы и системы защиты от деструктивных воздействий | выявлять попытки противоправного информационно-психологического воздействия, манипулирования и противодействовать им | выявлять попытки противоправного информационно-психологического воздействия, манипулирования и противодействовать им |

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

| | | | |
|---|---|---|---|
| | | | Максимальная сумма баллов - 5 баллов.<br>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал. |

## 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

### Примерная тематика доклада в форме презентации:

1. Законодательство Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.
2. Полномочия федерального органа исполнительной власти, органов государственной власти субъектов Российской Федерации в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию.
3. Виды информации, причиняющей вред здоровью и (или) развитию детей.
4. Секретность конфиденциальность, целостность и доступность информации. Основные свойства защищаемой информации при защите общества от информации, запрещенной к распространению.
5. Соотношение понятий «защита информации» и «информационная безопасность». Цель и задачи защиты информации, запрещенной к распространению.
6. Организационно — правовые принципы защиты общества от информации, запрещенной к распространению.
7. Понятие правовой защиты информации ее методов и способов. Правовое регулирование защиты информации.
8. Общая характеристика подзаконных и ведомственных нормативно – правовых актов, регулирующих защиту общества от информации, запрещенной к распространению.
9. Подзаконные, ведомственные и локальные правовые акты, действующие в сфере защиты информации, запрещенной к распространению.
10. Назначение и задачи подзаконных правовых актов, регулирующих процессы защиты персональных данных и коммерческой тайны.
11. Закрепление права предприятия на защиту информации в нормативных документах (коллективном договоре, трудовом договоре, иных локальных правовых актах организаций).
12. Понятие информации конфиденциального характера. Перечень сведений конфиденциального характера.
13. Правовая основа защиты информации, запрещенной к распространению.
14. Права и обязанности защищаемых лиц. Права и обязанности органов, обеспечивающих государственную защиту.
15. Правовые санкции за разглашение сведений о защищаемых лицах и мерах государственной защиты.
16. Конституционные гарантии права граждан РФ на информацию.

Конституционно - правовые гарантии свободы распространения информации в РФ.

17. Международный опыт конституционно-правового регулирования доступа граждан к информации. Право граждан на доступ к правовой информации.

18. Правовая информация: понятие, виды, социальная потребность. Гарантии прав граждан на доступ к информации о деятельности органов государственной власти.

19. Право на информацию о деятельности органов государственной власти как фактор обеспечения участия в управлении государством.

20. Правовое регулирование порядка распространения информации о деятельности органов государственной власти в РФ. Обеспечение открытости информации о деятельности органов государственной власти в рамках административной реформы.

## Примерная тематика заданий на контрольную работу:

1. Законодательство Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.

2. Полномочия федерального органа исполнительной власти, органов государственной власти субъектов Российской Федерации в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

3. Виды информации, причиняющей вред здоровью и (или) развитию детей.

4. Секретность, конфиденциальность, целостность и доступность информации. Основные свойства защищаемой информации при защите общества от информации, запрещенной к распространению.

5. Соотношение понятий «защита информации» и «информационная безопасность». Цель и задачи защиты информации запрещенной к распространению.

6. Организационно — правовые принципы защиты общества от информации, запрещенной к распространению.

7. Понятие правовой защиты информации, ее методов и способов. Правовое регулирование защиты информации.

8. Общая характеристика подзаконных и ведомственных нормативно – правовых актов, регулирующих защиту общества от информации, запрещенной к распространению.

9. Подзаконные, ведомственные и локальные правовые акты, действующие в сфере защиты информации запрещенной к распространению.

10. Назначение и задачи подзаконных правовых актов, регулирующих процессы защиты персональных данных и коммерческой тайны.

11. Закрепление права предприятия на защиту информации в нормативных документах (коллективном договоре, трудовом договоре, иных локальных правовых актах организаций).

12. Понятие информации конфиденциального характера. Перечень сведений конфиденциального характера.

13. Правовая основа защиты информации запрещенной к распространению.

14. Права и обязанности защищаемых лиц. Права и обязанности органов, обеспечивающих государственную защиту.

15. Правовые санкции за разглашение сведений о защищаемых лицах и мерах государственной защиты.

16. Конституционные гарантии права граждан РФ на информацию. Конституционно - правовые гарантии свободы распространения информации в РФ.

17. Международный опыт конституционно-правового регулирования доступа граждан к информации. Право граждан на доступ к правовой информации.

18. Правовая информация: понятие, виды, социальная потребность. Гарантии прав граждан на доступ к информации о деятельности органов государственной власти.

19. Право на информацию о деятельности органов государственной власти как фактор обеспечения участия в управлении государством.

20. Правовое регулирование порядка распространения информации о деятельности органов государственной власти в РФ. Обеспечение открытости информации о деятельности органов государственной власти в рамках административной реформы.

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

Формой контроля знаний по дисциплине «Защита общества от информации, запрещённой к распространению» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачёта с оценкой.

| 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 | ПК-4<br>ПСК-3 | 20 вопросов | Компьютерное тестирование ; время отведенное на процедуру - 30 минут | Результаты тестирования предоставляются в день проведения процедуры | Критерии оценки определяются процентным соотношением.<br>Не явка - Удовлетворительно - от 51% правильных ответов.<br>Хорошо - от 70%.<br>Отлично – от 90%. |
| Согласно учебному плану | тестирование | ПК-4<br>ПСК-3 | 20 вопросов | Компьютерное тестирование; время отведенное на процедуру – 30 минут | Результаты тестирования предоставляются в день проведения процедуры | Критерии оценки определяются процентным соотношением.<br>Не явка -0<br>Удовлетворительно - от 51% правильных ответов.<br>Хорошо - от 70%.<br>Отлично – от 90%.<br>Максимальная оценка – 5 баллов. |
| Согласно учеб- | Зачёт с оценкой | ПК-4<br>ПСК-3 | 3 вопроса | Зачёт с оценкой проводится в письменной | Результаты предоставляются в день | Критерии оценки:<br>«**Отлично**»:<br>• знание |

| | | | | | | |
|---|---|---|---|---|---|---|
| ному плану | | | | форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут. | проведения зачета с оценкой | основных понятий предмета;<br>• умение использовать и применять полученные знания на практике;<br>• работа на практических занятиях;<br>• знание основных научных теорий, изучаемых предметов;<br>• ответ на вопросы билета.<br>«**Хорошо**»:<br>• знание основных понятий предмета;<br>• умение использовать и применять полученные знания на практике;<br>• работа на практических занятиях;<br>• знание основных научных теорий, изучаемых предметов;<br>• ответы на вопросы билета<br>• неправильно решено практическое задание<br>«У**довлетворительно**»:<br>• демонстрирует частичные знания по темам дисциплин;<br>• незнание неумение использовать и применять полученные знания на практике;<br>• не работал на практических занятиях;<br>«**Неудовлетворительно**»:<br>• демонстри |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | рует частичные знания по темам дисциплин;<br>• незнание основных понятий предмета;<br>• неумение использовать и применять полученные знания на практике;<br>• не работал на практических занятиях;<br>• не отвечает на вопросы. |

### 4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

**1. С какой тайной связывают банковскую тайну?**

(!) Коммерческая тайна

(?) Государственная тайна

(?) Служебная тайна

(?) Тайна следствия и судопроизводства

**2. Какие операции не могут осуществляться при банковских отношениях?**

(?) Привлечение во вклады денежных средств физических и юридических лиц

(?) Открытие и ведение счетов физических и юридических лиц

(?) Размещение указанных средств от своего имени и за свой счет на условиях возврата

(!) Размещение указанных средств от своего имени и за свой счет

**3. Какова величина суммы застрахованного банковского вклада?**

(!) 1 млн. 400 тыс. руб.

(?) 800 тыс. руб.

(?) 100 тыс. руб.

(?) 150 тыс. руб.

**4. Основной законодательный акт, в котором определена Банковская Тайна?**

(?) Конституция РФ

(?) ФЗ. № 149 «Об информации, информационных технологиях и защите информации»

(!)ФЗ. № 395-1 «О Банках и Банковской деятельности»

(?) Доктрина ИБ

**5. Кредитная организация не вправе осуществлять…?**

(!) Лизинговые операции

(!) Оказание консультаций и информационных услуг

(!) Осуществление операций с драгоценными металлами и камнями в соответствии с законами

(?) Осуществление операций с драгоценными металлами и камнями

**6. В соответствии, с каким законом сотрудник подписывает документ о неразглашении?**

(?) Конституция РФ

(!) ФЗ. №86 «О ЦБ РФ»

(?) УК РФ

(?) ФЗ «О коммерческой тайне»

**7. В соответствии, с каким законом обеспечивается сохранность ПД при аудиторских проверках?**

(?) ФЗ. № 149 «Об информации, информационных технологиях и защите информации»

(?) ФЗ. №86 «О ЦБ РФ»

(?) ФЗ. № 395-1 «О Банках и Банковской деятельности»

(!) ФЗ. №107 «Об аудиторской деятельности»

**8. Кто занимается созданием центральной базы кредитных историй?**

(?) Вкладчик

(!) Бюро кредитных историй

(?) Специалист по ИБ

(?) Банк

**9. Кому не может быть предоставлен кредитный отчет?**

(?) Пользователь кредитной истории

(?) Субъекту кредитных историй

(?) В суд

(!) Родственникам

**10. Обязательно ли попадет кредитная история в центральное бюро кредитных историй?**

(!) Обязательно

(?) По желанию

(?) Не попадет

(?) Попадет через 5 лет

**11. В соответствии, с каким законом осуществляется страхование счетов?**

(?) ФЗ. №86 «О ЦБ РФ»

(?) ФЗ. № 395-1 «О Банках и Банковской деятельности»

(?) Конституцией РФ

(!) ФЗ. №177 «О страховых вкладах физических лиц в банковских орга-

низациях»

**12. Чем регламентируется работа бюро кредитных историй?**

(!) Законом о кредитных историях

(?) Конституцией РФ

(?) Уголовным кодексом

(?) Банком

**13. Кредитная история хранится в течении?**

(!) 15 лет с последнего изменения

(?) 16 лет с последнего изменения

(?) 10 лет с последнего изменения

(?) 5 лет с последнего изменения

**14. Что не входит в кредитную историю?**

(!) Сведения о месте работы

(?) ФИО

(?) Данные паспорта

(?) Индивидуальный номер налогоплательщика

**15. Правом на сохранение БТ не обладает?**

(!) Государство

(?) Доверитель

(?) Клиент

(?) Корреспондент

**16.Согласно закону РФ «Об авторском праве» автор это:**

(!) физическое лицо, творческим трудом которого создано произведение;

(?) юридическое лицо, творческим трудом которого создано произведение;

(?) физическое лицо, физическим трудом которого создано произведение;

(?) юридическое лицо, умственным трудом которого создано произведение.

**17. Авторское право это:**

(!) институт гражданского права, регулирующий отношения, связанные с созданием и использованием (изданием, исполнением, показом и т. д.) результатов творческой деятельности людей;

(?) институт гражданского права, регулирующий отношения, связанные с созданием и использованием (изданием, исполнением, показом и т. д.) периодических произведений;

(?) институт гражданского права, регулирующий отношения, связанные с разработкой нормативно правовой базы предприятий;

(?) институт уголовного права, регулирующий отношения, связанные с совершением преступных деяний.

**18. Что из перечисленного относится к смежным правам:**

(!) гражданские правоотношения тесно связанные с авторским правом, возникающие в ходе реализации исполнительных прав и прочих прав;

(?) гражданские правоотношения тесно связанные с авторским правом, возникающие в случае утери автором оригинала произведения;

(?) гражданские правоотношения тесно связанные с авторским правом, возникающие в ходе продажи авторских прав;

(?) юридические правоотношения не связанные с авторским правом.

**19. Что не является объектом авторского права:**

(?) фольклор;

(!) литературные произведения;

(!) музыкальные произведения;

(!) скульптуры.

**20. После смерти автора, авторское право защищается в течении:**

(!) 70 лет;

(?) 25 лет;

(?) 10 лет;

(?) 100 лет.

**21. К неделимому соавторству относится:**

(!) случаи, когда произведение образует неразрывное целое;

(?) случаи, когда созданное в соавторстве произведение состоит из частей, имеющих самостоятельное значение;

(?) случаи, когда произведение состоит из взаимозаменяемых частей;

(?) случаи, когда деление произведения не рассмотрено в договоре соавторов.

**22. Право на произведение, обнародованное под псевдонимом, действует в течении:**

(!) 70 лет;

(?) 100 лет;

(?) 25 лет;

(?) 10 лет.

**23. Правовому регулированию смежных прав посвящается:**

(!) часть 4 гражданского кодекса РФ;

(?) ФЗ №101 «Об авторском праве и смежных правах»;

(?) Постановление правительства РФ №93 «О смежных правах»;

(?) Указ президента РФ №60 «Перечень смежных прав».

**24. Право на отзыв это:**

(!) право позволяющее автору отказаться от ранее принятого решения об обнародовании произведения;

(?) право позволяющее другому лицу делать отзыв на произведение;

(?) право на составление отзыва на собственное произведение;

(?) право позволяющее автору отказаться от ранее принятого решения о составлении отзыва.

**25. Произведение считается обнародованным если:**

(!) в течении 30 дней после опубликования за пределами РФ оно было опубликовано на территории РФ;

(?) в течении 40 дней после опубликования за пределами РФ оно было опубликовано на территории РФ;

(?) после 10 дней поле опубликования в РФ;

(?) сразу после опубликования в РФ.

**26. К авторским правам не относятся:**

(!) специальное право;
(?) исключительное право;
(?) личные не имущественные права;
(?) иные права.

**27. К личным не имущественным правам не относится:**

(!) право на продажу произведения;
(?) право на обнародование произведения;
(?) право на имя;
(?) право авторства.

**28. К исключительному праву относятся:**

(!) право распространения;
(!) право публичного показа;
(?) право на отзыв;
(?) право на имя.

**29. К иным правам не относится:**

(!) право на издание;
(?) право на отзыв;
(?) право следования;
(?) право доступа.

**30. Авторское право действует на:**

(!) обнародованное произведение;
(!) необнародованное произведение;
(?) чужое произведение;
(?) федеральный закон.

**31. Определение коммерческой тайны в соответствии с ФЗ «О коммерческой тайне»:**

(!) Информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

(?) Информация, имеющая реальную или потенциальную ценность, в силу её неизвестности третьим лицам;

(?) Информация, которая может нанести ущерб, в случае её разглашения;

(?) Информация о деятельности коммерческой организации, которая может нанести непоправимый ущерб, в случае утечки.

**32. Конфиденциальная составляющая коммерческой тайны:**

(!) Конфиденциальная информация, отражающая следующие аспекты коммерческой деятельности: технические, экономические, организационные;

(?) Информация о коммерческой деятельности фирмы внутреннем и внешнем рынках;

(?) Информация об организационном порядке по работе с информацией конфиденциального характера;

(?) Персональные данные руководящего состава предприятия.

**33. Интеллектуальная составляющая коммерческой тайны:**

(!) Не обнародованные в официальном порядке результаты интеллектуальной деятельности: изобретения, полезные модели, промышленные образцы, оригинальные технологии, оригинальный набор информационных подходов;

(?) Обнародованные в официальном порядке результаты интеллектуальной деятельности: изобретения, полезные модели, промышленные образцы, оригинальные технологии, оригинальный набор информационных подходов;

(?) Документально зафиксированная информация об использовании и применении оригинальных технологий и подходов на предприятии;

(?) Часть коммерческой тайны, которая в явном виде не присутствует в перечне сведений, подразумевается.

**34. Кем и когда утверждён, перечень сведений конфиденциального характера:**

(!) Указ президента от 6 марта 1997 года №188;

(?) Постановление правительства от 5 декабря 2003 года № 89;

(?) Федеральный закон от 27 декабря 2002 года № 184-ФЗ;

(?) Федеральный закон от 28 декабря 2010 года № 390-ФЗ

**35. Назовите документ, связанный с защитой информации, составляющей коммерческую тайну, посвящённый требованиям и рекомендациям по технической защите конфиденциальной информации**

(!) «Специальные требования и рекомендации по защите конфиденциальной информации» решение президиума гостехкомиссии России № 7.2 от 2 марта 2001 года.

(?) Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации»;

(?) Федеральный закон № 98 «О коммерческой тайне»;

(?) Гражданский кодекс РФ часть 4.

**36. Какой нормативно - правовой акт регламентирует включение в договор с работодателем, условий о неразглашении охраняемой законом коммерческой тайны:**

(!) Трудовой кодекс РФ;

(?) Федеральный закон «О коммерческой тайне»;

(?) Гражданский кодекс РФ;

(?) Уголовный кодекс РФ.

**37. Каким документом определяются условия отнесения информации к сведениям, составляющим коммерческую тайну, обязанность соблюдения конфиденциальности такой информации, а так же ответственность за её разглашение:**

(!) Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации»;

(?) Гражданский кодекс РФ;

(?) Уголовный кодекс РФ;

(?) Федеральный закон № 98 «О коммерческой тайне».

**38. Каким нормативно-правовым актом определяется защита элементов коммерческой тайны, которые рассматриваются как объекты интеллектуальной деятельности:**

(!) Гражданский кодекс РФ от 18 декабря 2006 г. № 230-ФЗ часть 4. Глава 75 (право на секрет производства (ноу-хау));

(?) Федеральный закон «О коммерческой тайне»;

(?) Руководящий документ ФСТЭК «Специальные требования и рекомендации по защите конфиденциальной информации» (СТР-К)

(?) Уголовно-процессуальный кодекс РФ.

**39. Какие требования предъявляются к лицу-обладателю информацией, составляющей коммерческую тайну:**

(!) Оно владеет на законном основании; оно ограничивает доступ к информации, и установило режим коммерческой тайны в отношении этой информации;

(?) Оно является гражданином РФ; оно является законным держателем информации; оно обеспечивает защиту закрытой информации;

(?) Оно является юридическим лицом; оно установило режим конфиденциальной информации в отношении этой информации,

(?) Оно владеет информацией на законном основании; оно является гражданином РФ, проживающим на территории РФ не менее пяти лет; оно ограничило доступ к информации.

**40. Признаки информации, обретённой незаконно:**

(!) Получатель умышленно преодолевал меры по её охране; получатель знал, что получает информацию от лица, не имеющего право на её передачу получателю;

(?) Информация, так или иначе, имеет отношение к деловой активности конкретной фирмы;

(?) Информация, полученная из открытых источников;

(?) Плагиат.

**41. Каким законом определяется порядок предоставление информации, составляющей коммерческую тайну:**

(!) Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»

(?) Руководящий документ ФСТЭК «Специальные требования и рекомендации по защите конфиденциальной информации» (СТР-К)

(?) Федеральный закон № 149 « Об информации, информационных технологиях и о защите информации»;

(?) Федеральный закон № 98 «О коммерческой тайне».

**42. Дать определение контрагента в соответствии с ФЗ № 98 «О коммерческой тайне»:**

(!) Сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

(?) Сторона соглашения, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

(?) Обладатель информации;

(?) Лицо, которому стала известна информация, в силу исполнения им служебных обязанностей.

**43. Общие меры обеспечения соблюдения конфиденциальности информации:**

(!) Разработка перечня информации, ограничение и регламентирование доступа, разработка и регулирование правил по регулированию отношений, нанесение на документы грифа коммерческой тайны;

(?) Разработка и регулирование правил организации обращения с конфиденциальной информацией;

(?) Организация конфиденциального документооборота на предприятии;

(?) Заключение соглашения с сотрудниками по обработке конфиденциальной информации.

**44. Каких правил должен придерживаться работник при обработке информации конфиденциального характера:**

(!) Выполнять установленный режим защиты, не разглашать сведения, составляющие коммерческую тайну; после прекращения трудовых отношений, вернуть работодателю все документы, составляющие коммерческую тайну;

(?) Не разглашать сведения, составляющие коммерческую тайну; выполнять установленный режим защиты;

(?) Выполнять обязанности, согласно ФЗ № 149 «Об информации, информационных технологиях и о защите информации»;

(?) Выполнять требования инструкции по организации обработки конфиденциальной информации в организации.

**45. Срок действия права на секрет производства, с грифом коммерческая тайна:**

(!) Действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих коммерческую тайну в соответствии с гражданским кодексом РФ «Исключительное право на секрет производства» ст. 1467;

(?) Право на секрет производства с грифом коммерческая тайна не имеет срока давности;

(?) Право на секрет производства с грифом коммерческая тайна составляет тридцать календарных дней, с момента присвоения грифа;

(?) Действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих коммерческую тайну, согласно федеральному закону № 98;

**Кто утвердил перечень сведений конфиденциального характера № 188:**

(!)Президент.

(?)Премьер министр.

(?)ФСТЭК.

(?)ФСБ.

**46. Что понимается под мошенничеством, согласно статьи №159 УК РФ**

(!)Хищение имущества или приобретение права на чужое имущество путем злоупотребления доверием.

(?)Хищение имущества.

(?)Приобретение права на чужое имущество с помощью злоупотребления доверием.

(?)Получение имущества с помощью применения силы.

**47. К правовым методам защиты информации доктрина относит:**

(!)Разработка нормативно правовых актов, регламентирующих отношение в информационной сфере.

(?)Составление списка ответственных лиц.

(?)Указание по использованию физических средств ЗИ.

(?)Указание по использованию технических средств ЗИ.

**48. Сколько видов конфиденциальной информации существует в соответствии с указом президента №188 1997 года?**

(?)5.

(?)4.

(!)6.

(?)8.

**49. Врачебная тайна, адвокатская тайна, нотариальная тайна, тайна переписки. К какому виду конфиденциальной информации относятся перечисленные тайны?**

(?)Служебная тайна.

(?)Коммерческая тайна.

(?)Персональные данные.

(!)Профессиональная тайна.

**50. Субъектами банковской тайны являются:**

(!)Держатели.

(!)Кредитные организации.

(?)Вкладчики.

(?)Государство.

**51. Определение организационно-розыскной деятельности**

(!)Вид деятельности, осуществляющий по средствам ОРМ в целях защиты конституционных прав гражданина.

(?)Вид деятельности, направленный на безопасность общества, государства, личности.

(?)Вид деятельности, осуществляющийся по средства ОРМ в целях раскрытия инцидентов нарушения ИБ.

**52. Какие сведения относятся к информации конфиденциального характера**

(!)Сведения о возможных природных бедствиях.

(?)Информация, составляющая тайну следствия.

(?)Сведения, связь с профессиональной деятельностью.

(?)Сведения, связь с коммерческой деятельностью.

**53. Информация, составляющая коммерческую тайну:**

(?)Товарные знаки.

(?)Авторское право.

(?)Государственная тайна.

(!)Банковская тайна.

**54. Чем охраняется информация, ограниченного доступа?**

(!)Федеральными законами.

(?)Ведомственными приказами.

(?)Силовыми структурами (ведомствами).

**55. За разглашение сведений конфиденциального характера наступает ответственность:**

(?)Уголовная.

(?)Административная.

(?)Дисциплинарная.

(!)Все вышеперечисленные.

**56. С правовой точки зрения защите подлежит:**

(?)Любая закрытая информация.

(!)Информация, зафиксированная на материальном носителе.

(?)Любая коммерческая тайна.

(?)Всё вышеперечисленное.

### 4.2. Типовые вопросы, выносимые на зачёт с оценкой

1. Законодательство Российской Федерации о защите персонала от информации, причиняющей вред их здоровью и (или) развитию.
2. Полномочия федерального органа исполнительной власти, органов государственной власти субъектов Российской Федерации в сфере зашиты персонала от информации, причиняющей вред их здоровью и (или) развитию.
3. Виды информации, причиняющей вред здоровью и (или) развитию персонала.
4. Осуществление классификации информационной продукции.
5. Общие требования к обороту информационной продукции.
6. Знак информационной продукции.

7. Дополнительные требования к распространению информационной продукции посредством теле- и радиовещания.
8. Дополнительные требования к распространению информации посредством информационно-телекоммуникационных сетей.
9. Дополнительные требования к обороту отдельных видов информационной продукции для детей.
10. Дополнительные требования к обороту информационной продукции, запрещенной для персонала.
11. Общие требования к экспертизе информационной продукции.
12. Экспертное заключение.
13. Правовые последствия экспертизы информационной продукции.
14. Государственный надзор и контроль за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.
15. Общественный контроль в сфере защиты персонала от информации, причиняющей вред их здоровью и (или) развитию.
16. Ответственность за правонарушения в сфере защиты персонала от информации, причиняющей вред их здоровью и (или) развитию.
17. ФЗ № 252 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»»
18. Стадии информационного процесса. Доступ к информации.
19. Нормы действующего федерального законодательства.
20. Законодательство субъектов РФ.
21. Проект федерального закона о защите нравственности.
22. Правовое регулирование порнографии в США
23. Нормативное регулирование. Обеспечение доказательств. Принудительное саморегулирование
24. Презумпция невиновности. Факт и мнение.
25. Клевета и оскорбление. Освобождение от ответственности.
26. Защита от несанкционированного проникновения в личную жизнь в КОСТИТУЦИОННОМ ПРАВЕ РФ.
27. Реализация конституционных принципов на защиту личной жизни в УГОЛОВНОМ ПРАВЕ РФ.
28. Гарантии неприкосновенности частной жизни.
29. азличия прав на личную жизнь и на честь и достоинство.
30. Скрытая запись. Согласие на распространение сведений.
31. Защита частной жизни в США.
32. Государственная информация и информационные ресурсы. Информационные ресурсы местного самоуправления.
33. Информационная безопасность. Основные направления государственной информационной политики. Законодательная база. Экономическая политика. Социальная политика. Технологическая политика. Международное сотрудничество.
34. Право на защиту чести, достоинства и деловой репутации в системе субъективных гражданских прав.
35. Компенсация морального вреда как способ защиты чести, достоинства и деловой репутации.
36. Судебная защита чести, достоинства, деловой репутации. Судебная защита чести, достоинства, деловой репутации. Судебная защита чести, достоинства, деловой репутации.
37. Виды информации, причиняющей вред здоровью и развитию детей.

Возрастные ограничения, зависящие, от характера допускаемой к обороту

информации.

38. Знаки, обозначающие категорию информационной продукции, в зависимости от возраста сотрудников.

**Приложение 2**

*ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ*

*ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ*

*КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

# «ЗАЩИТА ОБЩЕСТВА ОТ ИНФОРМАЦИИ, ЗАПРЕЩЕННОЙ К РАСПРОСТРАНЕНИЮ»

**(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**

Королев
2020

## 1. Общие положения

Основными формами обучения студентов являются аудиторные занятия, включающие лекции и семинарские занятия.

Лекционные занятия проводятся в форме классической лекции. Лекционный материал в основном подготовлен в виде презентаций MS Power Point и предназначен для усвоения студентами теоретического материала. Ведение конспектов считается обязательным для более полного усвоения материала.

Семинарские занятия проводятся в форме обсуждения, закрепления и углубления учебного материала по отдельным вопросам изучаемых тем, изложенным ранее на лекционных занятиях, изучения структурных схем и основам работы отдельных должностных лиц службы информационной безопасности на типовом предприятии.

## 2. Указания по проведению практических занятий

### Тема 1. Законодательные основы защиты общества, личности, государства от информации, запрещенной к распространению

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Сфера действия настоящего Федерального закона Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью».
- Основные понятия, используемые в настоящем Федеральном законе.
- Законодательство Российской Федерации о защите общества (персонала) от информации, причиняющей вред их здоровью и (или) развитию.
- Полномочия федерального органа исполнительной власти, органов государственной власти субъектов Российской Федерации в сфере защиты человека от информации, причиняющей вред их здоровью и (или) развитию.
- Виды информации, причиняющей вред здоровью и (или) развитию человеку.

Продолжительность занятия - 1 ч.

## Тема 2. Источники информации запрещенной к распространению

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Осуществление классификации информационной продукции.
- Информационная продукция для детей, не достигших возраста шести лет.
- Информационная продукция для детей, достигших возраста шести лет.
- Информационная продукция для детей, достигших возраста двенадцати лет.
- Информационная продукция для детей, достигших возраста шестнадцати лет.

Продолжительность занятия - 1 ч.

## Тема 3. Требования к распространению информации в обществе

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Общие требования к обороту информационной продукции.
- Знак информационной продукции.
- Дополнительные требования к распространению информационной продукции посредством теле- и радиовещания.
- Дополнительные требования к распространению информации посредством информационно-телекоммуникационных сетей.
- Дополнительные требования к обороту отдельных видов информационной продукции для персонала предприятий.
- Дополнительные требования к обороту информационной продукции, запрещенной к распространению.

Продолжительность занятия - 1 ч.

## Тема 4. Экспертиза распространения информации запрещенной к распространению

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Общие требования к экспертизе информационной продукции.
- Экспертное заключение.
- Правовые последствия экспертизы информационной продукции.

Продолжительность занятия - 1 ч.

**Тема 5. Надзор и контроль в сфере защиты общества (персонала) от информации, причиняющей вред здоровью и (или) развитию**

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Государственный надзор и контроль за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.
- Общественный контроль в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

Продолжительность занятия - 1/1 ч.

**Тема 6. Ответственность за правонарушения в сфере защиты от информации, причиняющей вред их здоровью и (или) развитию**

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Ответственность за правонарушения в сфере зашиты персонала от информации, причиняющей вред их здоровью и (или) развитию.

Продолжительность занятия - 1 ч.

**Тема 7. Правовая охрана и защита прав и законных интересов человека, общества, государства от воздействия непристойной информации**

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Сущность непристойной информации особенности ответственности.
- Роль информации в жизни личности, общества, государства. Информационное общество. Стадии становления.
- Характеристика непристойной информации.
- Ответственность за распространение непристойной информации.
- Защита персонала от непристойной информации.
- ФЗ № 252 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Продолжительность занятия - 1 ч.

**Раздел II. Организационно - правовое обеспечение информационной безопасности защиты общества от информации запрещенной к распространению**

## Тема 8. О стратегии государственной информационной политики России в условиях развития информационного общества

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Роль информации в социально-экономическом развитии страны. Цели и принципы государственной информационной политики.
- Стратегические приоритеты государственной информационной политики. Доступность информации. Содержательное разнообразие информации. Качество информации.
- Государственная информация и информационные ресурсы. Информационные ресурсы местного самоуправления.
- Информационная безопасность. Основные направления государственной информационной политики. Законодательная база. Экономическая политика. Социальная политика. Технологическая политика. Международное сотрудничество.
- Первоочередные меры по реализации государственной информационной политики. Принятие и реализация федеральных законов: «О государственной информационной политике», «О государственных информационных ресурсах, реестрах и регистрах», «Об обеспечении доступа граждан и организаций к информации о деятельности государственных органов и органов местного самоуправления», «Об электронном документообороте», «О персональных данных».

Продолжительность занятия - 2 ч.

## Тема 9. Ограничения на распространение в СМИ информации запрещенной к распространению

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Нормы действующего федерального законодательства.
- Законодательство субъектов РФ.
- Проект федерального закона о защите нравственности.
- Правовое регулирование порнографии в США.

Продолжительность занятия - 1 ч.

## Тема 10. Интернет - информация и ее правовое регулирование

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Является ли Интернет средством массовой информации? Статья об «иных СМИ». Информационная безопасность.
- Правовое регулирование содержания сообщений.
- Нарушения авторского права.
- Нормативное регулирование. Обеспечение доказательств. Принудительное саморегулирование.

Продолжительность занятия - 1 ч.

## Тема 11. Защита чести, достоинства и деловой репутации персонала предприятий

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Основные принципы и понятия. Опровержение. Право на ответ.
- Моральный вред. Деловая репутация. Извинение.
- Презумпция невиновности. Факт и мнение.
- Клевета и оскорбление. Освобождение от ответственности.
- Дело «"Нью-Йорк Таймс" против Салливана».
- Решения Европейского суда по правам человека.

Продолжительность занятия - 1 ч.

## Тема 12. Неприкосновенность частной жизни граждан

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Защита от несанкционированного проникновения в личную жизнь в КОСТИТУЦИОННОМ ПРАВЕ РФ.
- Реализация конституционных принципов на защиту личной жизни в УГОЛОВНОМ ПРАВЕ РФ.
- Гарантии неприкосновенности частной жизни.
- Защита общественных интересов.
- Различия прав на личную жизнь и на честь и достоинство.
- Скрытая запись. Согласие на распространение сведений.
- Защита частной жизни в США.

Продолжительность занятия - 1 ч.

## Тема 13. Запрещенная информация и ее место в системе информа-

**ционных отношений**

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Клевета: способы защиты.
- Свобода политической дискуссии. Факты и оценки.
- Защита рекламы. Различные типы СМИ.
- Лицензирование. Ограничение государственных монополий.
- Стадии информационного процесса. Доступ к информации.

Продолжительность занятия - 1 ч.

### Тема 14. Ограничение свободы распространения информации в целях противодействия экстремистской деятельности

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Право на защиту чести, достоинства и деловой репутации в системе субъективных гражданских прав.
- Компенсация морального вреда как способ защиты чести, достоинства и деловой репутации.
- Судебная защита чести, достоинства, деловой репутации. Судебная защита чести, достоинства, деловой репутации. Судебная защита чести, достоинства, деловой репутации.
- Виды информации, причиняющей вред здоровью и развитию детей.
- Возрастные ограничения, зависящие, от характера допускаемой к обороту информации.
- Знаки, обозначающие категорию информационной продукции, в зависимости от возраста детей.

Продолжительность занятия - 1 ч.

### Тема 15. Проблемы реализации конституционного права граждан на доступ к информации.

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

- Конституционные гарантии права граждан РФ на информацию. Конституционно - правовые гарантии свободы распространения информации в РФ.
- Международный опыт конституционно-правового регулирования доступа граждан к информации. Право граждан на доступ к правовой

информации.

- Правовая информация :понятие, виды, социальная потребность. Гарантии прав граждан на доступ к информации о деятельности органов государственной власти.
- Право на информацию о деятельности органов государственной власти как фактор обеспечения участия в управлении государством.
- Правовое регулирование порядка распространения информации о деятельности органов государственной власти в РФ. Обеспечение открытости информации о деятельности органов государственной власти в рамках административной реформы.

Продолжительность занятия - 1 ч.

## 3. Указания по проведению лабораторных работ

Цель проведения лабораторных работ – ознакомление студентов с комплексом показателей для оценки защищённости информационных объектов, систем и ознакомление с программной средой, используемой для моделирования процессов оптимизации применения систем физической защиты.

Задачи выполнения лабораторных работ:

- определение положения механизмов защиты, включение которых в иерархию системы физической защиты информационных объектов повышает уровень их защищённости;
- мониторинг защищённости охраняемых информационных объектов, базирующийся на решении оптимизационных задач на основе рейтинговых показателей, учитывающий разноплановые экспертные оценки, включая экономические;
- анализ существующих систем физической защиты предприятий на предмет определения эффективности их применения исходя из предполагаемых затрат на создание таких систем, их эксплуатацию и реализацию для предотвращения ущерба от выявленных и потенциальных угроз;
- формирование потенциальной структуры защищённых информационных систем и технологий, путём задания иерархии эшелонов и перечня механизмов защиты для нейтрализации требуемого поля угроз и предотвращённого ущерба;
- формирование динамической модели физической защиты информационных систем для анализа последствий реализации угроз, приводящих к ущербу, близкому или превышающему допустимое для данного хозяйствующего субъекта значение.

Методика проведения лабораторных работ определяется моделью решаемых задач по обеспечению физической защиты информационных объектов, исследуемых студентами на занятии по заданию преподавателя.

Средства выполнения лабораторных работ:

- программный комплекс «Эксперт - 2.0»;
- программный комплекс «EASI»;

- инструменты интегрального метода оценки рисков при распределении ограниченных ресурсов;
- программный комплекс «Adobe Photoshop».

Этапы выполнения лабораторных работ:

1. Постановка задачи лабораторной работы.
2. Ознакомление обучаемых с содержанием и объёмом лабораторной работы.
3. Порядок выполнения лабораторной работы.
4. Регистрация результатов и оформление отчёта о лабораторной работе.
5. Заключительная часть лабораторной работы.

## Тематика лабораторных работ и задания к ним

**Лабораторная работа 1.**

*Тема:* **Выявление и анализ угроз охраняемым объектам с помощью программного комплекса «Эксперт - 2.0».**

*Цель занятия:* Ознакомление с программным комплексом оценки защищённости информационных систем «Эксперт - 2.0» и получение практических навыков в моделировании и оптимизации определения угроз безопасности информационным объектам, применения механизмов защиты в ходе осуществления мониторинга деятельности предприятий.

Учебные вопросы.

1. Формирование матрицы экспертных оценок с полями «механизмы защиты-угрозы» и «угрозы-эшелоны» для оценки достоверности активируемых механизмов защиты.
2. Формирование рейтинговых показателей в разрезе использования конкретных механизмов защиты и эшелонов для системы физической защиты в целом, а также показателей активности отдельных эшелонов и механизмов защиты.
3. Анализ активности системы физической защиты в разрезе использования конкретных механизмов и эшелонов защиты, формулирование предложений по улучшению рейтинга исследуемой системы.

*Продолжительность занятия – 4 часа.*

*Задание на лабораторную работу №1:*

1. Ознакомиться с системой показателей для оценки информационной защищённости исследуемых объектов.

2. Запустить программу «Эксперт - 2.0» и в интерактивном режиме сформировать перечень известных угроз, механизмов защиты и расставить их в иерархии эшелонов защиты для исследуемых объектов.

3. Сформировать матрицы экспертных оценок «Механизмы защиты – Угрозы» и «Угрозы – Эшелоны защиты» для повышения достоверности исходных данных и активации механизмов защиты.

4. Провести расчёт матрицы, определяющей распределение относительного потенциального ущерба по механизмам защиты и эшелонам безопасности на заданном множестве известных угроз.

5. Проанализировать активность системы информационной безопасности в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемого предприятия.

6. Действия пунктов 3-5 повторить для различных частот активизации угроз безопасности.

7. Сформировать рейтинговые показатели при использовании конкретных механизмов защиты и эшелонов информационной безопасности для указанных информационных объектов, а также показатели активности отдельных эшелонов и механизмов защиты.

8. Создать отчёт по лабораторной работе и сформулировать выводы.

**Лабораторная работа 2.**

*Тема:* **Исследование системы физической защиты с помощью программного комплекса «Эксперт – 2.0».**

*Цель занятия:* Ознакомление с программным комплексом оценки защищённости информационных систем «Эксперт - 2.0» и получение практических навыков в моделировании и оптимизации применения механизмов защиты для деятельности отдельных предприятий с учётом рисков и неопределённости внешней среды.

Учебные вопросы.

1. Корректировка матрицы экспертных оценок для достоверности активации механизмов защиты с расчётом матрицы, определяющей распределение достоверности активации по механизмам защиты и эшелонам безопасности для системы физической защиты на заданном множестве известных угроз.
2. Формирование рейтинговых показателей в разрезе использования конкретных механизмов защиты и эшелонов безопасности для системы физической защиты в целом, а также показателей активности отдельных эшелонов и механизмов защиты.
3. Анализ информационной защищенности исследуемых объектов с определением конкретных механизмов защиты, обеспечивающих наибольшую динамику рейтинговых показателей.

*Продолжительность занятия – 4 часа.*

*Задание на лабораторную работу №2:*

1. Ознакомиться с системой показателей для оценки защищённости исследуемых объектов в деятельности отдельных предприятий с учётом рисков и неопределённости внешней среды.

2. Запустить программу «Эксперт - 2.0» в интерактивном режиме, получить от преподавателя вариант многоуровневой системы защиты исследуемого объекта предприятия с индивидуальным распределением конкретных механизмов защиты по эшелонам безопасности.

3. Провести расчёт матрицы, определяющей распределение относительного ущерба по механизмам защиты и уровням адаптивной системы защищённости исследуемых объектов предприятия на заданном множестве известных угроз.

4. Проанализировать активность адаптивной защиты в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемых объектов предприятия.

5. Сформировать рейтинговые показатели в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемых объектов предприятия.

6. Проанализировать существующую защищённость и сформулировать предложения по улучшению рейтинга системы физической защиты исследуемых объектов предприятия в рамках реализации адаптивной системы защиты.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

**Лабораторная работа 3.**

*Тема:* **Исследование эффективности системы физической защиты предприятия по предполагаемым действиям нарушителя при определённых угрозах и состоянии элементов защиты с помощью программного комплекса оценки враждебных проникновений и действий "EASI".**

*Цель занятия:* Ознакомление студентов с комплексом показателей для оценки защищённости объектов предприятий и программным комплексом оценки враждебных проникновений и действий "Estimate of Adversary Sequence Interruption" (EASI), а так же получение практических навыков в моделировании применения механизмов физической защиты и оценки их эффективности на заданном пути нарушителя при определённых угрозах и состоянии самой системы защиты предприятия.

Учебные вопросы.

1. Анализ пути нарушителя при продвижении к охраняемому объекту.
2. Определение критической точки обнаружения и её влияние на параметры оценки прерывания последовательности действий нарушителя.
3. Построение и исследование диаграммы последовательности действий нарушителя для конкретной зоны охраняемого объекта.

*Продолжительность занятия – 4 часа.*

*Задание на лабораторную работу №3:*

1. Ознакомиться с краткими теоретическими сведениями по оценке физической защищённости охраняемых объектов и основными способами действий злоумышленников.

2. Ознакомиться с методикой применения модели "EASI" по оценке враждебных проникновений и действий нарушителя на охраняемых объектах.

3. Запустить модель "EASI" на персональном компьютере и смоделировать в интерактивном режиме возможные действия нарушителя на предложен-

ном охраняемом объекте с выбором определённых процедур и механизмов защиты.

4. Рассчитать основные показатели эффективности по введённым данным для выбранного пути проникновения нарушителя и сформированной системы защиты охраняемого объекта, оценить её значение.

5. Проанализировать эффективность исходной системы физической защиты охраняемого объекта, выявить её недостатки и сформировать дополнительные мероприятия и средства защиты на пути проникновения нарушителя для повышения основных критериев безопасности все данные занести в рабочую таблицу модели.

6. Оценить эффективность усовершенствованной системы защиты на основе добавленных элементов на охраняемом объекте, обосновать Ваши решения расчётами с занесением данных в рабочую таблицу модели и сформировать итоговые показатели эффективности системы физической защиты.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

**Лабораторная работа 4.**

*Тема:* **Исследование системы физической защиты и охраняемых объектов с помощью интегрального метода оценки рисков при распределении ограниченных ресурсов, имеющихся в распоряжении службы безопасности.**

*Цель занятия:* Изучение принципов компьютерного моделирования эффективности системы физической защиты на основе общего уравнения для расчёта рисков охраняемого объекта и получение практических навыков в работе со специализированными программными средствами защиты.

Учебные вопросы.

1. Использование общего уравнения для расчёта рисков охраняемого объекта как важного инструмента количественной оценки системы физической защиты.
2. Анализ и оценка рисков для выбора оптимального варианта защиты, допустимого для охраняемого объекта по критерию затраты-прибыль в исследуемой системе физической защиты.

*Продолжительность занятия – 4 часа.*

*Задание на лабораторную работу №4:*

1. Ознакомиться с инструментом количественной оценки системы физической защиты на основе общего уравнения для расчёта рисков охраняемого объекта.

2. Сформировать рейтинговые показатели риска в разрезе использования выбранных механизмов защиты для охраняемых объектов и для системы в целом, а также показатели активности отдельных элементов защиты.

3. Воспользовавшись инструментом количественной оценки системы физиической защиты на основе общего уравнения расчёта рисков проанализировать исходную защищенность исследуемого объекта, выделить конкретные ме-

ханизмы защиты, обеспечивающие наибольшую динамику рейтинговых показателей риска.

4. Сохранить в файле текущее состояние адаптивной системы физической защиты и показатели риска для дальнейших исследований.

5. Сравнить разнородную структуру системы физической защиты и рейтинговые показатели риска для заданных вариантов адаптивной защиты охраняемых объектов.

6. Результаты работы и итогового анализа сравнения поместить в Вашу папку на ПК.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

## 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-правого 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 | 60 |
| Вопросы, выносимые на самостоятельное изучение | 6 |
| Подготовка к практическим занятиям | 16 |
| Подготовка к лабораторным занятиям | 16 |
| Подготовка докладов | 10 |
| Выполнение практических заданий | 12 |

**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 | 6 | Изучение открытых источников |
| 2. | Подготовка к практическим занятиям | 16 | Изучение открытых источников при подготовке доклада на выбранную тему. |
| 3. | Подготовка к лабораторным занятиям | 16 | Изучение открытых источников при подготовке к работе. |
| 4. | Тематика докладов | 10 | См. п.1-8 |
| 5. | Выполнение практических заданий | 12 | 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)

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

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.

В процессе изложения материала необходимо давать ссылки на используемую литературу.

Заключение должно содержать сделанные автором работы выводы, итоги исследования.

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. Демушкин 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., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).

**Рекомендуемая литература:**


1. Ищейнов В.Я., Мецатунян 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 - Энциклопедия информационной безопасности. –

Публикации, статьи.

4. **www.biblioclub.ru** - Универсальная библиотека онлайн
5. **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

## 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 «Защита общества от информации, запрещенной к распространению».