

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета  С.М. Пасмурнов  
«31» августа 2017 г.



**РАБОЧАЯ ПРОГРАММА**

дисциплины

«Организационное и правовое обеспечение информационной безопасности»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация Безопасность распределённых компьютерных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2017

Автор программы



/ Паринова Л.В./

Заведующий кафедрой Систем информационной безопасности



/Остапенко А.Г./

Руководитель ОПОП



/ Остапенко А.Г./

Воронеж 2017

## 1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

**1.1. Цель дисциплины** приобретение студентами умения и навыков практической работы по избранной специальности и присваиваемой квалификации, научиться наблюдать, понимать и анализировать деятельность специалиста по информационной безопасности распределенных компьютерных систем

### 1.2. Задачи освоения дисциплины

- получение представления об информационном законодательстве Российской Федерации;
- получение представления об информационном законодательстве Российской Федерации;
- ознакомление с правилами лицензирования и сертификации в области защиты информации

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к дисциплинам базовой части блока Б1.

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Организационное и правовое обеспечение информационной безопасности» направлен на формирование следующих компетенций:

ОК-2 - способностью использовать основы экономических знаний в различных сферах деятельности

ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности

ОПК-5 - способностью использовать нормативные правовые акты в своей профессиональной деятельности

ОПК-6 - способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций

ПК-1 - способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности

ПК-13 - способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности

| Компетенция | Результаты обучения, характеризующие сформированность компетенции  |
|-------------|--|
| ОК-2        | знать основы экономических знаний; специфику и возможности использования экономических знаний в различных сферах деятельности; |

|       |  |
|-------|--|
|       | <p>способы использования экономических знаний в различных сферах деятельности.</p> <p>уметь определять специфику экономических знаний в различных сферах деятельности;</p> <p>определять возможности использования экономических знаний в различных сферах деятельности;</p> <p>владеть навыками определять специфику экономических знаний в различных сферах деятельности;</p> <p>навыками определять возможности использования экономических знаний в различных сферах деятельности;</p> <p>навыками использования экономических знаний в различных сферах деятельности.</p> |
| ОК-4  | <p>знать основные положения нормативно-правовых актов, направленных на обеспечение информационной безопасности</p> <p>уметь применять необходимые положения нормативно-правовых актов в нужной ситуации</p> <p>владеть способностью использовать основы правовых знаний в различных сферах деятельности</p>  |
| ОПК-5 | <p>знать о возможных социальных и культурных различиях членов коллектива</p> <p>уметь эффективно преодолевать конфликты</p> <p>владеть способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия</p>   |
| ОПК-6 | <p>знать основные положения нормативно-правовых актов, направленных на обеспечение информационной безопасности</p> <p>уметь использовать основные положения и методы защиты конфиденциальной информации в профессиональной деятельности;</p> <p>владеть способностью использовать нормативные правовые акты в своей профессиональной деятельности</p>  |
| ПК-1  | <p>знать приемы быстрого нахождения качественных материалов по проблемам компьютерной безопасности</p> <p>уметь осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности</p> <p>владеть способностью осуществлять подбор, изучение и обобщение научно-технической информа-</p>   |

|       |   |
|-------|---|
|       | ции, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности  |
| ПК-13 | знать приемы быстрого нахождения качественных материалов по проблемам компьютерной безопасности   |
|       | уметь осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности  |
|       | владеть способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности |

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Организационное и правовое обеспечение информационной безопасности» составляет 4 з.е.

Распределение трудоемкости дисциплины по видам занятий  
**очная форма обучения**

| Виды учебной работы                             | Всего часов | Семестры |
|---|-------------|----------|
|   |             | 10       |
| <b>Аудиторные занятия (всего)</b>               | 72          | 72       |
| В том числе:                                    |             |          |
| Лекции  | 36          | 36       |
| Практические занятия (ПЗ)                       | 36          | 36       |
| <b>Самостоятельная работа</b>                   | 72          | 72       |
| Виды промежуточной аттестации - зачет с оценкой | +           | +        |
| Общая трудоемкость:<br>академические часы       | 144         | 144      |
| зач.ед.   | 4           | 4        |

#### 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

**5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий**

**очная форма обучения**

| № п/п | Наименование темы | Содержание раздела | Лекц | Пра к | СРС | Всего , |
|-------|-------------------|--------------------|------|-------|-----|---------|
|-------|-------------------|--------------------|------|-------|-----|---------|

|   |   |  | зан. |   | час |    |
|---|---|--|------|---|-----|----|
| 1 | <p>Правовое обеспечение информационной безопасности.</p> <p>Роль и место дисциплины в формировании компетенций студентов по направлению подготовки 10.05.01. Основные понятия и определения. Основы теории государства и права как фундаментальной дисциплины для изучения организационно-правового обеспечения информационной безопасности</p> | <p>Особенности дисциплины и ее связь с другими дисциплинами. Методические рекомендации по изучению. Законодательство РФ в области информационной безопасности защиты государственной тайны и конфиденциальной информации. Защита информации. Процесс ЗИ. обеспечение и обслуживание процесса ЗИ. управление процессом ЗИ. координация деятельности в области ЗИ. Системы защиты информации. Государственная система ЗИ (ГСЗИ). Целевые (объектные) и функциональные подсистемы ЗИ. Системы систем подготовки кадров в области ЗИ систем лицензирования. сертификации, аттестования, проведения НИОКР, оказания услуг в области ЗИ. Система документов в области ЗИ.</p> <p>Место теории государства и права в системе юридических наук. Основные понятия теории государства и права. Правовые отношения. Виды правовых отношений в сфере ЗИ. Правовые нормы. Методы правового регулирования общественных отношений. Право, ограничение права, обязанность, ответственность в сфере информационных отношений. Классификация отраслей права.</p> | 6    | 6 | 12  | 24 |
| 2 | <p>Правовое обеспечение информационной безопасности. Система законодательного регулирования общественных отношений в области обеспечения информационной безопасности. Конституционные основы обеспечения информационной безопасности в РФ</p>   | <p>Концепция построения системы законодательного регулирования общественных отношений в области обеспечения информационной безопасности. Роль и место Конституции РФ. конституционных законов. Гражданского Уголовного кодексов. Кодекса об административных правонарушениях, Кодекса законов о труде, других общих и специальных законов в области ЗИ. защиты интеллектуальной собственности в регулировании общественных отношений в процессе создания, распространения и использования информации, информатизации и защиты информации.</p> <p>Основы конституционного строя. Права и свободы человека и гражданина как важнейшего субъекта ЗИ. Федеративное устройство России и его влияние на организацию 311. Функции Президента</p>  | 6    | 6 | 12  | 24 |

|   |  |  |   |   |    |    |
|---|--|--|---|---|----|----|
|   |  | РФ. Федерального Собрания. Правительства РФ. федеральных органов исполнительной власти, органов судебной власти, органов государственной власти субъектов РФ. органов местного самоуправления в решении вопросов обеспечения информационной безопасности.  |   |   |    |    |
| 3 | <p>Правовое обеспечение информационной безопасности.</p> <p>Регламентация вопросов обеспечения информационной безопасности в Гражданском кодексе РФ. Закон РФ «О государственной тайне».</p> <p>Федеральные законы «Об информации, информатизации и защите информации» и «Об участии в международном информационном обмене». Законы РФ «Об авторском праве и смежных правах», «О правовой охране программ для электронно-вычислительных машин и баз данных».</p> <p>Регламентация вопросов ЗИ в Федеральных законах общего характера</p> | <p>Информация как объект гражданских прав. Виды информации. подлежащие защите в процессе обычного гражданского оборота. Регламентация вопросов защиты служебной, коммерческой и банковской тайны, интеллектуальной собственности. Использование электронно-цифровой подписи при совершении сделок.</p> <p>Система защиты государственной тайны. Перечень сведений. составляющих государственную тайну.</p> <p>Отнесение сведений к государственной тайне и их засекречивание.</p> <p>Рассекречивание сведений и их носителей. Распоряжение сведениями. составляющими государственную тайну. Правовой режим защиты государственной тайны. Финансирование мероприятий по защите государственной тайны.</p> | 6 | 6 | 12 | 24 |
| 4 | <p>Правовое обеспечение информационной безопасности. Международное законодательство в области обеспечения информационной безопасности и защиты информации. Основы организации обеспечения информационной безопасности и ЗИ. Система документов в области обеспечения информационной безопасности и защиты информации</p>   | <p>Принципы правового регулирования вопросов обеспечения информационной безопасности и ЗИ в США. Франции. Великобритании. ФРГ и других государствах. Краткая характеристика основных законодательно-правовых документов в области ЗИ. действующих в указанных государствах.</p>  | 6 | 6 | 12 | 24 |
| 5 | <p>Организационное. обеспечение информационной безопасности. Цели и задачи. Лицен-</p>   | <p>Классификация объектов обеспечения информационной безопасности и защиты информации. Структуризация понятия «объект защиты». Со-</p>   | 6 | 6 | 12 | 24 |

|   |  |   |   |   |    |    |
|---|--|---|---|---|----|----|
|   | <p>зирование, сертификация и аттестация объектов ЗИ</p>  | <p>ставные части объекта защиты. Виды защищаемой информации, носителей информации и информационных процессов. Характеристика промышленных предприятий, учреждений. Информационно-телекоммуникационных систем как объектов защиты.</p> <p>Правовые основы лицензирование деятельности в области ЗИ. Структура системы лицензирования, функции ее органов. Порядок проведения лицензирования. Распределений полномочий по лицензированию деятельности в области ЗИ между федеральными органами государственной власти.</p> <p>Правовые основы сертификации ЗИ. Структура системы сертификации. функции ее органов. Порядок сертификации ЗИ. Распределений полномочий по сертификации средств ЗИ между федеральными органами государственной власти</p> <p>Правовые основы аттестования объектов по выполнению требований обеспечения защиты информации. Структура системы аттестования, функции ее органов. Порядок аттестования объектов органов управления, промышленных объектов. систем информатизации и связи. Распределений полномочий по аттестованию между федеральными органами государственной власти</p> |   |   |    |    |
| 6 | <p>Организационное обеспечение информационной безопасности Подготовка (переподготовка) и повышение квалификации специалистов в области ЗИ. Организация контроля состояния ЗИ. Организация ЗИ на объектах органов государственной власти и управления</p> | <p>Правовые основы контроля состояния ЗИ. Основные организационно-рапорядительные и нормативные документы по контролю состояния ЗИ. Цели и задачи контроля. Формы контроля: межведомственный контроль: ведомственный контроль: контроль, осуществляемый собственником информации. Органы контроля. Контроль организации и эффективности ЗИ. Методы контроля: информационно-логический: расчетный : инструментальный: инструментально-расчетный: программный. Нарушения установленных требований и норм ЗИ. Требования к содержанию Руководств по</p>  | 6 | 6 | 12 | 24 |

|              |  |   |           |           |           |            |
|--------------|--|---|-----------|-----------|-----------|------------|
|              |  | ЗИ на объекте. Цели и задачи ЗИ. Определение защищаемых информационных ресурсов. Оценка возможностей технических разведок и других источников угроз безопасности информации. Разработка организационных и технических мероприятий по ЗИ. Аттестование объектов. |           |           |           |            |
| <b>Итого</b> |  |   | <b>36</b> | <b>36</b> | <b>72</b> | <b>144</b> |

## 5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

## 6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

## 7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

#### 7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

| Компетенция | Результаты обучения, характеризующие сформированность компетенции  | Критерии оценивания  | Аттестован  | Не аттестован   |
|-------------|--|--|---|---|
| ОК-2        | знать основы экономических знаний; специфику и возможности использования экономических знаний в различных сферах деятельности; способы использования экономических знаний в различных сферах деятельности. | знание основ экономических знаний; специфику и возможности использования экономических знаний в различных сферах деятельности; способы использования экономических знаний в различных сферах деятельности. | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|             | уметь определять специфику экономических знаний в различных сферах деятельности; определять возможности использования экономических знаний в различных сферах  | умение определять специфику экономических знаний в различных сферах деятельности; определять возможности использования экономических знаний в различных сферах деятельности;                               | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |



|       |  |  |  |  |
|-------|--|--|--|--|
|       | <p>деятельности;</p> <p>владеть навыками определять специфику экономических знаний в различных сферах деятельности;</p> <p>навыками определять возможности использования экономических знаний в различных сферах деятельности;</p> <p>навыками использования экономических знаний в различных сферах деятельности.</p> | <p>владение навыками определять специфику экономических знаний в различных сферах деятельности;</p> <p>навыками определять возможности использования экономических знаний в различных сферах деятельности;</p> <p>навыками использования экономических знаний в различных сферах деятельности.</p> | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |
| ОК-4  | <p>знать основные положения нормативно-правовых актов, направленных на обеспечение информационной безопасности</p>   | <p>знание основных положений нормативно-правовых актов, направленных на обеспечение информационной безопасности</p>  | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |
|       | <p>уметь применять необходимые положения нормативно-правовых актов в нужной ситуации</p>   | <p>умение применять необходимые положения нормативно-правовых актов в нужной ситуации</p>  | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |
|       | <p>владеть способностью использовать основы правовых знаний в различных сферах деятельности</p>  | <p>владение способностью использовать основы правовых знаний в различных сферах деятельности</p>   | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |
| ОПК-5 | <p>знать о возможных социальных и культурных различиях членов коллектива</p>   | <p>знание о возможных социальных и культурных различиях членов коллектива</p>  | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |
|       | <p>уметь эффективно преодолевать конфликты</p>   | <p>умение эффективно преодолевать конфликты</p>  | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |
|       | <p>владеть способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия</p>   | <p>владение способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия</p>  | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |
| ОПК-6 | <p>знать основные положения нормативно-правовых актов, направленных на обеспечение информационной безопасности</p>   | <p>знание основных положений нормативно-правовых актов, направленных на обеспечение информационной безопасности</p>  | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |

|       |   |  |   |   |
|-------|---|--|---|---|
|       | уметь использовать основные положения и методы защиты конфиденциальной информации в профессиональной деятельности;  | умение использовать основные положения и методы защиты конфиденциальной информации в профессиональной деятельности;  | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|       | владеть способностью использовать нормативные правовые акты в своей профессиональной деятельности   | владение способностью использовать нормативные правовые акты в своей профессиональной деятельности   | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-1  | знать приемы быстрого нахождения качественных материалов по проблемам компьютерной безопасности   | знание приемов быстрого нахождения качественных материалов по проблемам компьютерной безопасности  | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|       | уметь осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности  | умение осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности  | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|       | владеть способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности | владение способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-13 | знать приемы быстрого нахождения качественных материалов по проблемам компьютерной безопасности   | знание приемов быстрого нахождения качественных материалов по проблемам компьютерной безопасности  | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
|       | уметь осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного   | умение осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности  | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

|  |   |  |   |   |
|--|---|--|---|---|
|  | опыта по проблемам компьютерной безопасности  |  |   |   |
|  | владеть способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности | владение способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

### 7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 10 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

| Компетенция | Результаты обучения, характеризующие сформированность компетенции  | Критерии оценивания                    | Отлично  | Хорошо  | Удовл.   | Неудовл.                             |
|-------------|--|--|--|---|--|--------------------------------------|
| ОК-2        | знать основы экономических знаний, специфику и возможности использования экономических знаний в различных сферах деятельности; способы использования экономических знаний в различных сферах деятельности. | Тест                                   | Выполнение теста на 90- 100%                           | Выполнение теста на 80- 90%   | Выполнение теста на 70- 80%                              | В тесте менее 70% правильных ответов |
|             | уметь определять специфику экономических знаний в различных сферах деятельности; определять возможности использования экономических знаний в различных сферах деятельности;                                | Решение стандартных практических задач | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены                     |
|             | владеть навыками определять специфику экономических знаний в раз-  | Решение прикладных задач в конкретной  | Задачи решены в полном объеме и                        | Продемонстрирован верный ход решения всех, но не получен                              | Продемонстрирован верный ход решения в                   | Задачи не решены                     |

|       |  |  |  |   |  |                                      |
|-------|--|--|--|---|--|--------------------------------------|
|       | личных сферах деятельности; навыками определять возможности использования экономических знаний в различных сферах деятельности; навыками использования экономических знаний в различных сферах деятельности. | предметной области                                       | получены верные ответы                                 | верный ответ во всех задачах  | большинстве задач  |                                      |
| ОК-4  | знать основные положения нормативно-правовых актов, направленных на обеспечение информационной безопасности  | Тест   | Выполнение теста на 90- 100%                           | Выполнение теста на 80- 90%   | Выполнение теста на 70- 80%                              | В тесте менее 70% правильных ответов |
|       | уметь применять необходимые положения нормативно-правовых актов в нужной ситуации  | Решение стандартных практических задач                   | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены                     |
|       | владеть способностью использовать основы правовых знаний в различных сферах деятельности   | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены                     |
| ОПК-5 | знать о возможных социальных и культурных различиях членов коллектива  | Тест   | Выполнение теста на 90- 100%                           | Выполнение теста на 80- 90%   | Выполнение теста на 70- 80%                              | В тесте менее 70% правильных ответов |
|       | уметь эффективно преодолевать конфликты  | Решение стандартных практических задач                   | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены                     |
|       | владеть способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия  | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены                     |
| ОПК-6 | знать основные положения нормативно-правовых актов, направленных на обеспечение информационной безопасности  | Тест   | Выполнение теста на 90- 100%                           | Выполнение теста на 80- 90%   | Выполнение теста на 70- 80%                              | В тесте менее 70% правильных ответов |
|       | уметь использовать   | Решение  | Задачи   | Продемонстр   | Продемонстр  | Задачи не                            |

|       |   |  |  |   |  |                                      |
|-------|---|--|--|---|--|--------------------------------------|
|       | основные положения и методы защиты конфиденциальной информации в профессиональной деятельности;   | стандартных практически задач                            | решены в полном объеме и получены верные ответы        | ирован верный ход решения всех, но не получен верный ответ во всех задачах            | ирован верный ход решения в большинстве задач            | решены                               |
|       | владеть способностью использовать нормативные правовые акты в своей профессиональной деятельности   | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены                     |
| ПК-1  | знать приемы быстрого нахождения качественных материалов по проблемам компьютерной безопасности   | Тест   | Выполнение теста на 90- 100%                           | Выполнение теста на 80- 90%   | Выполнение теста на 70- 80%                              | В тесте менее 70% правильных ответов |
|       | уметь осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности  | Решение стандартных практически задач                    | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены                     |
|       | владеть способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены                     |
| ПК-13 | знать приемы быстрого нахождения качественных материалов по проблемам компьютерной безопасности   | Тест   | Выполнение теста на 90- 100%                           | Выполнение теста на 80- 90%   | Выполнение теста на 70- 80%                              | В тесте менее 70% правильных ответов |
|       | уметь осуществлять подбор, изучение и обобщение науч-   | Решение стандартных практически задач                    | Задачи решены в полном объеме и                        | Продемонстрирован верный ход решения всех, но не получен                              | Продемонстрирован верный ход решения в                   | Задачи не решены                     |

|  |   |  |  |   |  |                  |
|--|---|--|--|---|--|------------------|
|  | но-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности  |  | получены верные ответы                                 | верный ответ во всех задачах  | большинстве задач  |                  |
|  | владеть способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены |

## 7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

### 7.2.1 Примерный перечень заданий для подготовки к тестированию

|   |  |
|---|--|
| ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности |  |
| 1.  | Информационное общество: понятие, структура, признаки.   |
| 2.  | Понятие информационной сферы общества.   |
| 3.  | Информация и ее виды.  |
| 4.  | Ответственность за правонарушения в информационной сфере.  |
| 5.  | Понятие коммерческой тайны. Информация, составляющая коммерческую тайну (секреты производства).                                |
| 6.  | Отнесение информации к информации, составляющей коммерческую тайну (секрет производства).                                      |
| 7.  | Понятие и виды персональных данных.  |
| 8.  | Принципы обработки персональных данных.  |
| 9.  | Порядок и условия обработки персональных данных.   |
| 10.   | Права и обязанности субъекта персональных данных.  |
| 11.   | Понятие и виды электронной подписи.  |
| 12.   | Правовой статус удостоверяющего центра.  |
| 13.   | Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи.                                |
| 14.   | Правовое регулирование отношений в сфере библиотечного дела.   |
| 15.   | Правовое регулирование отношений в области формирования обязательного экземпляра документов.                                   |
| 16.   | Правовое регулирование общественных отношений в сфере формирования, хранения, учета и использования архивов и архивных фондов. |
| 17.   | Понятие связи, ее структура, принципы функционирования.  |
| 18.   | Общая характеристика отношений в сфере связи и массовых коммуникаций.  |
| 19.   | Государственной регулирование деятельности в области связи.  |

|  |  |
|--|--|
| 20.  | Право и Интернет как социальные явления.   |
| 21.  | Правовое регулирование деятельности в киберпространстве.                                   |
| ОПК-5 - способностью использовать нормативные правовые акты в своей профессиональной деятельности  |  |
| 1.   | Сущность конституционного права на информацию и его гарантии.                              |
| 2.   | Правовые режимы информации.  |
| 3.   | Понятие информационной безопасности.   |
| 4.   | Понятие правонарушений в информационной сфере.   |
| 5.   | Понятие государственной тайны. Сведения, составляющие государственную тайну.               |
| 6.   | Отнесение сведений к государственной тайне, их засекречивание и рассекречивание.           |
| 7.   | Порядок распоряжения сведениями, составляющими государственную тайну.                      |
| 8.   | Защита сведений, составляющих государственную тайну.                                       |
| 9.   | Содержание и реализация исключительного права на секрет производства.                      |
| 10.  | Права и обязанности оператора при обработке персональных данных.                           |
| 11.  | Особенности регулирования интернет-отношений.  |
| ОПК-6 - способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций   |  |
| 1.   | Понятие и виды информационных правоотношений.  |
| 2.   | Субъекты, объекты, содержание информационных правоотношений.                               |
| 3.   | Законодательство Российской Федерации в области информационной безопасности.               |
| 4.   | Особенности обеспечения информационной безопасности в различных сферах общественной жизни. |
| 5.   | Юридическая ответственность за нарушение режима государственной тайны.                     |
| 6.   | Ответственность за нарушение положений законодательства о персональных данных.             |
| 7.   | Понятие электронного документа и электронного документооборота.                            |
| 8.   | Правовое регулирование и юридические риски электронного документооборота.                  |
| 9.   | Общая характеристика законодательства в сфере электронного документооборота.               |
| ПК-1 - способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности |  |
| 1.   | Ответственность за нарушение исключительного права на секрет производства.                 |
| 2.   | Контроль и надзор за обработкой персональных данных.                                       |
| 3.   | Киберпреступления: понятие, основные черты, формы проявления.                              |
| 4.   | Понятие и распространение массовой информации.   |
| 5.   | Понятие и правовой статус средства массовой информации.                                    |
| 6.   | Правовые формы организации деятельности средств массовой информации.                       |
| 7.   | Общие принципы работы средств массовой информации.   |
| 8.   | Правовые формы организации деятельности средств массовой информации.                       |
| 9.   | Специальная редакционная ответственность средств массовой информации.                      |
| <b>7.2.2 Примерный перечень заданий для решения стандартных задач</b>  |  |
| ОПК-8 - способностью к освоению новых образцов программных, технических средств и информационных технологий  |  |
| 1  | Кто является основным ответственным за определение уровня классифи-                        |

|   |   |
|---|---|
|   | <p>кации информации?<br/> Варианты ответа:<br/> Руководитель среднего звена<br/> Высшее руководство<br/> <b>Владелец</b><br/> Пользователь</p>  |
| 2   | <p>Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?<br/> Варианты ответа:<br/> <b>Сотрудники</b><br/> Хакеры<br/> Атакующие<br/> Контрагенты (лица, работающие по договору)</p>   |
| ПК-12 - способностью проводить инструментальный мониторинг защищенности компьютерных систем |   |
| 1   | <p>Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?<br/> Варианты ответа:<br/> Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования<br/> Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации<br/> <b>Улучшить контроль за безопасностью этой информации</b><br/> Снизить уровень классификации этой информации</p> |
| 2   | <p>Что самое главное должно продумать руководство при классификации данных?<br/> Варианты ответа:<br/> Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным<br/> <b>Необходимый уровень доступности, целостности и конфиденциальности</b><br/> Оценить уровень риска и отменить контрмеры<br/> Управление доступом, которое должно защищать данные</p>  |
| 3   | <p>Какие меры нужны для обеспечения целостности персональных данных в организации?<br/> -учет машинных носителей персональных данных;<br/> -обнаружением фактов несанкционированного доступа к персональным данным и принятием мер<br/> -восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним</p>   |

### 7.2.3 Примерный перечень заданий для решения прикладных задач

|   |
|---|
| ПК-17 - способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение |
| Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?  |



|  |
|--|
| <p>Варианты ответа:<br/> Владельцы данных<br/> Пользователи<br/> Администраторы<br/> <b>Руководство</b></p>  |
| <p>Что такое процедура?<br/> Варианты ответа:<br/> Правила использования программного и аппаратного обеспечения в компании<br/> <b>Пошаговая инструкция по выполнению задачи</b><br/> Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах<br/> Обязательные действия</p>   |
| <p>Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?<br/> Варианты ответа:<br/> Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски<br/> Когда риски не могут быть приняты во внимание по политическим соображениям<br/> Когда необходимые защитные меры слишком сложны<br/> <b>Когда стоимость контрмер превышает ценность актива и потенциальные потери</b></p> |
| <p>ПК-18 - способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации</p>   |
| <p>Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?<br/> Варианты ответа:<br/> <b>Поддержка высшего руководства</b><br/> Эффективные защитные меры и методы их внедрения<br/> Актуальные и адекватные политики и процедуры безопасности<br/> Проведение тренингов по безопасности для всех сотрудников</p>   |
| <p>Что такое политики безопасности?<br/> Варианты ответа:<br/> Пошаговые инструкции по выполнению задач безопасности<br/> Общие руководящие требования по достижению определенного уровня безопасности<br/> <b>Широкие, высокоуровневые заявления руководства</b><br/> Детализированные документы по обработке инцидентов безопасности</p>   |
| <p>Какая из приведенных техник является самой важной при выборе конкретных защитных мер?<br/> Варианты ответа:<br/> Анализ рисков<br/> <b>Анализ затрат / выгоды</b><br/> Результаты ALE<br/> Выявление уязвимостей и угроз, являющихся причиной риска</p>   |
| <p>Какие меры необходимо применить для устранения угрозы несанкционированного доступа в помещения организации?<br/> -организацию надежного пропускного режима;<br/> -определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и</p>   |

массивов информации, архивные данные и т. п.;  
-явный и скрытый контроль за работой персонала системы;

#### **7.2.4 Примерный перечень вопросов для подготовки к зачету**

Не предусмотрено учебным планом

#### **7.2.5 Примерный перечень заданий для решения прикладных задач**

1. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации. Защита информации.

2. Процесс ЗИ, обеспечение и обслуживание процесса ЗИ, управление процессом ЗИ, координация деятельности в области ЗИ.

3. Системы защиты информации. Государственная система ЗИ (ГСЗИ). Целевые (объектные) и функциональные подсистемы ЗИ.

4. Системы систем подготовки кадров в области ЗИ, систем лицензирования, сертификации, аттестования, проведения НИОКР, оказания услуг в области ЗИ. Система документов в области ЗИ.

5. Место теории государства и права в системе юридических наук. Основные понятия теории государства и права.

6. Правовые отношения. Виды правовых отношений в сфере ЗИ. Правовые нормы. Методы правового регулирования общественных отношений. Право, ограничение права, обязанность, ответственность в сфере информационных отношений. Классификация отраслей права.

7. Концепция построения системы законодательного регулирования общественных отношений в области обеспечения информационной безопасности. Роль и место Конституции РФ, конституционных законов, Гражданского Уголовного кодексов, Кодекса об административных правонарушениях, Кодекса законов о труде, других общих и специальных законов в области ЗИ, защиты интеллектуальной собственности в регулировании общественных отношений в процессе создания, распространения и использования информации, информатизации и защиты информации.

8. Основы конституционного строя. Права и свободы человека и гражданина как важнейшего субъекта ЗИ. Федеративное устройство России и его влияние на организацию ЗИ. Функции Президента РФ, Федерального Собрания, Правительства РФ, федеральных органов исполнительной власти, органов судебной власти, органов государственной власти субъектов РФ, органов местного самоуправления в решении вопросов обеспечения информационной безопасности.

9. Информация как объект гражданских прав. Виды информации, подлежащие защите в процессе обычного гражданского оборота.

10. Регламентация вопросов защиты служебной, коммерческой и банковской тайны, интеллектуальной собственности. Использование электронно-цифровой подписи при совершении сделок.

11. Система защиты государственной тайны. Перечень сведений, составляющих государственную тайну. Отнесение сведений к государственной тайне и их засекречивание.

12. Рассекречивание сведений и их носителей. Распоряжение сведениями

ями, составляющими государственную тайну. Правовой режим защиты государственной тайны. Финансирование мероприятий по защите государственной тайны.

13. Информационные ресурсы как объект защиты. Классификация информационных ресурсов.

14

14. Государственные и негосударственные информационные ресурсы. Персональные данные.

15. Пользование информационными ресурсами. Информатизация, информационные системы и средства их обеспечения. Защита информации и прав субъектов информационных отношений. Системы защиты информационных ресурсов

16. Предмет регулирования авторского права. Сфера действия авторского права. Объект авторского права. Смежные права. Сфера действия смежных прав. Субъекты смежных прав. Нарушение авторских и смежных прав. Защита авторских и смежных прав

17. Основные нормы и требования по ЗИ, содержащиеся в законах: «О безопасности», «Об обороне», «Об органах федеральной службы безопасности в Российской Федерации», «О федеральных органах правительственной связи и информации», «О внешней разведке», «О милиции», «О конверсии оборонной промышленности в Российской Федерации», «О закрытом административно-территориальном образовании», «О связи», «О рекламе», «О недрах» и др.

18. Принципы правового регулирования вопросов обеспечения информационной безопасности и ЗИ в США, Франции, Великобритании, ФРГ и других государствах. Краткая характеристика основных законодательно-правовых документов в области ЗИ, действующих в указанных государствах.

19. Основные положения концепции обеспечения информационной безопасности РФ. Основные положения концепции ЗИ в РФ.

20. Распределение полномочий по обеспечению информационной безопасности в РФ. Научно-технические проблемы, требующие скоординированных действий различных органов государственной власти.

21. Обоснование необходимой и достаточной системы документов в области ЗИ. Общегосударственные документы.

22. Организационно-распорядительные документы. Специальные нормативные документы Гостехкомиссии России по вопросам защиты информации от технических разведок, несанкционированного доступа и несанкционированных воздействий на информацию.

23. Нормативные документы государственной системы стандартизации. Плановые документы. Информационные документы.

Модуль II. Организационное обеспечение информационной безопасности

1. Классификация объектов обеспечения информационной безопасности и защиты информации. Структуризация понятия «объект защиты».

2. Составные части объекта защиты. Виды защищаемой информации, носителей информации и информационных процессов.

3. Характеристика промышленных предприятий, учреждений, информационно-телекоммуникационных систем как объектов защиты.

4. Правовые основы лицензирования деятельности в области ЗИ. Структура системы лицензирования, функции ее органов.

5. Порядок проведения лицензирования. Распределений полномочий по лицензированию деятельности в области ЗИ между федеральными органами государственной власти.

6. Правовые основы сертификации ЗИ. Структура системы сертификации, функции ее органов.

7. Порядок сертификации ЗИ. Распределений полномочий по сертификации средств ЗИ между федеральными органами государственной власти

8. Правовые основы аттестования объектов по выполнению требований обеспечения защиты информации.

9. Структура системы аттестования, функции ее органов.

10. Порядок аттестования объектов органов управления, промышленных объектов, систем информатизации и связи.

11. Распределений полномочий по аттестованию между федеральными органами государственной власти

12. Правовые основы подготовки специалистов в области ЗИ. Система учебных заведений. Перечень специальностей.

13. Основные нормативные документы по подготовке специалистов в области ЗИ.

14. Правовые основы контроля состояния ЗИ.

15. Основные организационно-распорядительные и нормативные документы по контролю состояния ЗИ.

16. Цели и задачи контроля.

17. Формы контроля: межведомственный контроль; ведомственный контроль; контроль, осуществляемый собственником информации.

18. Органы контроля. Контроль организации и эффективности ЗИ.

19. Методы контроля: информационно-логический; расчетный; инструментальный; инструментально-расчетный; программный.

20. Нарушения установленных требований и норм ЗИ.

21. Требования к содержанию Руководств по ЗИ на объекте.

22. Цели и задачи ЗИ.

23. Определение защищаемых информационных ресурсов. Оценка возможностей технических разведок и других источников угроз безопасности информации.

24. Разработка организационных и технических мероприятий по ЗИ.

25. Аттестование объектов.

**7.2.6. Методика выставления оценки при проведении промежуточной аттестации**

*(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в*

тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

### 7.2.7 Паспорт оценочных материалов

| № п/п | Контролируемые разделы (темы) дисциплины  | Код контролируемой компетенции         | Наименование оценочного средства                    |
|-------|---|--|---|
| 1     | Правовое обеспечение информационной безопасности. Роль и место дисциплины в формировании компетенций студентов по направлению подготовки 10.05.01. Основные понятия и определения. Основы теории государства и права как фундаментальной дисциплины для изучения организационно-правового обеспечения информационной безопасности           | ОК-2, ОК-4, ОПК- 5, ОПК-6, ПК-1, ПК-13 | Тест, контрольная работа, защита лабораторных работ |
| 2     | Правовое обеспечение информационной безопасности. Система законодательного регулирования общественных отношений в области обеспечения информационной безопасности. Конституционные основы обеспечения информационной безопасности в РФ  | ОК-2, ОК-4, ОПК- 5, ОПК-6, ПК-1, ПК-13 | Тест, контрольная работа, защита лабораторных работ |
| 3     | Правовое обеспечение информационной безопасности. Регламентация вопросов обеспечения информационной безопасности в Гражданском кодексе РФ. Закон РФ «О государственной тайне». Федеральные законы «Об информации, информатизации и защите информации» и «Об участии в международном информационном обмене». Законы РФ «Об авторском праве и | ОК-2, ОК-4, ОПК- 5, ОПК-6, ПК-1, ПК-13 | Тест, контрольная работа, защита лабораторных работ |

|   |   |  |   |
|---|---|--|---|
|   | смежных правах», «О правовой охране программ для электронно-вычислительных машин и баз данных».<br>Регламентация вопросов ЗИ в Федеральных законах общего характера   |  |   |
| 4 | Правовое обеспечение информационной безопасности. Международное законодательство в области обеспечения информационной безопасности и защиты информации. Основы организации обеспечения информационной безопасности и ЗИ. Система документов в области обеспечения информационной безопасности и защиты информации | ОК-2, ОК-4, ОПК- 5, ОПК-6, ПК-1, ПК-13 | Тест, контрольная работа, защита лабораторных работ |
| 5 | Организационное обеспечение информационной безопасности. Цели и задачи. Лицензирование, сертификация и аттестация объектов ЗИ   | ОК-2, ОК-4, ОПК- 5, ОПК-6, ПК-1, ПК-13 | Тест, контрольная работа, защита лабораторных работ |
| 6 | Организационное обеспечение информационной безопасности Подготовка (переподготовка) и повышение квалификации специалистов в области ЗИ. Организация контроля состояния ЗИ. Организация ЗИ на объектах органов государственной власти и управления   | ОК-2, ОК-4, ОПК- 5, ОПК-6, ПК-1, ПК-13 | Тест, контрольная работа, защита лабораторных работ |

### **7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности**

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на

бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

## **8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)**

### **8.1 Перечень учебной литературы, необходимой для освоения дисциплины**

#### *Основная*

1. Остапенко Г.А., Мешкова Е.А. Информационные операции и атаки в со-цнотехннческих системах: организационно-правовые аспекты противодействия: Учебное пособие / Под редакцией Ю.Н. Лаврухина. - М: Горячая линия - Телеком, 2007. - 295 с.

2. Остапенко Г.А., Остапенко О. А., Попов Е.А., Бутузов В.В. Риски систем: учеб, пособие [Электронный ресурс]. - Электрон.текстовые. граф, данные (2.11Мб).- Воронеж : ВГТУ.

3. Остапенко О.А. Обеспечение информационно-психологической безопасности: учеб, пособие [Электронный ресурс]. / О.А. Остапенко. П.А. Маслнхов. Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет». 2013. 235 с.

#### *Дополнительная*

1. Остапенко О.А., Батищев Р.В. Опасность, ущербы и риски систем: учеб, пособие / О.А. Остапенко. Р.В. Батищев - Воронеж: НОУВПО «Международный институт компьютерных технологий». 2007. - 206 с.

**8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:**

1. <http://www.eios.vorstu.ru> (электронная информационно-обучающая система ВГТУ)

2. <http://e.lanbook.com/> (ЭБС Лань)

3. <http://znanium.com/> (ЭБС Знаниум)

4. <http://IPRbookshop.ru/> (ЭБС IPRbooks (Айбукс))

## **9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА**

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

## 10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Организационное и правовое обеспечение информационной безопасности» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков в соответствии со следующей тематикой разделов курса.

| № п.п | Наименование практических занятия  |
|-------|--|
| 1.    | Основные понятия в области организационно-правового обеспечения информационной безопасности  |
| 2.    | Основы теории государства и права как фундаментальной дисциплины для изучения организационно-правового обеспечения информационной безопасности |
| 3.    | Система законодательного регулирования общественных отношений в области обеспечения информационной безопасности                                |
| 4.    | Конституционные основы обеспечения информационной безопасности в РФ  |
| 5.    | Регламентация вопросов обеспечения информационной безопасности в Гражданском кодексе РФ  |
| 6.    | Закон РФ «О государственной тайне»   |
| 7.    | Федеральные законы «Об информации, информатизации и защите информации» и «Об участии в международном информационном обмене»                    |
| 8.    | Законы РФ «Об авторском праве и смежных правах». «О правовой охране программ для электронно-вычислительных машин и баз данных»                 |
| 9.    | Регламентация вопросов ЗИ в Федеральных законах общего характера   |
| 10.   | Международное законодательство в области обеспечения информационной безопасности и защиты информации   |
| 11.   | Основы организации обеспечения информационной безопасности и ЗИ  |
| 12.   | Система документов в области обеспечения информационной безопасности и защиты информации   |
| 13.   | Лицензирование деятельности в области ЗИ   |
| 14.   | Сертификация средств ЗИ  |
| 15.   | Аттестация объектов по выполнению требований обеспечения защиты информации   |
| 16.   | Подготовка (переподготовка) и повышение квалификации специалистов в области ЗИ   |
| 17.   | Организация контроля состояния ЗИ  |
| 18.   | Организация ЗИ на объектах органов государственной власти и управления   |

Занятия проводятся путем решения конкретных задач в аудитории.

| Вид учебных занятий | Деятельность студента   |
|---------------------|---|
| Лекция              | Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой ли- |



|  |   |
|--|---|
|  | <p>тературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.</p>   |
| <p>Практическое занятие</p>                  | <p>Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.</p>  |
| <p>Самостоятельная работа</p>                | <p>Самостоятельная работа студентов способствует глубокому усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие:</p> <ul style="list-style-type: none"> <li>- работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций;</li> <li>- выполнение домашних заданий и расчетов;</li> <li>- работа над темами для самостоятельного изучения;</li> <li>- участие в работе студенческих научных конференций, олимпиад;</li> <li>- подготовка к промежуточной аттестации.</li> </ul> |
| <p>Подготовка к промежуточной аттестации</p> | <p>Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.</p>  |