Государственное бюджетное образовательное учреждение высшего образования Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

Подписано цифровой подписью: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
И.В. Бабина
«12» апреля 2022 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.О.12.02 «ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

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

Автор: Сухотерин А.И. Рабочая программа дисциплины: Организационное и правовое обеспечение информационной безопасности. – Королев МО: «Технологический университет», 2022.

Рецензент: **Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 12.04.2022 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания кафедры	№8 от 17.03.2022			

Рабочая программа согласована:

Руководитель ОПОП ВО к.т.н., доцент Вихров А.П.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания УМС	№4 от 12.04.2022			

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

Целями изучения дисциплины является:

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

В процессе обучения студент приобретает и совершенствует следующие компетенции:

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

Основными **задачами** дисциплины являются:

1. Теоретические основы обеспечения информационной безопасности на основе действующего российского законодательства с помощью с помощью современных принципов, методов, сил и средств в различных организационных структурах;
2. Практические аспекты правовой защиты информации защиты информации по базовым направлениям защиты государственной,

профессиональной, коммерческой тайны и конфиденциальной информации и формированием у обучающихся системы знаний.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации;
- знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации;
- знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации;
- знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности;
- знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
- знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
- знает систему организационных мер, направленных на защиту информации ограниченного доступа
- знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа
- знает основные угрозы безопасности информации и модели нарушителя объекта информатизации

Необходимые умения:

- умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав;
- умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;
- умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации;

- умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;

- умеет разрабатывать модели угроз и модели нарушителя объекта информатизации

- умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации

- умеет определить политику контроля доступа работников к информации ограниченного доступа

- умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика», «Введение в профессию», «Основы исследований информационной безопасности», «Основы информационной безопасности» и компетенциях: ОПК-1,6,7,8,9, УК-2,5,10 ПК-1.

Знания и компетенции, полученные при освоении дисциплины «Криптографические методы защиты информации», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», «Лицензирование и сертификация в области защиты информации», являются базовыми для изучения всех последующих дисциплин, прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины для студентов очной формы составляет 5 зачетных единиц, 180 часов.

Таблица1

Виды занятий	**Всего часов**	**Семестр** 4	**Семестр** 5	**Семестр** …	**Семестр** …
Общая трудоемкость	180	180	180		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	80	80			
Лекции (Л)	32	32			
Практические занятия (ПЗ)	48	48			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	94	94			
Другие виды контактной работы	**10**	**10**			
Практическая подготовка	нет	-			
Курсовые работы (проекты)	+	+			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2			
Вид итогового контроля	Экзамен	Экзамен			

Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. очное/очно-заочное	Практические. занятия, час. очное/очно-заочное	Занятия в интерактивной форме, час. очное/очно-заочное	Код компетенций
1	2	3	4	5
Раздел 1. Правовые основы обеспечения информационной безопасности				
Тема 1. Правовое обеспечение информационной безопасности	1	2	0.5	**ОПК-5**

Тема 2. Институт правовой защиты государственной тайны	2	2	0.5	**ОПК-5**
Тема 3. Нормативно – правовое регулирование сведений, составляющих служебную тайну	2	2	0.5	**ОПК-5**
Тема 4. Понятие и состав информационных систем и прав на них	2	2	0.5	**ОПК-5**
Тема 5. Институт правовой охраны программ для ЭВМ и баз данных	2	2	0.5	**ОПК-5**
Тема 6. Институт правовой защиты тайны связи	2	2	0.5	**ОПК-5**
Раздел 2. Основы правовой защиты информации				
Тема 7. Назначение и задачи подзаконных и ведомственных нормативно - правовых актов, регулирующих защиту государственной и служебной тайны	1	4	0.5	**ОПК-6**
Тема 8. Институт правовой защиты информации конфиденциального характера	2	2	0.5	**ОПК-6**
Тема 9. Институт правовой защиты тайны следствия и судопроизводства	2	2	0.5	**ОПК-6**

Тема 10. Институт правовой защиты тайны частной жизни и ПДн	2	2	0.5	**ОПК-6**

Тема 11. Институт правовой защиты профессиональной тайны	2	4	0.5	**ОПК-6**
Тема 12. Институт правовой защиты банковской тайны	2	4	0.5	**ОПК-6**
Тема 13. Институт правовой защиты коммерческой тайны.	2	4	0.5	**ОПК-6**
Тема 14. Основные объекты интеллектуальной собственности и их правовая защита	2	4	0.5	**ОПК-6**
Тема 15. Институт правовой защиты авторских и смежных прав	2	4	0.5	**ОПК-6**
Тема 16. Институт правовой защиты изобретений, полезных моделей и промышленных образцов	2	4	0.5	**ОПК-6**
Тема 17. Институт правовой охраны наименований и товарных знаков	2	2	0.5	**ОПК-6**

Итого:	32	48	16	

4.2. Содержание тем дисциплины

Раздел I
Правовые основы обеспечения информационной безопасности
Тема 1. Правовое обеспечение информационной безопасности

Основные угрозы информационной безопасности РФ. Правовые режимы распространения информации в исключительных ситуациях, представляющих угрозу безопасности РФ. Совершенствование правого регулирования информационной безопасности. Национальные интересы РФ в информационной среде и угрозы их безопасности. Цели и методы правового обеспечения информационной безопасности РФ. Нормативно – правовые акты в области информационной безопасности. Преступления в сфере компьютерной безопасности. Организационно – правовые методы их предупреждения и защиты от них. Особенности защиты информации и интеллектуальной собственности в сети Интернет.

Тема 2. Институт правовой защиты государственной тайны

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

Тема 3. Нормативно – правовое регулирование сведений, Составляющих служебную тайну

Правовая основа служебной тайны. Правовая защита служебной информации ограниченного распространения. Правовая защита служебной тайны, основу которой составляет конфиденциальная и внутренняя информация.

Тема 4. Понятие и состав информационных систем и прав на них

Понятие и состав информационных систем. Территориальные и ведомственные уровни формирования единого информационного пространства. Правовая охрана и защита прав на информационно – телекоммуникационные системы. Тенденции усиления борьбы с компьютерными преступлениями на международном уровне. Основные положения общеевропейской Конвенции о киберпреступности.

Информационные и компьютерные преступления. Термины и понятия связанные с правоотношениями в компьютерной сфере. Криминалистическая характеристика компьютерных преступлений.

Тема 5. Институт правовой охраны программ для ЭВМ и баз данных

Понятие и история правовой охраны программ для ЭВМ и баз данных. Основные положения четвертой части Гражданского кодекса РФ, касающейся правовой охраны программ для ЭВМ и баз данных. Выявление контрафакции программного обеспечения.

Тема 6. Институт правовой защиты тайны связи

Правовое регулирование деятельности в области обеспечения связи. Понятие тайны связи и ее правовая защита.

Раздел II
Основы правовой защиты информации

Тема 7. Назначение и задачи подзаконных и ведомственных нормативно - правовых актов, регулирующих защиту государственной и служебной тайны

Общая характеристика подзаконных и ведомственных нормативно – правовых актов, регулирующих защиту государственной и служебной тайны. Виды подзаконных, ведомственных и межведомственных правовых актов в сфере защиты информации. Назначение и задачи подзаконных и ведомственных правовых актов, регулирующих процессы защиты государственной тайны. Правовые основы деятельности подразделений по защите государственной и служебной тайны в органах государственной власти, на предприятиях, в учреждениях и организациях. Порядок допуска должностных лиц и граждан РФ к государственной тайне. Подзаконные, ведомственные и локальные правовые акты, действующие в сфере защиты основных видов конфиденциальной информации. Назначение и задачи подзаконных правовых актов, регулирующих процессы защиты персональных данных и коммерческой тайны. Закрепление права предприятия на защиту информации в нормативных документах (коллективном договоре, трудовом договоре, иных локальных правовых актах организаций). Правовые основы деятельности подразделений по защите конфиденциальной информации на предприятиях, в учреждениях и организациях. Организация доступа персонала к коммерческой тайне.

Тема 8. Институт правовой защиты информации конфиденциального характера

Понятие информации конфиденциального характера. Перечень сведений конфиденциального характера. Признаки и классификация сведений конфиденциального характера. Критерии выделения

конфиденциальной информации. Правовая основа защиты конфиденциальной информации. Проблемы технической защиты конфиденциальной информации. Подзаконные нормативно – правовые акты, специальные требования и рекомендации в области технической защиты конфиденциальной информации.

Тема 9. Институт правовой защиты тайны следствия и судопроизводства

Правовые основы защиты тайны предварительного расследования. Краткая историческая ретроспектива изучаемого вопроса. Правовые основы защиты тайны предварительного расследования. Уголовная ответственность за ее разглашение. Правовые основы защиты тайны судебного производства. Соотношения терминов « уголовное судопроизводство» и «судебное заседание». Содержание принципа гласности судебного разбирательства. Специфика тайны судебного разбирательства. Использование в ходе предварительного расследования и судебного разбирательства информации ограниченного доступа. Роль и место информации ограниченного доступа в уголовном процессе. Специфика защиты государственной тайны в уголовном процессе.

Тема 10. Институт правовой защиты тайны частной жизни и персональных данных

Право на неприкосновенность частной жизни. Понятие права на неприкосновенность частной жизни. Нормативные правовые акты, регулирующие правоотношения в данной области. Объекты и субъекты тайны частной жизни. Защита тайны частной жизни. Правовая охрана и защита права на неприкосновенность частной жизни. Способы его защиты. Уголовно – правовая ответственность за нарушение права на неприкосновенность частной жизни. Исключительные случаи ограничения прав граждан на неприкосновенность частной жизни. Законодательные основания для ограничений прав граждан на неприкосновенность тайны частной жизни. Основные положения российского законодательства, связанные с защитой персональных данных. Европейская конвенция о защите личности в связи с автоматической обработкой персональных данных. Правовая основа защиты персональных данных в Конституции РФ и других нормативно – правовых актах. Основные положения Федерального закона «О персональных данных» и некоторых подзаконных нормативно – правовых актах. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований ФЗ «О персональных данных».

Тема 11. Институт правовой защиты профессиональной тайны

Сущность профессиональной тайны. Понятие профессиональной тайны. Критерии охраноспособности права на профессиональную тайну.

Источники, связанные с профессиональной тайной. Субъекты и объекты правоотношений в области защиты профессиональной тайны. Субъекты правоотношений в области охраны профессиональной тайны. Объекты нарушения права на профессиональную тайну. Права доверителя в отношении сведений, ставших на законном основании известными держателю профессиональной тайны. Защита доверителем своих прав. Правовая защита профессиональной тайны. Права доверителя в отношении сведений, ставших на законном основании известными держателю профессиональной тайны. Защита доверителем своих прав.

Тема 12. Институт правовой защиты банковской тайны

Основные понятия, связанные с банковской тайной, и правовая основа ее защиты. Понятие банковской тайны. Объекты и субъекты банковской тайны. Способы защиты банковской тайны. Банковская тайна за рубежом. Банковская тайна в Швейцарии. Банковская тайна в США.

Тема 13. Институт правовой защиты коммерческой тайны

Понятие коммерческой тайны и ее генезис. Своеобразие ее содержания и основные исторические этапы развития. Действующие нормативно – правовые акты, устанавливающие требования по защите коммерческой тайны. Основные положения Федерального закона « О коммерческой тайне». Основные положения части четвертой Гражданского кодекса РФ, касающейся защиты коммерческой тайны. Ответственность, связанная с нарушением законодательства о коммерческой тайне. Зарубежный опыт правовой защиты коммерческой тайны.

Тема 14. Основные объекты интеллектуальной собственности и их правовая защита

Понятие результатов интеллектуальной деятельности, средств индивидуализации и иных объектов, созданных в результате деятельности, приравненной к интеллектуальной деятельности. Понятие объектов интеллектуальной собственности и их законодательный перечень. Результаты интеллектуальной деятельности, средства индивидуализации и иные объекты, созданные в результате деятельности, приравненной к интеллектуальной деятельности. Интеллектуальное право. Основание для возникновения интеллектуальных прав. Защита интеллектуальных прав. Автор результата интеллектуальной деятельности. Авторская правоспособность. Личные неимущественные права автора. Иные неимущественные права. Исключительное право на результат интеллектуальной деятельности. Виды правовой защиты интеллектуальных прав.

Тема 15. Институт правовой защиты авторских и смежных прав

Понятие и генезис авторских и смежных прав. История развития законодательства об авторском праве в России. Правовая защита авторских и смежных прав. Участие России. Правовая защита авторских и смежных прав. Участие России в международных соглашениях по защите авторских и смежных прав. Современное правовое регулирование авторских прав. Объекты и субъекты авторского права. Интеллектуальные права авторов произведений литературы, науки и искусства. Категории интеллектуальных прав авторов произведенной литературы, науки и искусства. Договор об отчуждении исключительного права на произведение. Лицензионный договор. Порядок передачи автором своих имущественных прав по этим договорам. Правовая защита смежных прав. Охрана прав артистов – исполнителей, производителей фонограмм, организации эфирного и кабельного вещания, на содержание баз данных, а также на произведения науки, литературы и искусства, впервые обнародованные после их перехода в общественное достояние. Возможность свободного использования объектов смежных прав. Лицензирование в области материализации отдельных результатов интеллектуальной деятельности. Ответственность за нарушение авторских и смежных прав. Гражданская, уголовная и административная ответственность, связанная с нарушениями авторского права и смежных прав.

Тема 16. Институт правовой защиты изобретений, полезных моделей и промышленных образцов

Понятие патентного права. История развития патентного права в России. Основные особенности патентного законодательства РФ. Характеристика объектов патентного права. Понятия изобретения, полезной модели и промышленного образца. Их общие и отрицательные признаки. Патент как форма охраны объектов патентного права. Понятие содержание патентных прав. Исключительное право патентообладателя. Порядок оформления патентов. Передача исключительного права на изобретения, полезные модели и промышленные образцы. Субъекты патентных прав. Способы передачи исключительного права – отчуждение и заключение лицензионного договора. Виды лицензионных договоров. Защита прав авторов и патентообладателей. Гражданско – правовая защита патентных прав. Административный порядок разрешения возникающих споров. Административная и уголовная ответственность, связанная с нарушением изобретательских и патентных прав. Контроль со стороны Роспатента за некоторыми направлениями реализации патентного законодательства. Участие России в работе международных организаций по защите прав авторов и патентообладателей. Международное и межгосударственное сотрудничество России в области защиты патентных прав.

Тема 17. Институт правовой охраны наименований и товарных знаков (средств индивидуализации юридических лиц,

товаров, работ, услуг и предприятий)

Понятие средств индивидуализации юридических лиц, товаров, работ, услуг и предприятий. Понятие и содержание фирменного наименования и коммерческого обозначения. Понятия товарного знака, знака обслуживания и наименования места происхождения товара. История товарных и их основные функции. Современное правовое регулирование отношений в области охраны средств индивидуализации. Правовое регулирование прав на фирменное наименование. Правовое регулирование прав на коммерческое обозначение. Виды товарных знаков. Правовое регулирование прав на товарный знак. Субъекты прав на товарный знак. Оформление прав на товарный знак. Оформление прав на товарный знак, знак обслуживания и наименование места происхождения товара. использование товарного знака, знака обслуживания и наименования места происхождения товара. Защита прав на товарный знак, знак обслуживания и наименование места происхождения товара. Порядок прекращения правовой охраны товарного знака. Действие в России международных правовых актов по охране средств индивидуализации. Правовой статус общеизвестных товарных знаков. Регистрация и использование в качестве доменных имен средств индивидуализации.

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

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

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Организационное и правовое обеспечение информационной безопасности» , приведена в Приложении 1.

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

Основная литература:

1.Организационно-правовое обеспечение информационной безопасности : учебник / А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев [и др.] ; под редакцией А. А. Александрова, М. П. Сычева. — Москва : МГТУ им. Баумана, 2018. — 291 с. — ISBN 978-5-7038-4723-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

https://e.lanbook.com/book/172840 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.
2.Крыжановский, А. В. Организационное и правовое обеспечение информационной безопасности : методические указания / А. В. Крыжановский. — Самара : ПГУТИ, 2018. — 56 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182279 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

3.Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, Н. Н. Прохожев. — Санкт-Петербург : НИУ ИТМО, 2016. — 168 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/91449 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.
4.Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности : учебное пособие / Г. П. Жигулин. — Санкт-Петербург : НИУ ИТМО, 2014. — 173 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/70952 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

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

Интернет-ресурсы:

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

9. Методические указания для обучающихся, по освоению дисциплины

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

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

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Электронные ресурсы образовательной среды Университета.
2. Рабочая программа и методическое обеспечение по дисциплине: «Организационное и правовое обеспечение информационной безопасности»

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

Лекционные занятия:

– аудитория, оснащенная презентационной техникой (проектор, экран);

– комплект электронных презентаций / слайдов на темы:

Практические занятия:

– компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;

– рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;

– рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

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

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

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

№ п/п	Индекс компе-тенции	Содержание компетенции	Раздел дисциплины обеспечивающий формирование компетенции	: В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	Темы 1,4,5,6,7 -17		- умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; - умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих	- знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; - знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации; - знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты

					работу по обеспечению информационной безопасности в организации; - умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в	государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; - знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности;

					организации ;	
2.	ОПК-6	Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Темы 1,2,3,6,7 -17		- умеет разрабатывать модели угроз и модели нарушителя объекта информатизации - умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации - умеет определить политику контроля доступа работников к информации ограниченного доступа - умеет формулировать основные требования, предъявляемые к физической защите	- знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; - знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях; - знает систему организационных мер, направленных на защиту информации ограниченного доступа - знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного

					объекта и пропускному режиму в организации	доступа - знает основные угрозы безопасности информации и модели нарушителя объекта информатизации

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

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ОПК-5,6	*Доклад*	***А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на продвинутом уровне – 4 балла;*** • ***компетенция освоена на базовом уровне – 3 балла;*** ***В) не сформирована (компетенция не сформирована) – 2 и менее баллов***	***Например:*** ***Проводится в письменной и/или устной форме.*** ***Критерии оценки:*** ***1. Соответствие содержания доклада заявленной тематике (1 балл).*** ***2. Качество источников и их количество при подготовке работы (1 балл).*** ***3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).*** ***4. Качество самой представленной работы (1 балл).*** ***5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).*** ***Максимальная сумма баллов - 5 баллов.***
ОПК-5,6	***Выполнение контрольной работы***	***А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на***	***При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида***

		продвинутом уровне – 4 балла; • ***компетенция освоена на базовом уровне – 3 балла;*** ***В) не сформирована (компетенция не сформирована) – 2 и менее баллов***	
ОПК-5,6	***Курсовая работа***	***А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на продвинутом уровне – 4 балла;*** • ***компетенция освоена на базовом уровне – 3 балла;*** ***В) не сформирована (компетенция не сформирована) – 2 и менее баллов***	***Например:*** ***Проводится в письменной форме.*** ***1. Оформление в соответствии с требованиями (1 балл).*** ***2. Соответствует методическим указаниям в части структуры (1 балл).*** ***3. Содержание курсовой работы соответствует заявленной тематике (1 балл).*** ***4. Поставленные цели и задачи достигнуты (1 балл).*** ***5. Качественный и количественный состав использованных источников (1 балл).*** ***Максимальная оценка – 5 баллов.***

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Правовые основы защиты тайны предварительного расследования.
2. Правовые основы защиты тайны предварительного расследования. Уголовная ответственность за ее разглашение.
3. Правовые основы защиты тайны судебного производства. Соотношения терминов « уголовное судопроизводство» и «судебное заседание».
4. Содержание принципа гласности судебного разбирательства. Специфика тайны судебного разбирательства.

5. Использование в ходе предварительного расследования и судебного разбирательства информации ограниченного доступа.
6. Роль и место информации ограниченного доступа в уголовном процессе. Специфика защиты государственной тайны в уголовном процессе.
7. Право на неприкосновенность частной жизни. Понятие права на неприкосновенность частной жизни.
8. Правовая охрана и защита права на неприкосновенность частной жизни.
9. Уголовно – правовая ответственность за нарушение права на неприкосновенность частной жизни.
10. Законодательные основания для ограничений прав граждан на неприкосновенность тайны частной жизни.
11. Основные положения российского законодательства, связанные с защитой персональных данных.
12. Европейская конвенция о защите личности в связи с автоматической обработкой персональных данных.
13. Правовая основа защиты персональных данных в Конституции РФ и других нормативно – правовых актах.
14. Основные положения Федерального закона «О персональных данных» и других подзаконных нормативно – правовых актах.
15. Принципы и условия обработки персональных данных. Права субъекта персональных данных.
16. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований ФЗ «О персональных данных».
17. Объекты нарушения права на профессиональную тайну.
18. Права доверителя в отношении сведений, ставших на законном основании известными держателю профессиональной тайны. Защита доверителем своих прав.
19. Правовая защита профессиональной тайны.
20. Права доверителя в отношении сведений, ставших на законном основании известными держателю профессиональной тайны. Защита доверителем своих прав.

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

Формой контроля знаний по дисциплине «Организационное и правовое обеспечение информационной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ОПК-56	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ОПК-5,6	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком	Экзамен	ОПК-5,6	2 теоретических вопроса + практическое задание	Экзамен проводится в устной форме, путем ответа на вопросы. Время,	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета;

образовательного процесса				отведенное на процедуру – 30 минут.		• умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетвори-тельно**»: • демонстрирует частичные

						знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. С какой тайной связывают банковскую тайну?

(!) Коммерческая тайна

(?) Государственная тайна

(?) Служебная тайна

(?) Тайна следствия и судопроизводства

2. Какие операции не могут осуществляться при банковских отношениях?

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

(?) Открытие и ведение счетов физических и юридических лиц

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

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

3. Какова величина суммы застрахованного банковского вклада?

(!) 1 млн. 400 тыс. руб.

(?) 800 тыс. руб.

(?) 100 тыс. руб.

(?) 150 тыс. руб.

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

(?) Конституция РФ

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

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

(?) Доктрина ИБ

5. Кредитная организация не вправе осуществлять…?

(!) Лизинговые операции

(!) Оказание консультаций и информационных услуг

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

(?) Осуществление операций с драгоценными металлами и камнями

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

(?) Конституция РФ

(!) ФЗ. №86 «О ЦБ РФ»

(?) УК РФ

(?) ФЗ «О коммерческой тайне»

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

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

(?) ФЗ. №86 «О ЦБ РФ»

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

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

8. Кто занимается созданием центральной базы кредитных историй?

(?) Вкладчик

(!) Бюро кредитных историй

(?) Специалист по ИБ

(?) Банк

9. Кому не может быть предоставлен кредитный отчет?

(?) Пользователь кредитной истории

(?) Субъекту кредитных историй

(?) В суд

(!) Родственникам

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

(!) Обязательно
(?) По желанию
(?) Не попадет
(?) Попадет через 5 лет

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

(?) ФЗ. №86 «О ЦБ РФ»
(?) ФЗ. № 395-1 «О Банках и Банковской деятельности»
(?) Конституцией РФ
(!) ФЗ. №177 «О страховых вкладах физических лиц в банковских организациях»

12. Чем регламентируется работа бюро кредитных историй?

(!) Законом о кредитных историях
(?) Конституцией РФ
(?) Уголовным кодексом
(?) Банком

13. Кредитная история хранится в течении?

(!) 15 лет с последнего изменения
(?) 16 лет с последнего изменения
(?) 10 лет с последнего изменения
(?) 5 лет с последнего изменения

14. Что не входит в кредитную историю?

(!) Сведения о месте работы
(?) ФИО
(?) Данные паспорта
(?) Индивидуальный номер налогоплательщика

15. Правом на сохранение БТ не обладает?

(!) Государство
(?) Доверитель
(?) Клиент
(?) Корреспондент

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

(!) физическое лицо, творческим трудом которого создано произведение;
(?) юридическое лицо, творческим трудом которого создано произведение;
(?) физическое лицо, физическим трудом которого создано произведение;
(?) юридическое лицо, умственным трудом которого создано произведение.

17. Авторское право это:

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

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

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

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

18. Что из перечисленного относится к смежным правам:

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

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

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

(?) юридические правоотношения не связанные с авторским правом.

19. Что не является объектом авторского права:

(?) фольклор;

(!) литературные произведения;

(!) музыкальные произведения;

(!) скульптуры.

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

(!) 70 лет;

(?) 25 лет;

(?) 10 лет;

(?) 100 лет.

21. К неделимому соавторству относится:

(!) случаи, когда произведение образует неразрывное целое;

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

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

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

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

(!) 70 лет;

(?) 100 лет;

(?) 25 лет;

(?) 10 лет.

23. Правовому регулированию смежных прав посвящается:

(!) часть 4 гражданского кодекса РФ;

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

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

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

24. Право на отзыв это:

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

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

(?) право на составление отзыва на собственное произведение;

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

25. Произведение считается обнародованным если:

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

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

(?) после 10 дней поле опубликования в РФ;

(?) сразу после опубликования в РФ.

26. К авторским правам не относятся:

(!) специальное право;

(?) исключительное право;

(?) личные не имущественные права;

(?) иные права.

27. К личным не имущественным правам не относится:

(!) право на продажу произведения;

(?) право на обнародование произведения;

(?) право на имя;

(?) право авторства.

28. К исключительному праву относятся:

(!) право распространения;

(!) право публичного показа;

(?) право на отзыв;

(?) право на имя.

29. К иным правам не относится:

(!) право на издание;

(?) право на отзыв;

(?) право следования;

(?) право доступа.

30. Авторское право действует на:

(!) обнародованное произведение;

(!) необнародованное произведение;

(?) чужое произведение;

(?) федеральный закон.

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

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

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

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

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

32. Конфиденциальная составляющая коммерческой тайны:

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

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

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

(?) Персональные данные руководящего состава предприятия.

33. Интеллектуальная составляющая коммерческой тайны:

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

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

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

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

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

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

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

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

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

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

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

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

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

(?) Гражданский кодекс РФ часть 4.

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

(!) Трудовой кодекс РФ;

(?) Федеральный закон «О коммерческой тайне»;

(?) Гражданский кодекс РФ;

(?) Уголовный кодекс РФ.

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

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

(?) Гражданский кодекс РФ;

(?) Уголовный кодекс РФ;

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

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

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

(?) Федеральный закон «О коммерческой тайне»;

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

(?) Уголовно-процессуальный кодекс РФ.

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

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

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

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

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

40. Признаки информации, обретённой незаконно:

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

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

(?) Информация, полученная из открытых источников;

(?) Плагиат.

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

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

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

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

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

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

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

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

(?) Обладатель информации;

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

43. Общие меры обеспечения соблюдения конфиденциальности информации:

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

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

(?) Организация конфиденциального документооборота на предприятии;

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

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

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

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

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

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

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

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

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

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

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

Кто утвердил перечень сведений конфиденциального характера № 188:

(!)Президент.

(?)Премьер министр.

(?)ФСТЭК.

(?)ФСБ.

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

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

(?)Хищение имущества.

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

(?)Получение имущества с помощью применения силы.

47. К правовым методам защиты информации доктрина относит:

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

(?)Составление списка ответственных лиц.

(?)Указание по использованию физических средств ЗИ.

(?)Указание по использованию технических средств ЗИ.

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

(?)5.

(?)4.

(!)6.

(?)8.

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

(?)Служебная тайна.

(?)Коммерческая тайна.

(?)Персональные данные.

(!)Профессиональная тайна.

50. Субъектами банковской тайны являются:

(!)Держатели.

(!)Кредитные организации.

(?)Вкладчики.

(?)Государство.

51. Определение организационно-розыскной деятельности

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

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

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

52. Какие сведения относятся к информации конфиденциального характера

(!)Сведения о возможных природных бедствиях.

(?)Информация, составляющая тайну следствия.

(?)Сведения, связь с профессиональной деятельностью.

(?)Сведения, связь с коммерческой деятельностью.

53. Информация, составляющая коммерческую тайну:

(?)Товарные знаки.

(?)Авторское право.

(?)Государственная тайна.

(!)Банковская тайна.

54. Чем охраняется информация, ограниченного доступа?

(!)Федеральными законами.
(?)Ведомственными приказами.
(?)Силовыми структурами (ведомствами).

55. За разглашение сведений конфиденциального характера наступает ответственность:

(?)Уголовная.
(?)Административная.
(?)Дисциплинарная.
(!)Все вышеперечисленные.

56. С правовой точки зрения защите подлежит:

(?)Любая закрытая информация.
(!)Информация, зафиксированная на материальном носителе.
(?)Любая коммерческая тайна.
(?)Всё вышеперечисленное.

Примерная тематика курсовых проектов (работ)

1. Разработка правового обеспечение СИБ на малом (среднем, большом или корпоративном) предприятии.
2. Разработка организационного обеспечение СИБ на малом (среднем, большом или корпоративном) предприятии.
3. Построение программно-аппаратного обеспечение СИБ в коммерческих производственных структурах.
4. Построение инженерно-техническое обеспечение СИБ на малом (среднем, большом или корпоративном) предприятии.
5. Разработка методического обеспечение СИБ на государственном (коммерческом) предприятии.
6. Построение материально-технического обеспечения СИБ на предприятии.
7. Разработка подсистемы физической защиты информационных объектов в СИБ современного предприятия.
8. Построение СИБ для автоматизированных систем обработки информации на предприятии.
9. Построение подсистемы управление СИБ на малом (среднем, большом или корпоративном) предприятии.
10. Разработка подсистемы управление СИБ предприятия в условиях чрезвычайных ситуаций.
11. Разработка и внедрения политики информационной безопасности при реализации СИБ на предприятии.
12. Разработка подсистемы автоматизированного планирование в СИБ на предприятии.
13. Организация и проведение аудита СИБ на малом (среднем, большом или корпоративном) предприятии.
14. Анализ и управление рисками при проектировании СИБ предприятия.

15. Разработка моделей угроз и нарушителей при проектировании СИБ на малом (среднем, большом или корпоративном) предприятии.
16. Разработка моделей оценки эффективности проектирования СИБ на малом (среднем, большом или корпоративном) предприятии.
17. Разработка технологии делового планирования при организации СИБ предпринимательских структур.
18. Определение возможностей несанкционированного доступа к защищаемой информации в СИБ предприятия.
19. Определение основных компонентов СИБ предприятия.
20. Определение условий функционирования СИБ предприятия.
21. Разработка модели СИБ современного предприятия.
22. Организационное построение СИБ типового предприятия.
23. Управление СИБ в условиях чрезвычайных ситуаций на предприятии.
24. Методы и модели оценки эффективности СИБ типового предприятия.

Типовые вопросы, выносимые на экзамен

1. Основные угрозы информационной безопасности РФ.
2. Правовые режимы распространения информации в исключительных ситуациях, представляющих угрозу безопасности РФ.
3. Совершенствование правого регулирования информационной безопасности.
4. Законодательная основа защиты государственной тайны.
5. Уголовно – правовая защита сведений, составляющих государственную тайну.
6. Правовая защита служебной информации ограниченного распространения.
7. Правовая защита служебной тайны, основу которой составляет конфиденциальная.
8. Правовая защита служебной информации ограниченного распространения.
9. Правовая охрана и защита прав на информационно – телекоммуникационные системы.
10. Основные положения общеевропейской Конвенции о киберпреступности.
11. Криминалистическая характеристика компьютерных преступлений.
12. Понятие и история правовой охраны программ для ЭВМ и баз данных.
13. Правовое регулирование деятельности в области обеспечения связи. Понятие тайны связи и ее правовая защита.
14. Обеспечение безопасности ведомственной информации, информационных ресурсов, средств и систем информации.
15. Основные цели и задачи правовой защиты информации.

16. Методы правовой защиты информации.
17. Подзаконные, ведомственные и локальные правовые акты, действующие в сфере защиты основных видов конфиденциальной информации.
18. Сущность государственной защиты участников уголовного судопроизводства.
19. Правовые основы защиты тайны предварительного расследования.
20. Использование в ходе предварительного расследования и судебного разбирательства информации ограниченного доступа.
21. Право на неприкосновенность частной жизни.
22. Основные положения Федерального закона «О персональных данных» и некоторых подзаконных нормативно – правовых актов.
23. Субъекты и объекты правоотношений в области защиты профессиональной тайны.
24. Ответственность, связанная с нарушением законодательства о коммерческой тайне.
25. Современное правовое регулирование авторских прав.
26. Интеллектуальные права авторов произведений литературы, науки и искусства. Правовая защита смежных прав.
27. Патент как форма охраны объектов патентного права.
28. Передача исключительного права на изобретения, полезные модели и промышленные образцы.
29. Соотношение понятий «защита информации» и «информационная безопасность». Цель и задачи защиты информации.
30. Организационно – правовые принципы защиты информации.
31. Методы правовой защиты информации.
32. Понятие правовой защиты информации, ее методов и способов.
33. Закрепление права предприятия на защиту информации в нормативных документах (коллективном договоре, трудовом договоре, иных локальных правовых актах организаций).
34. Права и обязанности органов, обеспечивающих государственную защиту.
35. Соотношения терминов « уголовное судопроизводство» и «судебное заседание».
36. Содержание принципа гласности судебного разбирательства.
37. Роль и место информации ограниченного доступа в уголовном процессе. Право на неприкосновенность частной жизни.
38. Правовая охрана и защита права на неприкосновенность частной жизни.
39. Уголовно – правовая ответственность за нарушение права на неприкосновенность частной жизни.
40. Основные положения российского законодательства, связанные с защитой персональных данных.

41. Европейская конвенция о защите личности в связи с автоматической обработкой персональных данных.
42. Правовая основа защиты персональных данных в Конституции РФ и других нормативно – правовых актах.
43. Основные положения Федерального закона «О персональных данных» и некоторых подзаконных нормативно – правовых актах.
44. Ответственность за нарушение требований ФЗ «О персональных данных».
45. Субъекты и объекты правоотношений в области защиты профессиональной тайны.
46. Права доверителя в отношении сведений, ставших на законном основании известными держателю профессиональной тайны.
47. Основные понятия, связанные с банковской тайной, и правовая основа ее защиты.
48. Объекты и субъекты банковской тайны.
49. Действующие нормативно – правовые акты, устанавливающие требования по защите коммерческой тайны.
50. Понятие результатов интеллектуальной деятельности, средств индивидуализации и иных объектов, созданных в результате деятельности, приравненной к интеллектуальной деятельности.
51. Понятие объектов интеллектуальной собственности и их законодательный перечень.
52. Правовая защита авторских и смежных прав.
53. Лицензирование в области материализации отдельных результатов интеллектуальной деятельности.
54. Понятие патентного права.
55. Патент как форма охраны объектов патентного права.
56. Административная и уголовная ответственность, связанная с нарушением изобретательских и патентных прав.
57. Контроль со стороны Роспатента за некоторыми направлениями реализации патентного законодательства.
58. Международное и межгосударственное сотрудничество России в области защиты патентных прав.
59. Современное правовое регулирование отношений в области охраны средств индивидуализации.
60. Правовое регулирование прав на коммерческое обозначение.
61. Использование товарного знака, знака обслуживания и наименования места происхождения товара, как механизма защиты.

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

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

1. Общие положения

Целями изучения дисциплины является:

– Ускоренная адаптация студентов в предметную область информационная безопасность (защита интеллектуальной собственности), опираясь на весь спектр научных воззрений, на развитие и правовую защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации;

– Повысить уровень правовых знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;

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

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

– Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации и охраны интеллектуальной собственности на предприятиях и в организациях.

Задачами дисциплины является:

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

2. Указания по проведению практических занятий

Тема 1. Правовые основы обеспечения информационной безопасности

Практическое занятие 1.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

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

Учебные вопросы:

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

Продолжительность занятия - 6 ч.

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

Практическое занятие 2.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

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

Учебные вопросы:

1.Законодательная основа защиты государственной тайны.

2. Обеспечение защиты государственной тайны.

3. Нормативное регулирование оборота сведений, составляющих государственную тайну, в системе МВД РФ.

4. Уголовно – правовая защита сведений, составляющих государственную тайну.

Продолжительность занятия - 6 ч.

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

Практическое занятие 3.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

2. исторические истоки патентного права

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

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

Учебные вопросы:

1.Понятие и состав информационных систем.

2.Территориальные и ведомственные уровни формирования единого информационного пространства.

3. Правовая охрана и защита прав на информационно – телекоммуникационные системы.

4. Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы.

Продолжительность занятия - 6 ч.

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

Практическое занятие 4.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

2. объекты и субъекты промышленной собственности и патентного права

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

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

Учебные вопросы:

1.Тенденции усиления борьбы с компьютерными преступлениями на международном уровне.

2. Основные положения общеевропейской Конвенции о киберпреступности.

3.Информационные и компьютерные преступления.

4.Термины и понятия связанные с правоотношениями в компьютерной сфере.

5. Криминалистическая характеристика компьютерных преступлений.

Продолжительность занятия - 6 ч.

Тема 5. Основные объекты интеллектуальной собственности и их правовая защита

Практическое занятие 5.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

2. оформление прав патентообладателя

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

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

Учебные вопросы:

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

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

3. Выявление контрафакции программного обеспечения.

Продолжительность занятия - 6 ч.

Тема 6. Институт правовой защиты авторских и смежных прав

Практическое занятие 6.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

2. оформление прав патентообладателя (заявка на изобретение).

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

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

Учебные вопросы:

1.Международные нормативные правовые акты.

2.Российские официальные документы и нормативные правовые акты.

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

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

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

Продолжительность занятия - 6 ч.

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

Практическое занятие 7.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

2. оформление прав патентообладателя (заявка на полезную модель и на промышленный образец).

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

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

Учебные вопросы:

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

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

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

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

6. Зарубежный опыт правовой защиты коммерческой тайны.

Продолжительность занятия - 6 ч.

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

Практическое занятие 8.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

2. объем правовой охраны предоставляемый патентом.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

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

Учебные вопросы:

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

Продолжительность занятия - 6 ч.

4. Указания по проведению курсовой работы (проекта)

Курсовые работы (проекты)

В процессе обучения студенты выполняют курсовую работу, задание на которую разрабатывается индивидуально для каждого студента и выдается на первом аудиторном занятии. Срок выполнения курсовой работы – 6-ая неделя семестра. Отчет по контрольной работе должен содержать требования к программно-аппаратным средствам защиты информации.

Курсовые работы для студентов

Курсовая работа для студентов очно-заочного обучения представляет собой объединение контрольной работы и домашнего задания, выполняемых студентами очного отделения. Задания на курсовую работу выдаются на

первом занятии. Срок окончания выполнения контрольной работы – последнее аудиторное занятие. Требования к выполнению курсовой работы указаны в п.3.

4.1 Перечень тематик курсовых работ (проектов)

1. Методология защиты информации как теоретический базис построения СИБ предприятия. Методологические основы организации СИБ предприятия.
2. Принципы организации СИБ предприятия. Основные требования, предъявляемые к СИБ предприятия.
3. Содержательная характеристика этапов разработки СИБ предприятия. Основные факторы, влияющие на организацию обеспечения ИБ предприятия.
4. Характер и степень влияния различных факторов на организацию СИБ предприятия.
5. Методика определения состава защищаемой информации на предприятии.
6. Этапы работы по выявлению состава защищаемой информации на предприятии.
7. Функции руководства предприятия и руководителей подразделений по обеспечению информационной безопасности.
8. Функции экспертной комиссии по защите информации на предприятии.
9. Функции и структура службы информационной безопасности на предприятии.
10. Классификация защищаемой информации по видам тайн и степеням конфиденциальности (секретности) в системе информационной безопасности на предприятии.
11. Нормативное закрепление состава защищаемой информации и структура перечня сведений, относимых к различным видам тайны при реализации СИБ на предприятии.
12. Внедрение перечня защищаемых сведений и порядок внесения в них изменений (дополнений) в СИБ на предприятии.
13. Факторы, определяющие состав носителей с защищаемой информацией в СИБ на предприятии.
14. Методика выявления состава носителей защищаемой информации в СИБ на предприятии.
15. Хранилища носителей с защищаемой информацией в СИБ на предприятии.
16. Особенности помещений для работы с защищаемой информацией как объекты СИБ предприятия.
17. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами СИБ предприятия.
18. Факторы, определяющие необходимость защиты периметра и здания предприятия в СИБ предприятия.

19. Персонал предприятия как объект защиты в СИБ.
20. Определение дестабилизирующих воздействий на защищаемую информацию в СИБ предприятия.
21. Выявление способов воздействия на защищаемую информацию в СИБ предприятия.
22. Оценка ущерба от потенциального дестабилизирующего воздействия на защищаемую информацию в СИБ предприятия.
23. Методика выявления каналов несанкционированного доступа к защищаемой информации в СИБ предприятия.
24. Определение возможных методов несанкционированного доступа к защищаемой информации в СИБ предприятия.
25. Оценка степени опасности применения различных методов НСД в СИБ предприятия.
26. Виды потенциальных последствий несанкционированного доступа в СИБ предприятия.
27. Методика выявления нарушителей (злоумышленников) в СИБ предприятия.
28. Определение возможностей несанкционированного доступа нарушителей (злоумышленников) в СИБ предприятия.
29. Оценка степени уязвимости защищаемой информации в СИБ предприятия.
30. Факторы, влияющие на выбор потребных компонентов СИБ предприятия.
31. Объекты защиты, определяющие потребный состав компонентов СИБ предприятия.
32. Требования, предъявляемые к выбору методов и средств защиты информации в СИБ предприятия
33. Факторы и обстоятельства, влияющие на качество защиты информации в СИБ предприятия.
34. Виды обеспечения функционирования СИБ предприятия.
35. Выбор структуры СИБ в зависимости от объектов защиты, характера и условий функционирования предприятия.
36. Функциональная модель СИБ предприятия.
37. Организационная модель СИБ предприятия.
38. Информационная модель СИБ предприятия.
39. Кибернетическая модель СИБ предприятия.

4.2 Методические указания по выполнению курсовых работ

Цель курсовой работы – закрепление теоретических знаний, полученных при
освоении дисциплины, и их адаптация к конкретной предметной области.
Выбор темы курсовой работы осуществляется студентом либо самостоятельно, либо с помощью преподавателя.

На титульном листе указывается: наименование учреждения образования; факультета и кафедры; полное наименование дисциплины (записывается с прописной буквы); тема курсовой работы; шифр учебной группы; фамилия, имя, отчество студента в родительном падеже; фамилия и инициалы преподавателя.

Оформление курсовой работы:

- текст должен быть напечатан на одной стороне листа белой бумаги формата А4;
- работу выполнять шрифтом Times New Roman;
- размер шрифта -14;
- межстрочный интервал -1,5;
- поля: 30 мм — левое, 20 мм - правое, 20 мм — верхнее и нижнее;
- применять сквозную нумерацию страниц;
- объем работы-10-12 страниц.

Курсовые работы выполнять в строгом соответствии с вариантом студента, утвержденным преподавателем.

Текст работы должен быть написан в строгом соответствии с правилами русской орфографии, синтаксиса и пунктуации. Описки, ошибки при расчетах, обнаруженные в процессе выполнения курсовой работы, допускается исправлять аккуратной подчисткой и нанесением на том же месте исправленного текста.

В конце курсовой работы приводится перечень использованной литературы.

В конце курсовой работы необходимо ставить подпись и дату.

Дата написания (завершения) курсовой работы проставляется после списка использованной литературы в левой части страницы, а подпись студента - с правой части страницы. Оформляется дата двумя способами: словесно-числовым или только числовым (арабскими цифрами), например 1 января 2012 г. или 01. 01.2012.

Примечание:

- Курсовая работа, оформленная небрежно, а также выполненная по неправильно выбранному варианту, возвращается студенту без проверки с указанием причин возврата.
- В случае выполнения работы по неправильно выбранному варианту студент должен выполнить работу согласно своему варианту задания.
- Не засчитывается и возвращается студенту на доработку с подробной рецензией курсовая работа, если в ней не раскрыты теоретические вопросы задания или ответы на них полностью переписаны из учебной литературы, без адаптации к конкретному заданию.
- Доработанный вариант незачтенной курсовой работы представляется на рецензирование вместе с прежним вариантом, при этом правильно выполненная часть задания не переписывается.

- Студенты, не выполнившие курсовую работу, к итоговой аттестации не допускаются.

Сроки сдачи курсовой работы определяются техническим заданием, выданным преподавателем.

5. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Тема 2. Международные стандарты информационной безопасности**	***Подготовка докладов по темам:*** 1. Предназначение стандартов информационной безопасности (ИБ), необходимость их использования. 2. Общие критерии безопасности информационных технологий (стандарт ISO 15408). 3. Взаимосвязь между общими критериями и общей методологией оценки. 4. Структура технического отчета об оценке. 5. Стандарты для беспроводных сетей.
2.	**Тема 3. Отечественные стандарты информационной безопасности**	***Подготовка докладов по темам:*** 1. Стандарты в сети Internet. 2. Отечественные стандарты безопасности информационных технологий. 3. Нормативные документы по критериям оценки защищенности средств вычислительной техники (СВТ) и автоматизированных систем (АС). 4. Документы, регулирующие информационную безопасность. Достоинства ГОСТ Р ИСО/МЭК 15408 - 2002. 5. Структура функционального класса. 6. Структура функционального семейства.
3	**Тема 4. Критерии оценки доверенных компьютерных систем («Оранжевая книга»)**	***Подготовка докладов по темам:*** 1. Общая схема представления класса. 2. Структура функционального компонента. 3. Критерии оценки доверенных компьютерных систем («Оранжевая книга»). Назначение и структура требований. 4. Группы классов защищенности и их характеристики. 5. Руководящие документы Гостехкомиссии России (ФСТЭК). 6. Межсетевые экраны. Показатели защищенности. 7. Классификация АС и требования по защите информации. 8. Программное обеспечение средств защиты информации. 9. Общие критерии. Основные положения. 10. Структура и содержание профиля защиты. 11. Структура и содержание задания по безопасности.

4	**Тема 5. Руководящие документы Гостехкомиссии России (ФСТЭК).**	***Подготовка докладов по темам:*** 1. Функциональные требования безопасности. 2. Требования доверия. Методы оценки. Оценочные уровни доверия. 3. Основные положения концепции защиты СВТ и АС от НСД к информации 4. Средства вычислительной техники. Защита от НСД к информации. Показатели защищённости от НСД к информации 5. Автоматизированные системы. Защита от НСД к информации. Классификация. АС и требования по защите информации 6. ISO/IEC 17799:2005 7. ISO/IEC 27001:2005 8. BS 7799-3:2006
	Тема: Защита интеллектуальной собственности	***Подготовка докладов по темам:*** 1. Объекты и субъекты промышленной собственности. 2. Оформление прав правообладателя. 3. Объем правовой охраны, представляемый патентом. 4. Неалгоритмизированные методы инженерного творчества. 5. Алгоритмизированные методы инженерного творчества. 6. Инженер как субъект труда и жизни. 7. Виды и ступени инженерного творчества. 8. Интеллектуальное право на результаты интеллектуальной деятельности.

Примерные темы докладов

5. Указания по проведению контрольных работ

5.1. Требования к структуре

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

5.2. Требования к содержанию (основной части)

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

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

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

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

5. Необходимо давать ссылки на используемую литературу.

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

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

5.3. Требования к оформлению

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

5.4.Примерная тематика контрольных работ:

1.Характеристика организационных мероприятий по обеспечению информационной безопасности.
2. Организационные мероприятия разового характера по обеспечению информационной безопасности.
3. Периодически проводимые организационные мероприятия по обеспечению информационной безопасности.
4. Постоянно проводимые организационные мероприятия по обеспечению информационной безопасности.
5. Характеристика службы информационной безопасности .
6. Типовая структура службаинформационной безопасности.
7. Характеристика сотрудников службы информационной безопасности
8. Персонал как источник угрозы безопасности информации.
9. Организационные мероприятия по работе с персоналом, получающим доступ к информации ограниченного доступа.
10. Организационные методы добывания информации через персонал.
11. Подготовительная работа по приему сотрудников на работу с информацией ограниченного доступа.
12. Прием сотрудников на работу с информацией ограниченного доступа.
13. Разрешительная система допуска к информации ограниченного доступа.
14. Режим секретности по работе с документами со сведениями относимых к государственной тайне.
15. Оформления допуска к государственной тайне.
16. Работы с персоналом, владеющим информацией ограниченного доступа.
17. Увольнения сотрудников, владеющих информацией ограниченного доступа.
18. Организационные принципы защищенного документооборота.

19. Технологическая система обработки и хранения документов ограниченного доступа.
20. Типовые технологии обработки и хранения документов ограниченного доступа.
21. Учет и контроль документов ограниченного доступа.
22. Проверка наличия документов ограниченного доступа.
23. Организация уничтожения документов ограниченного доступа.
24. Защита информации при проведении совещаний.
25. Защита информации при проведении переговоров.
26. Безопасность информации в рекламно - выставочных материалах.
27. Организация защиты информации при работе с посетителями.
28. Организация приема посетителей на режимных объектах.
29. Документация кадровых органов, содержащая конфиденциальную информацию.
30. Организация работы с конфиденциальной документацией кадровых органов.
31. Организационно-правовые основы охраны объектов.
32. Технологии организации охраны объектов.
33. Привлекаемые силы для охраны информационных объектов.
34. Организация физической охраны информационных объектов.
35. Технические средства охраны информационных объектов.
36. Организация пропускного режима.

Вариант 2

Примерная тематика контрольных работ:

1. Секретность, конфиденциальность, целостность и доступность информации. Основные свойства защищаемой информации.
2. Соотношение понятий «защита информации» и «информационная безопасность». Цель и задачи защиты информации.
3. Организационно – правовые принципы защиты информации.
4. Понятие правовой защиты информации, ее методов и способов. Правовое регулирование защиты информации.
5. Общая характеристика подзаконных и ведомственных нормативно – правовых актов, регулирующих защиту государственной и служебной тайны.
6. Виды подзаконных, ведомственных и межведомственных правовых актов в сфере защиты информации.
7. Порядок допуска должностных лиц и граждан РФ к государственной тайне.
8. Подзаконные, ведомственные и локальные правовые акты, действующие в сфере защиты основных видов конфиденциальной информации.
9. Назначение и задачи подзаконных правовых актов, регулирующих процессы защиты персональных данных и коммерческой тайны.

10. Закрепление права предприятия на защиту информации в нормативных документах (коллективном договоре, трудовом договоре, иных локальных правовых актах организаций).
11. Правовые основы деятельности подразделений по защите конфиденциальной информации на предприятиях, в учреждениях и организациях. Организация доступа персонала к коммерческой тайне.
12. Понятие информации конфиденциального характера. Перечень сведений конфиденциального характера.
13. Правовая основа защиты конфиденциальной информации.
14. Общая характеристика правового регулирования государственной защиты участников уголовного судопроизводства в РФ.
15. Законодательство РФ о государственной защите участников уголовного судопроизводства.
16. Принципы осуществления государственной защиты участников уголовного судопроизводства.
17. Сущность государственной защиты участников уголовного судопроизводства.
18. Содержание мер государственной защиты участников уголовного судопроизводства.
19. Правовые основания применения государственной защиты.
20. Права и обязанности защищаемых лиц. Права и обязанности органов, обеспечивающих государственную защиту.
21. Правовые санкции за разглашение сведений о защищаемых лицах и мерах государственной защиты.

6. Указания по проведению курсовой работы (курсового проекта)

Курсовые работы (проекты)

В процессе обучения студенты выполняют курсовую работу, задание на которую разрабатывается индивидуально для каждого студента и выдается на первом аудиторном занятии. Срок выполнения курсовой работы – 6-ая неделя семестра. Отчет по контрольной работе должен содержать требования к организационному и правовому обеспечению информационной безопасности.

Курсовые работы для студентов

Курсовая работа для студентов очно-заочного обучения представляет собой объединение контрольной работы и домашнего задания, выполняемых студентами очного отделения. Задания на курсовую работу выдаются на первом занятии. Срок окончания выполнения контрольной работы –

последнее аудиторное занятие. Требования к выполнению курсовой работы указаны в п.6.

6.1 Перечень тематик курсовых работ (проектов)

1. Характеристика организационных мероприятий по обеспечению информационной безопасности.
2. Организационные мероприятия разового характера по обеспечению информационной безопасности.
3. Периодически проводимые организационные мероприятия по обеспечению информационной безопасности.
4. Постоянно проводимые организационные мероприятия по обеспечению информационной безопасности.
5. Характеристика службы информационной безопасности .
6. Типовая структура службаинформационной безопасности.
7. Характеристика сотрудников службы информационной безопасности
8. Персонал как источник угрозы безопасности информации.
9. Организационные мероприятия по работе с персоналом, получающим доступ к информации ограниченного доступа.
10. Организационные методы добывания информации через персонал.
11. Подготовительная работа по приему сотрудников на работу с информацией ограниченного доступа.
12. Прием сотрудников на работу с информацией ограниченного доступа.
13. Разрешительная система допуска к информации ограниченного доступа.
14. Режим секретности по работе с документами со сведениями относимых к государственной тайне.
15. Оформления допуска к государственной тайне.
16. Работы с персоналом, владеющим информацией ограниченного доступа.
17. Увольнения сотрудников, владеющих информацией ограниченного доступа.
18. Организационные принципы защищенного документооборота.
19. Технологическая система обработки и хранения документов ограниченного доступа.
20. Типовые технологии обработки и хранения документов ограниченного доступа.
21. Учет и контроль документов ограниченного доступа.
22. Проверка наличия документов ограниченного доступа.
23. Организация уничтожения документов ограниченного доступа.
24. Защита информации при проведении совещаний.
25. Защита информации при проведении переговоров.
26. Безопасность информации в рекламно - выставочных материалах.
27. Организация защиты информации при работе с посетителями.
28. Организация приема посетителей на режимных объектах.
29. Документация кадровых органов, содержащая конфиденциальную информацию.

30. Организация работы с конфиденциальной документацией кадровых органов.
31. Организационно-правовые основы охраны объектов.
32. Технологии организации охраны объектов.
33. Привлекаемые силы для охраны информационных объектов.
34. Организация физической охраны информационных объектов.
35. Технические средства охраны информационных объектов.
36. Организация пропускного режима.
37. Виды пропусков и порядок их оформления.
38. Оборудование контрольно-пропускных пунктов для прохода людей.
39. Оборудование транспортных контрольно-пропускных пунктов.
40. Организация допуска на территорию предприятия.

6.2 Методические указания по выполнению курсовых работ

Цель курсовой работы – закрепление теоретических знаний, полученных при
освоении дисциплины, и их адаптация к конкретной предметной области.
Выбор темы курсовой работы осуществляется студентом либо самостоятельно, либо с помощью преподавателя.

На титульном листе указывается: наименование учреждения образования; факультета и кафедры; полное наименование дисциплины (записывается с прописной буквы); тема курсовой работы; шифр учебной группы; фамилия, имя, отчество студента в родительном падеже; фамилия и инициалы преподавателя.

Оформление курсовой работы:
- текст должен быть напечатан на одной стороне листа белой бумаги формата А4;
- работу выполнять шрифтом Times New Roman;
- размер шрифта -14;
- межстрочный интервал -1,5;
- поля: 30 мм — левое, 20 мм - правое, 20 мм — верхнее и нижнее;
- применять сквозную нумерацию страниц;
- объем работы-10-12 страниц.

Курсовые работы выполнять в строгом соответствии с вариантом студента, утвержденным преподавателем.

Текст работы должен быть написан в строгом соответствии с правилами русской орфографии, синтаксиса и пунктуации. Описки, ошибки при расчетах, обнаруженные в процессе выполнения курсовой работы, допускается исправлять аккуратной подчисткой и нанесением на том же месте исправленного текста.

В конце курсовой работы приводится перечень использованной литературы.

В конце курсовой работы необходимо ставить подпись и дату.

Дата написания (завершения) курсовой работы проставляется после списка использованной литературы в левой части страницы, а подпись студента - с правой части страницы. Оформляется дата двумя способами: словесно-числовым или только числовым (арабскими цифрами), например 1 января 2012 г. или 01. 01.2012.

Примечание:

- Курсовая работа, оформленная небрежно, а также выполненная по неправильно выбранному варианту, возвращается студенту без проверки с указанием причин возврата.
- В случае выполнения работы по неправильно выбранному варианту студент должен выполнить работу согласно своему варианту задания.
- Не засчитывается и возвращается студенту на доработку с подробной рецензией курсовая работа, если в ней не раскрыты теоретические вопросы задания или ответы на них полностью переписаны из учебной литературы, без адаптации к конкретному заданию.
- Доработанный вариант незачтенной курсовой работы представляется на рецензирование вместе с прежним вариантом, при этом правильно выполненная часть задания не переписывается.
- Студенты, не выполнившие курсовую работу, к итоговой аттестации не допускаются.

Сроки сдачи курсовой работы определяются техническим заданием, выданным преподавателем.

7. Перечень основной и дополнительной учебной литературы

Основная литература:

1.Организационно-правовое обеспечение информационной безопасности : учебник / А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев [и др.] ; под редакцией А. А. Александрова, М. П. Сычева. — Москва : МГТУ им. Баумана, 2018. — 291 с. — ISBN 978-5-7038-4723-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/172840 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

2.Крыжановский, А. В. Организационное и правовое обеспечение информационной безопасности : методические указания / А. В. Крыжановский. — Самара : ПГУТИ, 2018. — 56 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182279 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

3.Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, Н. Н. Прохожев. — Санкт-Петербург : НИУ ИТМО, 2016. — 168 с. — Текст : электронный // Лань : электронно-

библиотечная система. — URL: https://e.lanbook.com/book/91449 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.
4.Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности : учебное пособие / Г. П. Жигулин. — Санкт-Петербург : НИУ ИТМО, 2014. — 173 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/70952 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

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

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета.
2. Рабочая программа и методическое обеспечение по дисциплине «Организационно и правовое обеспечение информационной безопасности».