**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
**Московский областной филиал**

**Факультет государственного управления и права**
**Кафедра правового обеспечения государственной и муниципальной службы**

УТВЕРЖДЕНО
Директор
Московского областного
филиала РАНХиГС

Электронная подпись

**ПРОГРАММА СПЕЦИАЛИТЕТА**

Правовое обеспечение национальной безопасности,
государственно-правовая специализация
*(наименование образовательной программы)*

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
## реализуемой без применения электронного (онлайн) курса

Б1.В.02.05 Правовое обеспечение информационной безопасности
*(код и наименование РПД)*

*40.05.01 Правовое обеспечение национальной безопасности*
*(код, наименование направления подготовки/специальности)*

*очная*
*(форма(формы) обучения)*

Год набора - 2025

Красногорск, 2024 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
00DAA02066BBB2FFF23A159B9219BEBE55
Владелец: Арсенян Арташес Завенович
Действителен: с 23.10.2023 до 15.01.2025

**Автор(ы)–составитель(и):**
Кандидат юридических наук, доцент Богмацера Эдуард Викторович

Заведующий кафедрой правового обеспечения государственной и муниципальной службы Богмацера Эдуард Викторович

Рабочая программа дисциплины *«Б1.В.02.05 Правовое обеспечение информационной безопасности»* рассмотрена и одобрена на заседании кафедры правового обеспечения государственной и муниципальной службы
Протокол от 29 августа 2024 г. № 12.

**СОДЕРЖАНИЕ**

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения программы ..... 4

2. Объем и место дисциплины (модуля) в структуре образовательной программы ..... 8

3.Содержание и структура дисциплины (модуля) ..... 8

4. Материалы текущего контроля успеваемости обучающихся ..... 12

6. Методические материалы для освоения дисциплины ..... 22

7. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет" ..... 26

7.1. Основная литература. ..... 26

7.2. Дополнительная литература ..... 26

7.3. Интернет-ресурсы, справочные системы. ..... 28

7.4. Интернет ресурсы ..... 29

7.5. Иные источники ..... 29

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы ..... 29

**1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения программы**

1.1. Дисциплина Б1.В.02.05 «Правовое обеспечение информационной безопасности» обеспечивает овладение следующими компетенциями:

| Код компетенции | Наименование компетенции | Код этапа освоения компетенции | Наименование этапа освоения компетенции |
|---|---|---|---|
| ПКрОС-1 | Способность обеспечивать безопасность личности, общества, государства правовыми средствами | ПКрОС-1/З.1 | - способность к определению объектов безопасности личности, общества, государства и их жизненно важных интересов;<br>- способность к прогнозированию, выявлению, анализу и оценке угроз и рисков безопасности личности, общества, государства, в том числе с применением риск- ориентированного подхода;<br>- способность выработки правовых мер по нейтрализации угроз безопасности личности, общества, государства; |

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

| **Профессиональные действия** | **Код этапа освоения компетен-ции** | **Результаты обучения** |
|---|---|---|
| Федеральный закон "О государственной гражданской службе Российской Федерации" от 27.07.2004 N 79-ФЗ<br>Профессиональные навыки: эффективного руководства органом (подразделением); оперативного принятия и реализации управленческих решений, взаимодействия с другими государственными органами (подразделениями); | ПКр ОС-1/З.1 | **на уровне знаний:**<br>- знать законодательство в избранной и смежных сферах деятельности;<br>- знать особенности осуществления избранной и смежных форм деятельности;<br>- знать формы и механизмы взаимодействия Государственных органов в процессе их деятельности. |
| | | **на уровне умений:**<br>- применять нормы права в конкретной сфере деятельности;<br>- грамотно, в соответствии с |

| | | |
|---|---|---|
| осуществления нормотворческой деятельности, эффективного планирования работы, организации и осуществления контроля, анализа и прогнозирования последствий принимаемых решений.<br>Федеральный закон "О прокуратуре Российской Федерации" от 17.01.1992 N 2202-1 Профессиональные навыки: эффективного руководства органом (подразделением); оперативного принятия и реализации управленческих решений, взаимодействия с другими государственными органами (подразделениями); осуществления нормотворческой деятельности, эффективного планирования работы, организации и осуществления контроля, анализа и прогнозирования последствий принимаемых решений.<br>Федеральный закон от 3 апреля 1995 г.N 40-ФЗ "О федеральной службе безопасности" Профессиональные навыки: эффективного руководства органом (подразделением); оперативного принятия и реализации управленческих решений, взаимодействия с другими государственными органами (подразделениями); осуществления нормотворческой деятельности, эффективного планирования работы, организации и осуществления контроля, анализа и прогнозирования последствий принимаемых решений. | | законодательством выполнять служебные обязанности;<br>- анализировать практику, разрабатывать, планировать, внедрять управленческие решения;<br>- ориентироваться в быстро меняющейся обстановке и оперативно реагировать на изменения.<br>**на уровне навыков:**<br>- аккуратной и грамотной работы с нормативными и служебными документами;<br>- осмысленного подчинения требованиям служебной/рабочей дисциплины;<br>- понимания и соблюдения субординации в своей служебной деятельности и во взаимодействии с другими инстанциями. |

| | | |
|---|---|---|
| Федеральный закон от 28 декабря 2010 г. N 403-ФЗ "О Следственном комитете Российской Федерации<br>Профессиональные навыки: эффективного руководства органом (подразделением); оперативного принятия и реализации управленческих решений, взаимодействия с другими государственными органами (подразделениями); осуществления нормотворческой деятельности, эффективного планирования работы, организации и осуществления контроля, анализа и прогнозирования последствий принимаемых решений.<br>Федеральный закон "О полиции" от 7 февраля 2011 г. N 3-ФЗ<br>Профессиональные навыки: эффективного руководства органом (подразделением); оперативного принятия и реализации управленческих решений, взаимодействия с другими государственными органами (подразделениями); осуществления нормотворческой деятельности, эффективного планирования работы, организации и осуществления контроля, анализа и прогнозирования последствий принимаемых решений.<br>Федеральный закон от 19 июля 2018 г. N 197-ФЗ "О службе в уголовно-исполнительной системе Российской Федерации и о внесении изменений в<br>Закон Российской Федерации "Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы" | | |

| | | |
|---|---|---|
| Профессиональные навыки: эффективного руководства органом (подразделением); оперативного принятия и реализации управленческих решений, взаимодействия с другими государственными органами (подразделениями); осуществления нормотворческой деятельности, эффективного планирования работы, организации и осуществления контроля, анализа и прогнозирования последствий принимаемых решений.<br>Федеральный закон "Об органах принудительного Исполнения Российской Федерации" от 21.07.1997 N 118-Ф<br>Профессиональные навыки: эффективного руководства органом (подразделением); оперативного принятия и реализации управленческих решений, взаимодействия с другими государственными органами (подразделениями); осуществления нормотворческой деятельности, эффективного планирования работы, организации и осуществления контроля, анализа и прогнозирования последствий принимаемых решений. | | |

**2. Объем и место дисциплины (модуля) в структуре образовательной программы**

**Объем дисциплины**

Общая трудоемкость дисциплины составляет 108 ч. (3 з.е.)

Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся: - очная форма обучения: лекции – 24 ч., практические занятия – 24 ч., самостоятельная работа – 56 ч.

**Место дисциплины в структуре ОП ВО**

Дисциплина «Правовое обеспечение информационной безопасности» относится к дисциплинам вариативной части профессионального цикла. Изучается на 4 курсе в 7-м семестре.

Дисциплина входит в Модуль «Обеспечение национальной безопасности».

Для освоения дисциплины «Правовое обеспечение информационной безопасности» обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения дисциплин: «Теория государства и права», «Конституционное право России», «Основы теории национальной безопасности», «Основы правового обеспечения национальной безопасности».

Форма промежуточной аттестации в соответствии с учебным планом – **зачет**

**3.Содержание и структура дисциплины (модуля)**

| № п/п | Наименование тем (разделов) | Объем дисциплины (модуля), час. | | | | | | Форма текущего контроля успеваемости[4], промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|
| | | Всего | Контактная работа обучающихся с преподавателем по видам учебных занятий | | | | СР | |
| | | | Л/ ДОТ | ЛР/ ДОТ | ПЗ/ ДОТ | Л/ ДОТ | | |
| ***Очная форма обучения*** | | | | | | | | |
| | Тема №1 Информационная безопасность (ИБ) РФ и задачи по ее обеспечению. Тема № 2 Нормативно-правовая база обеспечения ИБ в России. Тема № 3 Информация как объект правового регулирования и защиты Тема № 4 Система субъектов обеспечения ИБ в России и их правовой статус. Тема № 5 Преступность в информационной сфере и ее криминологическая и уголовно-правовая правовая | 104 | 24 | | 24 | | 56 | УО Зачет |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | характеристика.<br>Тема № 6 Правовая защита личности в информационной сфере.<br>Тема № 7 Правовой режим государственной тайны и меры по ее обеспечению.<br>Тема № 8 Правовые и организационные способы защиты информации в сфере высоких технологий.<br>Тема № 9 Правовое обеспечение права интеллектуальной собственности (ПИС).<br>Тема №10 Правовая защита коммерческой тайны (КТ).<br>Тема № 11 Правовое регулирование отношений в сфере лицензирования и сертификации.<br>Тема № 12 Предупреждение преступлений в информационной сфере в современной России<br>Тема № 13 Юридическая ответственность за правонарушения в сфере ИБ | | | | | | | |
| Промежуточная аттестация | | 4 | | | | 4 | | Зачет |
| **Всего:** | | **108** | **24** | | **24** | **4** | **56** | |

*Примечание: УО – устный опрос*

**Содержание дисциплины (модуля)**

**Тема №1 Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.**

Понятие ИБ и информационного общества. Цели, задачи и принципы обеспечения ИБ. Угроза национальной безопасности и их виды. Информационные войны и информационное оружие. Информационный терроризм. Информационное общество в РФ и его характеристики. Информационная сфера и ее области. Национальные интересы России в информационной сфере. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.

**Тема № 2 Нормативно-правовая база обеспечения ИБ в России.**

Понятие правового обеспечения и правовой защиты. История формирования законодательства РФ об информации и ее защите. Система нормативно-правовых актов России, регулирующих отношения в сфере ИБ. Международно-правовые нормы и стандарты в сфере ИБ. Место Окинавской Хартии глобального информационного общества в системе международно-правовых актов обеспечения ИБ. Предмет и метод правового регулирования в сфере ИБ страны. Информационное право. Информационные отношения. Виды ведомственных и корпоративных норм и их место в системе правового регулирования ИБ в РФ. Правовое регулирование деятельности средств массовой информации. Основные тенденции развития законодательства РФ в сфере ИБ. Особенности стандартизации нормативной базы в сфере ИБ в современном мире.

**Тема № 3 . Информация как объект правового регулирования и защиты.**

Информация, ее виды и признаки. Информация как объект юридической защиты. Информационная сфера общества и ее характеристики. Информационные ресурсы. Понятие и виды. Виды и источники информации, подлежащие защите. Правовой режим защиты государственной тайны. Способы обеспечения сохранности информации, составляющей государственную тайну и система контроля за состоянием ее защиты. Основные принципы засекречивания информации. Конфиденциальная информация и возможные каналы ее утечки. Информационная инфраструктура и информационная среда. Их структура и характеристики. Международный опыт деятельности по правовому обеспечению ИБ и основные направления его развития. Государственная политика РФ в сфере правового обеспечения ИБ.

**Тема № 4 Система субъектов обеспечения ИБ в России и их правовой статус.**

Понятие государственного управления в сфере обеспечения ИБ. Система органов государственной власти, обеспечивающая ИБ и особенности их компетентности. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами. Служба Специальной связи и информации Федеральной службы охраны РФ, ее задачи и правовой статус.

**Тема № 5 Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.**

Понятие и виды преступности в информационной сфере. Основные этапы и тенденции развития компьютерной преступности в России. Особенности детерминации преступлений, совершаемых в информационной сфере. Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет. Понятие преступления в сфере компьютерной информации. Виды преступлений в сфере компьютерной информации. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Особенности объективных признаков компьютерных преступлений. Основные способы их совершения. Субъективные признаки компьютерных преступлений. Характерные мотивы и цели их совершения. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.

**Тема № 6 Правовая защита личности в информационной сфере.**

Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере. Конституционные гарантии правовой охраны прав личности в информационной сфере. Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни. Правовой механизм защиты права на неприкосновенность частной жизни. Врачебная тайна как институт защиты

интересов личности. Защита права на личную информацию с ограниченным доступом. Персональная тайна и ее виды. Обработка и правовая охрана персональных данных. Правовая база обеспечения защиты личности от воздействия «вредной» информации. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.

**Тема № 7 Правовой режим государственной тайны и меры по ее обеспечению.**

Понятие государственной тайны и правового режима ее обеспечения. Принципы и механизм отнесения сведений к государственной тайне (ГТ). Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну. Субъекты обеспечения режима государственной тайны и их правовой статус. Организационно-правовые меры защиты ГТ. Допуск и доступ к ГТ. Обеспечение ИБ при международном обмене информацией. Система контроля за режимом обеспечения ГТ. Особенности юридической ответственности за нарушение режима обеспечения ГТ.

**Тема № 8 Правовые и организационные способы защиты информации в сфере высоких технологий.**

Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий. Компьютерные преступления и особенности их идентификации и предупреждения. Правовые основы применения «электронной цифровой подписи» (ЭЦП). Криптографическая защита информации (КЗИ). Правовые и организационные способы обеспечения КЗИ в России и других странах современного мира. Контроль за разработкой, производством и применением криптографических средств. КЗИ и их правовая основа. Органы лицензирования и сертификации и их правовой статус

**Тема № 9 Правовое обеспечение права интеллектуальной собственности (ПИС).**

Понятие интеллектуальной собственности и ее правовой статус. Законодательство РФ об авторских и смежных правах. Особенности правоотношений, обеспечивающих ПИС. Объекты и субъекты ПИС. Правовой механизм обеспечения защиты авторских и смежных прав. Государственная регистрация ПИС. Особенности правовой защиты программ для электронных вычислительных машин и баз данных. Патентное право и патентные правоотношения. Правовой статус участников. Сфера действия патентного законодательства. Показатели и условия патентоспособности. Правовой статус автора и патентообладателя. Механизм правовой защиты прав автора и патентообладателей. Товарный знак и механизм его правовой защиты. Государственная регистрация товарного знака. Прекращение права на товарный знак. Программы для ЭВМ и механизм их правовой защиты. Правовое регулирование договорных отношений в сфере ПИС.

**Тема №10 Правовая защита коммерческой тайны (КТ).**

Понятие КТ и ее правовой статус. Признаки КТ. Защита КТ и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель. Объекты защиты КТ. Особенности правового обеспечения режима КТ. Промышленный шпионаж и его объекты. Критерии определения секретности при определении режима КТ. Организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений. Режим представления информации, составляющей КТ органам государственной власти. Юридическая ответственность за нарушения режима обеспечения КТ.

**Тема № 11 Правовое регулирование отношений в сфере лицензирования и сертификации.**

Правовое обеспечение деятельности организаций по лицензированию и сертификации в сфере ИБ. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию в сфере ИБ. Система государственного лицензирования в сфере ИБ и ее функции. Субъекты лицензирования в сфере ИБ и их правовой статус. Порядок лицензирования, приостановления или аннулирования действия лицензии. Специальная экспертиза предприятия и государственная аттестация их руководителей. Контроль за условиями обеспечения ИБ лицензиатами. Понятие сертификации средств защиты информации (ССЗИ) и ее правовая основа в РФ. Цели создания системы ССЗИ. Организационная структура системы ССЗИ и особенности правового статуса ее субъектов. Объекты сертификационной деятельности и режимы сертификации. Особенности аттестации и контроля за деятельностью объектов обработки особо важной информации. Юридическая ответственность за нарушением правил лицензирования и сертификации.

**Тема № 12 Предупреждение преступлений в информационной сфере в современной России.**

Информационная безопасность России и задачи по ее обеспечению. Система детерминант преступности в информационной сфере. Уровневый подход. Мотивационная сфера лиц, совершающих правонарушения в сфере ИБ. Субъекты деятельности по обеспечению противодействия правонарушениям в сфере ИБ и их правовой статус. Оперативно-розыскные и криминалистические мероприятия по борьбе с преступлениями в сфере ИБ. Особенности расследования преступлений в сфере ИБ. Совершенствование правовых норм как средство обеспечения профилактического воздействия на отношения в сфере ИБ. Зарубежный опыт борьбы с преступностью в сфере ИБ.

**Тема № 13 Юридическая ответственность за правонарушения в сфере ИБ.**

Понятие и виды юридической ответственности (ЮО) за правонарушения в сфере ИБ. Уголовная ответственность за правонарушения в сфере ИБ и ее особенности.

Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны. Уголовная ответственность за компьютерные преступления и особенности их реализации в современной России. Правовое регулирование отношений, связанных с привлечением к ответственности лиц, совершивших административные правонарушения в сфере ИБ. Составы административных правонарушений, посягающих на ИБ страны. Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

## 4. Материалы текущего контроля успеваемости обучающихся

В ходе реализации дисциплины «Правовое обеспечение информационной безопасности» используются следующие методы текущего контроля успеваемости обучающихся:

| Тема (раздел) | Методы текущего контроля успеваемости |
|---|---|
| Тема 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению. | УО |
| Тема 2. Нормативно-правовая база обеспечения ИБ в России. | УО |
| Тема 3. Информация как объект правового регулирования и защиты. | УО |
| Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус. | УО |
| Тема 5. Преступность в информационной сфере и ее | УО |

| | |
|---|---|
| криминологическая и уголовно-правовая характеристика. | |
| Тема 6. Правовая защита личности в информационной сфере | УО |
| Тема 7. Правовой режим государственной тайны и меры по ее обеспечению. | УО |
| Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий. | УО |
| Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС) | УО |
| Тема 10. Правовая защита коммерческой тайны (КТ). | УО |
| Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации. | УО |
| Тема 12. Предупреждение преступлений в информационной сфере в современной России. | УО |
| Тема 13. Юридическая ответственность за правонарушения в сфере ИБ | УО |

Зачет проводится с применением метода устного опроса и собеседования по вопросам к зачету.

**Материалы текущего контроля успеваемости обучающихся**

**Примерные оценочные материалы по теме 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.**

**Вопросы для устного опроса.**

Понятие ИБ и информационного общества. Цели, задачи и принципы обеспечения ИБ. Угроза национальной безопасности и их виды. Информационные войны и информационное оружие. Информационный терроризм. Информационное общество в РФ и его характеристики. Информационная сфера и ее области. Национальные интересы России в информационной сфере. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.

**Примерные оценочные материалы по теме 2. Нормативно-правовая база обеспечения ИБ в России.**

**Вопросы для устного опроса.**

Понятие правового обеспечения и правовой защиты. История формирования законодательства РФ об информации и ее защите. Система нормативно-правовых актов России, регулирующих отношения в сфере ИБ. Международно-правовые нормы и стандарты в сфере ИБ. Место Окинавской Хартии глобального информационного общества в системе международно-правовых актов обеспечения ИБ. Предмет и метод правового регулирования в сфере ИБ страны. Информационное право. Информационные отношения. Виды ведомственных и корпоративных норм и их место в системе правового регулирования ИБ в РФ. Правовое регулирование деятельности средств массовой информации. Основные тенденции развития законодательства РФ в сфере ИБ. Особенности стандартизации нормативной базы в сфере ИБ в современном мире.

**Примерные оценочные материалы по теме 3. Информация как объект правового регулирования и защиты.**

**Вопросы для устного опроса.**

Информация, ее виды и признаки. Информация как объект юридической защиты Информационная сфера общества и ее характеристики. Информационные ресурсы. Понятие и виды. Виды и источники информации, подлежащие защите. Правовой режим защиты государственной тайны. Способы обеспечения сохранности информации, составляющей государственную тайну и система контроля за состоянием ее защиты. Основные принципы засекречивания информации. Конфиденциальная информация и

возможные каналы ее утечки. Информационная инфраструктура и информационная среда. Их структура и характеристики. Международный опыт деятельности по правовому обеспечению ИБ и основные направления его развития. Государственная политика РФ в сфере правового обеспечения ИБ.

**Примерные оценочные материалы по теме 4. Система субъектов обеспечения ИБ в России и их правовой статус.**

**Вопросы для устного опроса.**

Понятие государственного управления в сфере обеспечения ИБ. Система органов государственной власти, обеспечивающая ИБ и особенности их компетентности. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами. Служба Специальной связи и информации Федеральной службы охраны РФ, ее задачи и правовой статус.

**Примерные оценочные материалы по теме 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.**

**Вопросы для устного опроса.**

Понятие и виды преступности в информационной сфере. Основные этапы и тенденции развития компьютерной преступности в России. Особенности детерминации преступлений, совершаемых в информационной сфере. Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет. Понятие преступления в сфере компьютерной информации. Виды преступлений в сфере компьютерной информации. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Особенности объективных признаков компьютерных преступлений. Основные способы их совершения. Субъективные признаки компьютерных преступлений. Характерные мотивы и цели их совершения. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.

**Примерные оценочные материалы по теме 6. Правовая защита личности в информационной сфере.**

**Вопросы для устного опроса.**

Система и структура нормативных актов, обеспечивающих защиту прав личности информационной сфере. Конституционные гарантии правовой охраны прав личности информационной сфере. Правовые средства защиты права на доступ к информации неприкосновенности частной жизни. Правовой механизм защиты права на неприкосновенность частной жизни. Врачебная тайна как институт защиты интересов личности. Защита права на личную информацию с ограниченным доступом. Персональная тайна и ее виды. Обработка и правовая охрана персональных данных. Правовая база обеспечения защиты личности от воздействия «вредной» информации. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.

**Примерные оценочные материалы по теме 7. Правовой режим государственной тайны и меры по ее обеспечению.**

**Вопросы для устного опроса.**

Понятие государственной тайны и правового режима ее обеспечения. Принципы и механизм отнесения сведений к государственной тайне (ГТ). Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну.

Субъекты обеспечения режима государственной тайны и их правовой статус. Организационно-правовые меры защиты ГТ. Допуск и доступ к ГТ. Обеспечение ИБ при международном обмене информацией. Система контроля за режимом обеспечения ГТ. Особенности юридической ответственности за нарушение режима обеспечения ГТ.

**Примерные оценочные материалы по теме 8. Правовые и организационные способы защиты информации в сфере высоких технологий.**

**Вопросы для устного опроса.**

Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий. Компьютерные преступления и особенности их идентификации и предупреждения. Правовые основы применения «электронной цифровой подписи» (ЭЦП). Криптографическая защита информации (КЗИ). Правовые и организационные способы обеспечения КЗИ в России и других странах современного мира. Контроль за разработкой, производством и применением криптографических средств. КЗИ и их правовая основа. Органы лицензирования и сертификации и их правовой статус.

**Примерные оценочные материалы по теме 9. Правовое обеспечение права интеллектуальной собственности (ПИС).**

**Вопросы для устного опроса.**

Понятие интеллектуальной собственности и ее правовой статус.
Законодательство РФ об авторских и смежных правах. Особенности правоотношений, обеспечивающих ПИС. Объекты и субъекты ПИС. Правовой механизм обеспечения защиты авторских и смежных прав. Государственная регистрация ПИС. Особенности правовой защиты программ для электронных вычислительных машин и баз данных. Патентное право и патентные правоотношения. Правовой статус участников. Сфера действия патентного законодательства. Показатели и условия патентоспособности. Правовой статус автора и патентообладателя. Механизм правовой защиты прав автора и патентообладателей. Товарный знак и механизм его правовой защиты. Государственная регистрация товарного знака. Прекращение права на товарный знак. Программы для ЭВМ и механизм их правовой защиты. Правовое регулирование договорных отношений в сфере ПИС.

**Примерные оценочные материалы по теме 10. Правовая защита коммерческой тайны (КТ).**

**Вопросы для устного опроса.**

Понятие КТ и ее правовой статус. Признаки КТ. Защита КТ и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель. Объекты защиты КТ. Особенности правового обеспечения режима КТ. Промышленный шпионаж и его объекты. Критерии определения секретности при определении режима КТ. Организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений. Режим представления информации, составляющей КТ органам государственной власти. Юридическая ответственность за нарушения режима обеспечения КТ.

**Примерные оценочные материалы по теме 11. Правовое регулирование отношений в сфере лицензирования и сертификации.**

**Вопросы для устного опроса.**

Правовое обеспечение деятельности организаций по лицензированию и сертификации в сфере ИБ. Понятие лицензирования по российскому законодательству.

Виды деятельности, подлежащие лицензированию в сфере ИБ. Система государственного лицензирования в сфере ИБ и ее функции. Субъекты лицензирования в сфере ИБ и их правовой статус. Порядок лицензирования, приостановления или аннулирования действия лицензии. Специальная экспертиза предприятия и государственная аттестация их руководителей. Контроль за условиями обеспечения ИБ лицензиатами. Понятие сертификации средств защиты информации (ССЗИ) и ее правовая основа в РФ. Цели создания системы ССЗИ. Организационная структура системы ССЗИ и особенности правового статуса ее субъектов. Объекты сертификационной деятельности и режимы сертификации. Особенности аттестации и контроля за деятельностью объектов обработки особо важной информации. Юридическая ответственность за нарушением правил лицензирования и сертификации.

**Примерные оценочные материалы по теме 12. Предупреждение преступлений в информационной сфере в современной России.**

**Вопросы для устного опроса.**

Информационная безопасность России и задачи по ее обеспечению. Система детерминант преступности в информационной сфере. Уровневый подход. Мотивационная сфера лиц, совершающих правонарушения в сфере ИБ. Субъекты деятельности по обеспечению противодействия правонарушениям в сфере ИБ и их правовой статус. Оперативно-розыскные и криминалистические мероприятия по борьбе с преступлениями в сфере ИБ. Особенности расследования преступлений в сфере ИБ. Совершенствование правовых норм как средство обеспечения профилактического воздействия на отношения в сфере ИБ. Зарубежный опыт борьбы с преступностью в сфере ИБ.

**Примерные оценочные материалы по теме 13. Юридическая ответственность за правонарушения в сфере ИБ.**

**Вопросы для устного опроса.**

Понятие и виды юридической ответственности (ЮО) за правонарушения в сфере ИБ. Уголовная ответственность за правонарушения в сфере ИБ и ее особенности. Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны. Уголовная ответственность за компьютерные преступления и особенности их реализации в современной России. Правовое регулирование отношений, связанных с привлечением к ответственности лиц, совершивших административные правонарушения в сфере ИБ. Составы административных правонарушений, посягающих на ИБ страны. Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

**Критерии оценивания устных ответов в рамках текущего контроля**

| Критерии | Баллы |
|---|---|
| Ответ дан полностью, ответ верный, ответ дан с использованием действующих нормативных правовых актов, обучающийся точно использует юридическую терминологию, ответ изложен последовательно, ответ развёрнутый, аргументированный, сформированы умения квалифицированно толковать нормативные правовые акты и давать юридические заключения. | 1 |
| Ответ дан полностью, ответ верный, ответ | 0,75 |

| | |
|---|---|
| дан с использованием действующих нормативных правовых актов, обучающийся точно использует юридическую терминологию, но ответ изложен непоследовательно, ответ односложный, неаргументированный, сформированы умения квалифицированно толковать нормативные правовые акты и давать юридические заключения | |
| Ответ дан полностью, ответ верный, ответ дан с использованием действующих нормативных правовых актов, обучающийся точно использует юридическую терминологию, но ответ изложен непоследовательно, ответ односложный, неаргументированный, не использованы акты высших судов и иная необходимая судебная практика, умения квалифицированно толковать нормативные правовые акты и давать юридические заключения недостаточно сформированы. | 0,5 |
| Ответ дан не полностью либо ответ частично верный, ответ дан с использованием действующих нормативных правовых актов, но изложен непоследовательно, ответ односложный, неаргументированный, не использованы акты высших судов и иная необходимая судебная практика; обучающийся испытывает трудности с толкованием нормативных правовых актов и дачей юридических заключений. | 0,25 |
| Ответ неверный либо ответ отсутствует, либо дан с использованием недействующих нормативных правовых актов, обучающийся не умеет толковать нормативные правовые акты и давать юридические заключения. | 0 |

**Оценочные материалы промежуточной аттестации**

| Код компетенции | Наименование компетенции | Код компонента и(или) этапа компетенции | Наименование компонента и(или) этапа компетенции |
|---|---|---|---|
| ПКс ОС-1 | Способность выявлять, пресекать и раскрывать преступления, посягающие на национальную безопасность и ее виды. | ПКс ОС-1 | - способность обнаружить действие или бездействие, содержащее признаки, характеризующие его как |

| | | | |
|---|---|---|---|
| | | | преступление, посягающее на национальную безопасность и ее виды;<br>- способность осуществлять действия, обеспечивающие прекращение уже начатых преступлений, посягающих на национальную безопасность и ее виды;<br>-способность получить информацию, дающую основание для выдвижения версии о совершении преступления, посягающего на национальную безопасность и ее виды определенным лицом (лицами), а также проверить и отвергнуть все иные взаимоисключающие ее версии. |
| **Компонент компетенции** | **Индикатор оценивания** | | **Критерий оценивания** |
| ПКс ОС-1 | комплексный подход к выявлению преступлений, посягающих на национальную безопасность и ее виды комплексность система мер, позволяющая осуществить оперативность пресечение преступлений в кратчайшие сроки способствование раскрытию преступлений, посягающих на национальную безопасность и ее виды результативность | | |

**5. Оценочные материалы промежуточной аттестации**

**Рекомендуемые оценочные материалы промежуточной аттестации**

**Вопросы для подготовки к зачету по дисциплине**

**«Правовое обеспечение информационной безопасности»**

1. Понятие информационной безопасности.
2. Цели, задачи и принципы обеспечения ИБ.
3. Угрозы ИБ. Понятие, виды.
4. Понятие и характеристика информационного общества в РФ.
5. Понятие и области информационной сферы.
6. Национальные интересы России в информационной сфере.

7. Понятие и принципы государственной политики РФ в сфере обеспечения ИБ.

8. Понятие правового обеспечения ИБ.

9. Информационное право России в структуре ее правовой системы.

10.Международно-правовые документы, регулирующие сферу ИБ. Общая характеристика и место в правовой системе РФ.

11. Средства массовой информации и их правовой статус.

12. Информация как объект юридической защиты.

13. Информационная сфера общества и ее характеристика.

14. Виды и источники информации, подлежащие защите.

15. Понятие государственной тайны и правовой режим ее защиты.

16. Способы обеспечения государственной тайны и система контроля за состоянием ее защиты.

17. Понятие и характеристики информационной структуры и информационной среды.

18. Государственная политика в сфере правового обеспечения ИБ.

19. Органы государственной власти, обеспечивающие ИБ и их правовой статус.

20. Особенности правового статуса органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами.

21. Служба Специальной связи и информации Федеральной службы охраны РФ. Задачи и правовой статус.

22. Понятие и виды преступлений в информационной сфере.

23. Особенности детерминации преступлений, совершаемых в информационной сфере.

24. Компьютерные преступления. Особенности идентификации, расследования и предупреждения.

25. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.

26. Конституционные гарантии правовой охраны прав личности в информационной сфере.

27. Защита права на личную информацию с ограниченным доступом.

28. Обработка и правовая охрана персональных данных.

29. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.

30. Государственная тайна (ГТ) и правовой режим ее обеспечения.

31. Процедура засекречивания и рассекречивания сведений, составляющих ГТ.

32. Организационно-правовые меры защиты ГТ.

33. Юридическая ответственность за нарушение режима обеспечения ГТ.

34. Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям.

35. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий.

36. Понятие электронной цифровой подписи. «Правовые» основы ее применения.

37. Понятие криптографической защиты информации (КЗИ).

38. Правовые и организационные способы обеспечения КЗИ в России и других странах.

39. Органы лицензирования и сертификации сферы ИБ и их правовой статус.

40. Понятие интеллектуальной собственности и ее правовой статус в РФ.

41. Правовой механизм обеспечения авторских и смежных прав.

42. Правовая защита программ для ЭВМ и баз данных.

43. Правовой статус участников патентных правоотношений.

44. Механизм правовой защиты автора и патентообладателя.

45. Товарный знак и механизм его правовой защиты.

46. Правовое регулирование договорных отношений в сфере права интеллектуальной собственности.

47. Коммерческая тайна и ее правовой статус.

48. Способы правового закрепления права собственности на промышленный образец и полезную модель.

49. Организационные меры обеспечения защиты коммерческой тайны и особенности их реализации в рамках гражданско-правовых (договорных) отношений.

50. Режим представления информации, составляющей коммерческую тайну органам государственной власти.

51. Понятие лицензирования по российскому законодательству.

52. Виды деятельности, подлежащие лицензированию в сфере ИБ.

53. Система государственного лицензирования в сфере ИБ и ее функции.

54. Понятие сертификации средств защиты информации и ее правовая основа в РФ.

55. Объекты сертификационной деятельности и режимы сертификации в сфере ИБ в России.

56. Юридическая ответственности за нарушение правил лицензирования и сертификации в сфере ИБ.

57. ИБ России и задачи органов государственной власти по предупреждению деяний, на нее посягающих.

58. Применение уровневого подхода к анализу системы детерминант преступности в информационной сфере.

59. Оперативно-розыскные и криминалистические мероприятия в борьбе с преступлениями в сфере ИБ.

60. Понятие и виды юридической ответственности за правонарушения в сфере ИБ.

61. Уголовная ответственность за правонарушения в сфере ИБ и ее особенности.

62. Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны.

63. Уголовная ответственность за компьютерные преступления и особенности ее реализации в современной России.

64. Составы административных правонарушений, посягающих на ИБ страны.

65. Особенности производства по делам об административных правонарушениях, посягающих на ИБ.

66. Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус

**Шкала оценивания.**

Знания, умения и навыки обучающегося на зачете оцениваются как «зачтено» или «не зачтено» с возможностью последующего конвертирования в систему ESTC и БРС. Итоговая оценка по дисциплине является суммой баллов результатов текущего контроля и промежуточных аттестаций.

| № п/п | Вид отчетности | Баллы | Оценка ECTS/балл |
|---|---|---|---|
| Текущий контроль: | | | |
| 1. | Работа на практических занятиях: | 12/36 | |
| 2. | Опрос | 0,25 - 1 | 3/12 |
| 3. | Кейс-задания | 0,5 - 1 | 6/12 |
| 4. | Тестовые задания | 0,25 - 1 | 3/12 |

| Промежуточная аттестация (экзамен): | | | |
|---|---|---|---|
| | Зачет | | до 64 |
| 1. | Ответ на теоретический вопрос | от 20 до 64 | от 20 до 64 |
| ИТОГО: | | | |

**Конвертирование итоговой оценки по дисциплине в систему ESTC и БРС:**

| **Оценка** | **Критерий оценивания** | **Результаты обучения** |
|---|---|---|
| P (Passed) – «зачтено» (14-64 баллов) | **системность** системный подход к определению объектов безопасности личности, общества, государства и их жизненно важных интересов объективность выявление объективных обстоятельств, способствующих возникновению угроз и рисков безопасности личности, общества, государства; **оперативность** система правовых мер, позволяющая осуществить нейтрализацию угроз безопасности личности, общества, государства в кратчайшие сроки | **на уровне знаний:** - знать законодательство в избранной и смежных сферах деятельности; - знать особенности осуществления избранной и смежных форм деятельности; - знать формы и механизмы взаимодействия государственных органов в процессе их деятельности. **на уровне умений:** - применять нормы права в конкретной сфере деятельности; - грамотно, в соответствии с законодательством выполнять служебные обязанности; - анализировать практику, разрабатывать, планировать, внедрять управленческие решения; ориентироваться в быстро меняющейся обстановке и оперативно реагировать на изменения. **на уровне навыков:** - аккуратной и грамотной работы с нормативными и служебными документами; - осмысленного подчинения требованиям служебной/рабочей дисциплины; - понимания и соблюдения субординации в своей служебной деятельности и во взаимодействии с другими инстанциями. |
| NP (Not passed) – «не зачтено» (0- 14 баллов) | **системность** отсутствует системный подход к определению | |

| | | |
|---|---|---|
| | объектов безопасности личности, общества, государства и их жизненно важных интересов<br>**объективность**<br>неумение выявить объективные обстоятельства, способствующие возникновению угроз и рисков безопасности личности, общества, государства;<br>**оперативность**<br>неспособность применения системы правовых мер, позволяющей осуществить нейтрализацию угроз безопасности личности, общества, государства в кратчайшие сроки | |

## 6. Методические материалы для освоения дисциплины

К зачету по дисциплине «Правовое обеспечение информационной безопасности» необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период зачетно-экзаменационной сессии, как правило, показывают не слишком удовлетворительные результаты.

В самом начале освоения дисциплины познакомьтесь со следующей учебно-методической документацией:

- рабочей программой дисциплины «Правовое обеспечение информационной безопасности»;
- перечнем знаний, умений и навыков, которыми обучающийся должен овладеть,
- тематическими планами занятий,
- контрольными мероприятиями,
- учебником, учебными пособиями, а также электронными ресурсами,
- перечнем вопросов к зачету.

После этого должно сформироваться четкое представление об объеме и характере знаний, умений и навыков, которыми необходимо овладеть по дисциплине. Систематическое выполнение заданий на практических занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета.

Промежуточная аттестация по дисциплине «Правовое обеспечение информационной безопасности» проводится в соответствии с Учебным планом по семестрам – в 7 семестре для очной формы обучения в виде зачета.

Вопросы по тематике дисциплины «Правовое обеспечение информационной безопасности» включены в перечень вопросов для подготовки к экзамену по модулю «Обеспечение национальной безопасности». Обучающийся допускается к зачету по дисциплине в случае выполнения им учебного плана по дисциплине. В случае наличия учебной задолженности обучающийся отрабатывает пропущенные занятия в форме, предложенной преподавателем. Обучение по дисциплине «Правовое обеспечение информационной безопасности» предполагает контактную форму работы (лекционные, практические занятия, а также консультации) и самостоятельную работу обучающихся.

***6.1. Методические рекомендации по подготовке к лекционным и практическим занятиям***

Дисциплина «Правовое обеспечение информационной безопасности» ориентирована на освоение обучающимися наиболее полной информации по вопросам правового обеспечения национальной безопасности.

В связи с чем предполагается следующая последовательность в подготовке обучающихся к лекции:

- ознакомление с материалом предыдущей лекции;
- знакомство с тематикой предстоящей лекции (по тематическому плану, представленному в настоящей рабочей программе дисциплины);
- ознакомление с учебными пособиями, учебниками, научными статьями по теме предстоящего лекционного занятия;
- подготовка вопросов лектору по проблеме предстоящей лекции.

Цель практических занятий заключается в ознакомлении обучающихся с различными подходами к исследованию проблемных вопросов обеспечения национальной безопасности. Подготовка к практическим занятиям предполагает проработку ответов на вопросы, предложенные в каждой теме каждого раздела настоящей рабочей программы дисциплины, а также выработку навыков работы с научной юридической литературой и библиографией, справочниками, справочно-правовыми базами.

**Вопросы для самостоятельной подготовки к практическим занятиям**

**Тема 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.**

Понятие ИБ и информационного общества. Цели, задачи и принципы обеспечения ИБ. Угроза национальной безопасности и их виды. Информационные войны и информационное оружие. Информационный терроризм. Информационное общество в РФ и его характеристики. Информационная сфера и ее области. Национальные интересы России в информационной сфере. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.

**Тема 2. Нормативно-правовая база обеспечения ИБ в России.**

Понятие правового обеспечения и правовой защиты. История формирования законодательства РФ об информации и ее защите. Система нормативно-правовых актов России, регулирующих отношения в сфере ИБ. Международно-правовые нормы и стандарты в сфере ИБ. Место Окинавской Хартии глобального информационного общества в системе международно-правовых актов обеспечения ИБ. Предмет и метод правового регулирования в сфере ИБ страны. Информационное право. Информационные отношения. Виды ведомственных и корпоративных норм и их место в системе правового регулирования ИБ в РФ. Правовое регулирование деятельности средств массовой информации. Основные тенденции развития законодательства РФ в сфере ИБ. Особенности стандартизации нормативной базы в сфере ИБ в современном мире.

**Тема 3. Информация как объект правового регулирования и защиты.**

Информация, ее виды и признаки. Информация как объект юридической защиты. Информационная сфера общества и ее характеристики. Информационные ресурсы. Понятие и виды. Виды и источники информации, подлежащие защите. Правовой режим защиты государственной тайны. Способы обеспечения сохранности информации, составляющей государственную тайну и система контроля за состоянием ее защиты. Основные принципы засекречивания информации. Конфиденциальная информация и возможные каналы ее утечки. Информационная инфраструктура и информационная среда. Их структура и характеристики. Международный опыт деятельности по правовому обеспечению ИБ и основные направления его развития. Государственная политика РФ в сфере правового обеспечения ИБ.

**Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус.**

Понятие государственного управления в сфере обеспечения ИБ. Система органов государственной власти, обеспечивающая ИБ и особенности их компетентности. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами. Служба Специальной связи и информации Федеральной службы охраны РФ, ее задачи и правовой статус.

**Тема 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.**

Понятие и виды преступности в информационной сфере. Основные этапы и тенденции развития компьютерной преступности в России. Особенности детерминации преступлений, совершаемых в информационной сфере. Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет. Понятие преступления в сфере компьютерной информации. Виды преступлений в сфере компьютерной информации. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Особенности объективных признаков компьютерных преступлений. Основные способы их совершения. Субъективные признаки компьютерных преступлений. Характерные мотивы и цели их совершения. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.

**Тема 6. Правовая защита личности в информационной сфере.**

Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере. Конституционные гарантии правовой охраны прав личности в информационной сфере. Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни. Правовой механизм защиты права на неприкосновенность частной жизни. Врачебная тайна как институт защиты интересов личности. Защита права на личную информацию с ограниченным доступом. Персональная тайна и ее виды. Обработка и правовая охрана персональных данных. Правовая база обеспечения защиты личности от воздействия «вредной» информации. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.

**Тема 7. Правовой режим государственной тайны и меры по ее обеспечению.**

Понятие государственной тайны и правового режима ее обеспечения. Принципы и механизм отнесения сведений к государственной тайне (ГТ). Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну. Субъекты обеспечения режима государственной тайны и их правовой статус. Организационно-правовые меры защиты ГТ. Допуск и доступ к ГТ. Обеспечение ИБ при международном обмене информацией. Система контроля за режимом обеспечения ГТ. Особенности юридической ответственности за нарушение режима обеспечения ГТ.

**Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий.**

Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий. Компьютерные преступления и особенности их идентификации и предупреждения. Правовые основы применения «электронной цифровой подписи» (ЭЦП). Криптографическая защита информации (КЗИ). Правовые и организационные способы обеспечения КЗИ в России и других странах современного мира. Контроль за разработкой, производством и применением криптографических средств. КЗИ и их правовая основа. Органы лицензирования и сертификации и их правовой статус.

**Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС).**

Понятие интеллектуальной собственности и ее правовой статус. Законодательство РФ об авторских и смежных правах. Особенности правоотношений,

обеспечивающих ПИС. Объекты и субъекты ПИС. Правовой механизм обеспечения защиты авторских и смежных прав. Государственная регистрация ПИС. Особенности правовой защиты программ для электронных вычислительных машин и баз данных. Патентное право и патентные правоотношения. Правовой статус участников. Сфера действия патентного законодательства. Показатели и условия патентоспособности. Правовой статус автора и патентообладателя. Механизм правовой защиты прав автора и патентообладателей. Товарный знак и механизм его правовой защиты. Государственная регистрация товарного знака. Прекращение права на товарный знак. Программы для ЭВМ и механизм их правовой защиты. Правовое регулирование договорных отношений в сфере ПИС.

**Тема 10. Правовая защита коммерческой тайны (КТ).**

Понятие КТ и ее правовой статус. Признаки КТ. Защита КТ и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель. Объекты защиты КТ. Особенности правового обеспечения режима КТ. Промышленный шпионаж и его объекты. Критерии определения секретности при определении режима КТ. Организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений. Режим представления информации, составляющей КТ органам государственной власти. Юридическая ответственность за нарушения режима обеспечения КТ.

**Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации.**

Правовое обеспечение деятельности организаций по лицензированию и сертификации в сфере ИБ. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию в сфере ИБ. Система государственного лицензирования в сфере ИБ и ее функции. Субъекты лицензирования в сфере ИБ и их правовой статус. Порядок лицензирования, приостановления или аннулирования действия лицензии. Специальная экспертиза предприятия и государственная аттестация их руководителей. Контроль за условиями обеспечения ИБ лицензиатами. Понятие сертификации средств защиты информации (ССЗИ) и ее правовая основа в РФ. Цели создания системы ССЗИ. Организационная структура системы ССЗИ и особенности правового статуса ее субъектов. Объекты сертификационной деятельности и режимы сертификации. Особенности аттестации и контроля за деятельностью объектов обработки особо важной информации. Юридическая ответственность за нарушением правил лицензирования и сертификации.

**Тема 12. Предупреждение преступлений в информационной сфере в современной России.**

Информационная безопасность России и задачи по ее обеспечению. Система детерминант преступности в информационной сфере. Уровневый подход. Мотивационная сфера лиц, совершающих правонарушения в сфере ИБ. Субъекты деятельности по обеспечению противодействия правонарушениям в сфере ИБ и их правовой статус. Оперативно-розыскные и криминалистические мероприятия по борьбе с преступлениями в сфере ИБ. Особенности расследования преступлений в сфере ИБ. Совершенствование правовых норм как средство обеспечения профилактического воздействия на отношения в сфере ИБ. Зарубежный опыт борьбы с преступностью в сфере ИБ.

**Тема 13. Юридическая ответственность за правонарушения в сфере ИБ.**

Понятие и виды юридической ответственности (ЮО) за правонарушения в сфере ИБ. Уголовная ответственность за правонарушения в сфере ИБ и ее особенности. Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны. Уголовная ответственность за компьютерные преступления и особенности их реализации в современной России. Правовое регулирование отношений, связанных с привлечением к ответственности лиц, совершивших административные правонарушения в сфере ИБ. Составы административных правонарушений,

посягающих на ИБ страны. Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

## 7. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет"

### 7.1. Основная литература.

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469235

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470131

### 7.2. Дополнительная литература

1..Белопушкин В.И., Кириллычев А.Н. Правовые аспекты обеспечения информационной безопасности. М., МГТУ, 2003 г.;

2..В.П. Петров, С.В. Петров «Информационная безопасность в истории и современной жизнедеятельности.»: учебно-методическое пособие. - М.: ЮОУО ДО г. Москвы, 2007.

3..Верещагин Д. Влияние: Система дальнейшего энергоинформационного развития. – Спб: Изд-во «Невский проспект».

4..Внуков, А. А. Защита информации: учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Режим доступа : www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C- D213E1A984E1.

5..Волчинская Е.К. О стратегии и проблемах развития законодательства в сфере обеспечения информационной безопасности. Материалы конференции «Инфофорум». – 2004.

6..Государственная тайна в Российской Федерации: учебно-методическое пособие / Под ред. чл.-кор. Международной академии информатизации М.А.Вуса. – Издательство С.-Пб. Университета, 1999.

7..Доктрина информационной безопасности Российской Федерации. 2004 г. 48 с;

8..Замятин А., Замятин В., Юсупов Р. Опасности информационно-психологической войны. // «ОБЖ. Основы безопасности жизни». №6. 2002.

9..Извеков Н.Н. Исторические традиции как средство укрепления национального иммунитета в информационных войнах III тысячелетия. // Информационный сборник «Безопасность». №№7-12 2001.

10. Информационная безопасность. Information Security. Издательство: Оружие и технологии России, 2009. - 256 с.

11. Информационные технологии в юридической деятельности : учебник и практикум для СПО / Т. М. Беляева, А. Т. Кудинов, Н. В. Пальянова, С. Г. Чубукова ; отв. ред. С. Г. Чубукова. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017. — 314 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-00565-3. — Режим доступа : www.biblio-online.ru/book/0CC76DA0-57FF-4471-A4E6-6E60C43C36B7.

12. Кара-Мурза С.Г. Манипуляция сознанием в России сегодня. – М.: Изд-во «Эксмо», 2001.

13. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. Издательство: Тесей, 2008. - 176 с.

14. Лопатин В.Н. Концептуальные основы развития российского законодательства в области обеспечения информационной безопасности // Компьютерная преступность и информационная безопасность / Под общ. Ред. А.П.Леонова. – Минск: АРИЛ, 2000.

15. Мельников В. П., Клейменов С. А., Петраков А. М.. Информационная безопасность и защита информации. Издательство: Академия, 2009 г. 336 с;

16. Минаев В. А., Фисун А. П. Правовое обеспечение информационной безопасности. – М.: Издательство: Маросейка, 2008.

17. Нестеров, С. А. Информационная безопасность : учебник и практикум для

18. академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа : www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7.

19. Одинцов А. А.. Защита предпринимательства (экономическая и информационная безопасность). Учебное пособие. Издательство: Международные отношения, 2003. - 328 с.

20. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Режим доступа : www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847.

21. Панарин И.Н., Панарина Л.Г. Информационная война и мир. – М.: Изд-во «ОЛМА-ПРЕСС», 2003.

22. Петров В. П., Петров С. В. Информационная безопасность человека и

23. общества. Издательство: НЦ ЭНАС, 2007.

24. Расторгуев С. П. Основы информационной безопасности. Издательство: Академия, 2007. - 192 с.

25. Родионов М.А. Информационное противоборство: история и современность. // Информационный сборник «Безопасность». №№7-8 2002.

26. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты.

27. СПб.: Питер, 2008. — 272 с.

28. С.Н.Семкин А.Н. Семкин Основы правового обеспечения защиты информации. М.:Горячая линия –Телеком, 2007.

29. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия. – М.: “Дашков и К”, 2006.

30. Семененко В.А. Информационная безопасность. Учебное пособие. – М.: МГИУ, 2006. – 277 с.

31. Семкин С.Н., Семкин А.Н. Основы правового обеспечения информационной безопасности. – М.: Труд, 2003.

32. Стрельцов А. А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. 2005. - 304 с.

33. Тихонов В. А., Райх В. В. Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты. Издательство: Гелиос АРВ, 2007 г.;

34. Уманский С.В. Психологическое воздействие: манипуляция или психотерапия. В кн. «Психологическая теория и практика в изменяющейся России» (Тезисы окладов Всероссийской научной конференции). – Челябинск: Изд-во ЮУрГУ, 2006.

**7.3. Интернет-ресурсы, справочные системы.**

1. Окинавская хартия глобального информационного общества: Принята на о. Окинава 22.07.2000 // Дипломатический вестник. 2000. № 8. С. 51-56.

2. Конституция Российской Федерации: Принята всенародным голосованием 12.12.1993 (в посл. ред.) // СЗ РФ. 1996. № 5. Ст. 410.

3. Гражданский кодекс Российской Федерации (часть вторая) от26.01.1996 № 14-ФЗ (в посл. ред.) // Российская газета. 1996. 6 февраля.

4. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (в посл. ред.) // Российская газета. 2006. 22 декабря.

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в посл. ред.) // СЗ РФ. 1996. № 25. Ст. 2954.

6. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (посл. ред.) // Российская газета. 2001. 31 декабря.

7. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (в посл. ред.) // Российская газета. 2006. 29 июля.

8. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ (в посл. ред.) // Российская газета. 2004. 5 августа.

9. Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ (в посл. ред.) // Российская газета. 2011. 6 мая.

10. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (в посл. ред.) // Российская газета. 2006. 29 июля.

11. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (в посл. ред.) // Российская газета. 1995. 18 августа.

12. Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ (в посл. ред.) // Российская газета. 2002. 31 декабря.

13. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ (в посл. ред.) // Российская газета. 2003. 10 июля.

14. Федеральный закон «Об электронной цифровой подписи» от 10.01.2002 № 1-ФЗ (в посл. ред.) // Российская газета. 2002. 12 января.

15. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 № 395-1(в посл. ред.) // Российская газета. 1996. 10 февраля.

16. Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1 (в посл. ред.) // СЗ РФ 1997. № 41. Стр. 8220-8235.

17. Указ Президента РФ «Об утверждении Перечня сведений, отнесенных к государственной тайне» от 30.11.1995 № 1203 (в посл. ред.) // Российская газета. 1995. 27 декабря.

18. Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 06.03.1997 № 188 (в посл. ред.) // Российская газета. 1997. 14 марта.

19. Указ Президента РФ «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» от 30.05.2005 № 609 (в посл. ред.) // Российская газета. 2005. 7 июня.

20. Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 № 351 (в посл. ред.) // СЗ РФ. 2008. № 12. Ст. 1110.

21. Указ Президента РФ «О Доктрине информационной безопасности Российской Федерации» от 05.12.2016 № 646 // СПС «КонсультантПлюс»

22. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // СПС «КонсультантПлюс»

23. Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687 // Российская газета. 2008. 24 сентября.

24. Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17.11.2007 № 781 // Российская газета. 2007. 21 ноября.

25. Постановление Правительства РФ «О порядке проведения проверки наличия в заявках на выдачу патента на изобретение или полезную модель, созданные в Российской Федерации, сведений, составляющих государственную тайну» от 24.12.2007 № 928 (в посл. ред.) // Российская газета. 2007. 28 декабря.

### 7.4. Интернет ресурсы

1. http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/b46904541430deb3c3256c4e003844b5
2. http://jurisprudence.club/informatsionnoe-pravo_703/sistema-pravovogo obespecheniya.html
3. http://law.edu.ru/book/book.asp?bookID=1288184
4. http://xn----7sbabeyocb2bkdagddhcqh9acx1a8cxksc.xn--80afh5aqv.xn--p1ai/

### 7.5. Иные источники

Источники, доступные через справочно-правовую системы «КонсультантПлюс»: Колоткина О.А. Дифференциация видов безопасности в российском законодательстве: теоретико-правовой анализ // Российская юстиция. 2018. № 11. С. 31 - 34

## 8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Освоение дисциплины осуществляется в учебной аудитории, соответствующей по вместимости количеству студентов потока или учебной группы. Для успешного освоения дисциплины аудитория оборудована мультимедийным комплексом и экраном для демонстрации слайдовых презентаций и иных форм визуализации учебного материала.

Для демонстрации презентаций студентов на практических занятиях могут использоваться мультимедийные средства, имеющиеся в распоряжении кафедры (проектор, экран, ноутбук).

| Перечень информационных технологий, программных продуктов, используемых при осуществлении образовательного процесса по дисциплине | |
|---|---|
| 1 | Операционная система (MS Windows XP/Vista/7-10); |
| 2 | Пакет офисных программ (MicrosoftOffice или OpenOffice); |
| 3 | Антивирусная программа (NOD32, Dr.Web, Kaspersky и др.); |
| 4 | Интернет-браузер (Internet Explorer, Opera, Mozilla Firefox, Google Chrome идр.); |
| 5 | Различные утилиты (Архиваторы, программы записи компакт-дисков, файловые менеджеры, программы просмотра изображений и др.); |
| 6 | • Универсальная интернет-энциклопедия Wikipedia http://ru.wikipedia.org<br>• ЭБС Лань http://e.lanbook.com<br>• ЭБС IPRbooks http://www.iprbookshop.ru<br>• ЭБС Юрайт http://www.biblio-online.ru<br>• Сервис полнотекстового поиска по книгам http://books.google.ru/<br>• Научная электронная библиотека eLIBRARY.RU http://elibrary.ru<br>• Федеральный образовательный портал «Российское образование» |

| | |
|---|---|
| | http://www.edu.ru |

**8.1. Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение**: Лекционные, практические занятия и самостоятельная работа проводятся с использованием электронного обучения и дистанционных образовательных технологий. Учебные и учебно-методические материалы размещены в системе дистанционного обучения: https://lms.ranepa.ru. В системе дистанционного обучения https://lms.ranepa.ru. могут быть размещены тексты для использования в рамках практических занятий как с использованием, так и без использования ЭО и ДОТ.

Для проведения лекций необходима аудитория с презентационным оборудованием, компьютер под управлением операционной системы Windows с доступом в Интернет и установленным программным обеспечением MicrosoftOffice (Word, PowerPoint, Excel) и AdobeReader.

Для лабораторных занятий необходим компьютерный класс, оснащённый компьютерами под управлением операционной системой Windows с доступом в Интернет и установленным прикладным программным обеспечением EconometricViews (версии не ниже 8) либо пакеты Gretl или R, Stata (версии не ниже 10) либо пакет R, MicrosoftOffice (Word, PowerPoint, Excel) и AdobeReader. Компьютер преподавателя должен быть оснащен проектором.

Учебные аудитории, предназначенные для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, должны быть оборудованы:

- специализированной мебелью (аудиторные столы и стулья);
- техническими средствами обучения (мультимедийный проектор; персональный компьютер (ноутбук) с программным обеспечением: операционная система Windows 7/8/10; офисный пакет Microsoft Office2010/2013/2016, включающий программу подготовки и демонстрации презентаций Microsoft PowerPoint);
- экраном для демонстрации презентаций и фильмов;
- учебной доской (маркерной).

Учебные аудитории, предназначенные для самостоятельной работы, должны быть оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и использования электронно-библиотечных и информационно-справочных систем, а также с обеспечением доступа в электронную информационно-образовательную среду (сайт) Московского областного филиала РАНХиГС.