УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий
от «_18_» __05_____2021__г., протокол №_4/21_
Председатель _____М.А. Волков___
(подпись, расшифровка подписи)
«_18_» ___05_____ 2021___г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Организационное и правовое обеспечение информационной безопасности
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	3

Специальность: 10.05.03 "Информационная безопасность автоматизированных систем"
(код специальности (направления), полное наименование)

Специализация: "Безопасность открытых информационных систем"
полное наименование

Форма обучения:_____очная_____
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: «_01_»_____09_____2021_г.

Программа актуализирована на заседании кафедры: протокол № 13 от 11.05.2022 г.
Программа актуализирована на заседании кафедры: протокол № 12 от 12.04.2023 г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Иванцов Андрей Михайлович	ИБ и ТУ	Кандидат технических наук, доцент

СОГЛАСОВАНО
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
_____/ Андреев А.С. / *(подпись) (Ф.И.О.)* «_12_»___05_____2021_ г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Дисциплина «Организационное и правовое обеспечение информационной безопасности» является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Дисциплина реализует требования федерального государственного образовательного стандарта высшего профессионального образования по специальности "Информационная безопасность автоматизированных систем".

Задачи освоения дисциплины:

изучить основные документы по информационной безопасности;

обеспечить освоение студентами практических навыков работы с нормативно-правовой базой в области обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Организационное и правовое обеспечение информационной безопасности» изучается в 5 семестре и относится к дисциплинам обязательной части блока Б1.О. Дисциплина основывается на знаниях, полученных при изучении дисциплин «Основы информационной безопасности», «Правоведение».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

- знание базовых профессиональных понятий и определений в области информационной безопасности;
- способность использовать нормативные правовые документы;
- способность использовать основные положения и методы социальных и гуманитарных наук;
- способность анализировать социально-значимые проблемы и процессы.

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: «Основы управленческой деятельности», «Профессиональная этика», а также в ходе всех видов практик и в повседневной деятельности.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	**Знать:** основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации 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 правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности **Уметь:** обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации **Владеть:** навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации
ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать:** 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 **Уметь:** организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю **Владеть:** навыками организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами
ОПК-14 - Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований	**Знать:** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах **Уметь:** осуществлять разработку, внедрение и эксплуатацию ав-

по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	томатизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования типовых проектных решений **Владеть:** навыками осуществления разработки, внедрения и эксплуатации автоматизированных систем с учетом требований по защите информации

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 3.

4.2. Объем дисциплины по видам учебной работы (в часах):

Вид учебной работы	Количество часов (форма обучения ____очная_____)			
	Всего по плану	В т.ч. по семестрам		
		5		
Контактная работа обучающихся с преподавателем	54	54/54*		
Аудиторные занятия:	54	54/54*		
Лекции	18	18/18*		
Практические и семинарские занятия	36	36/36*		
Лабораторные работы (лабораторный практикум)				
Самостоятельная работа	54	54		
Форма текущего контроля знаний и контроля самостоятельной работы: Тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на семинарах; - рефераты на заданные темы		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	зачет	зачет		
Всего часов по дисциплине	108	108		

* В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения

4.3. Содержание дисциплины (модуля.) Распределение часов по темам и видам учебной работы:

Форма обучения _____очная_____

Название и разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практические занятия, семинары	Лабораторные работы			
Раздел 1. Правовое обеспечение информационной безопасности							
1. Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности. Правовая охрана результатов интеллектуальной деятельности.	12	2	4			6	Тесты Т1, реф. 1, 2, 9
2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной инф.	12	2	4		4	6	Тесты Т2, реф. 4
3. Законодательство РФ по вопросам защиты персональных данных.	12	2	4		4	6	Тесты Т3, реф 5, 6
4. Государственная система лицензирования и сертификации в области защиты информации.	12	2	4			6	Тесты Т4, реф 7,8
Раздел 2. Организационное обеспечение информационной безопасности							
5. Методы обеспечения физической безопасности. Особенности защиты компьютерной информации.	12	2	4		4	6	Тесты Т5, реф. 10, 11, 12
6. Организация режима секретности. Допуск к государственной тайне.	12	2	4			6	Тесты Т6, реф. 3, 13
Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры							
7. Основы обеспечения безопасности объектов критической информационной инфраструктуры	12	2	4			6	Тесты Т7, реф. 14, 15, 16

8. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры	12	2	4		2	6	Тесты Т8, реф. 17
9. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры	12	2	4		2	6	Тесты Т98, реф. 18
Итого:	108	18	36		18	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Правовое обеспечение информационной безопасности

Тема 1. Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности.

Структура информационной сферы и характеристика ее элементов. Субъекты и объекты правоотношений в области информационной безопасности. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения. Информация ограниченного доступа. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации Понятие и виды защищаемой информации по законодательству РФ. Правовая охрана результатов интеллектуальной деятельности

Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав. Объекты и субъекты авторского права. Авторские права (личные неимущественные права и исключительное право). Правовая охрана баз данных, топологий интегральных микросхем и единых технологий. Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.

Тема 2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации.

Понятие коммерческой, профессиональной тайн и служебной информации по российскому законодательству. Коммерческая, профессиональная тайны. Служебная тайна. Правовые режимы тайн. Юридическая ответственность за нарушения правовых режимов информации ограниченного доступа (дисциплинарная, гражданско-правовая, административная, уголовная).

Тема 3. Законодательство Российской Федерации по вопросам защиты персональных данных.

Основные мероприятия по вопросам защиты информации и документы, разрабатываемые на предприятии в соответствии с Федеральным законом РФ «О персональных данных».

Тема 4. Государственная система лицензирования и сертификации в области защиты информации.

В данной теме рассмотрены основные руководящие документы, определяющие порядок лицензирования и сертификации в области защиты информации, виды деятельности, подлежащие лицензированию, основные принципы и правила системы лицензирования; сертификация средств защиты информации.

Раздел 2. Организационное обеспечение информационной безопасности

Тема 5. Методы обеспечения физической безопасности. Особенности защиты компьютерной информации.

Объекты обеспечения физической безопасности: сооружения, предметы, люди. Методы и средства технической охраны объектов информатизации. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения. Безопасность при транспортировке носителей информации. Инженерная защита. Пропускной режим. Особенности защиты компьютерной информации. Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах. Аппаратные закладки. Виброакустический канал утечки информации. Визуальный канал утечки информации. Программные и аппаратные средства защиты от несанкционированного доступа. Парольная система доступа. Защита на различных уровнях: операционная система, прикладные программы. Программные закладки. Разграничение доступа. Регистрация. Остаточная информация. Защита от копирования.

Тема 6. Организация режима секретности. Допуск к государственной тайне

Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Виды представления информации. Пути прохождения информации. Учет получения, перемещения, преобразования, хранения и уничтожения информации. Первые отделы. Категорирование объектов. Подбор и расстановка кадров. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование. Процедура оформления и переоформления допусков и ее документирование, подлежащие согласованию с органами государственной безопасности. Особенности инструктажа и документальное оформление контракта об оформлении допуска к государственной тайне. Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны.

Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры

Тема 7. Основы обеспечения безопасности объектов критической информационной инфраструктуры

Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации. Угрозы безопасности информации, обрабатываемой на объекте КИИ. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации.

Тема 8. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры

Категорирование объектов КИИ. Требования по обеспечению безопасности значимых объектов КИИ. Система безопасности значимого объекта КИИ. Стадии (этапы) работ по созданию систем безопасности. Выявление управленческих, технологических производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.

Тема 9. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры

Разработка документов по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий:

Раздел 1. Правовое обеспечение информационной безопасности

Тема 1. Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности (семинар). Правовая охрана результатов интеллектуальной деятельности.

1. Информация как объект правоотношений.
2. Виды и содержание тайн.
3. Законодательная база охраны государственной тайны.
4. Законодательная база охраны коммерческой тайны.
5. Законодательная база охраны служебной тайны.
6. Правовая охрана результатов интеллектуальной деятельности.

Тема 2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации (семинар).

1. Законодательство о коммерческой тайне.
2. Правовые основы защиты служебной тайны.
3. Правовые основы защиты профессиональных тайн.

Тема 3. Законодательство Российской Федерации по вопросам защиты персональных данных (семинар)**.**

1. Требования законодательства России по вопросам защиты персональных данных.

2. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных.

Тема 4. Государственная система лицензирования и сертификации в области защиты информации (семинар)**.**

1. Основные руководящие документы, определяющие порядок лицензирования и сертификации в области защиты информации.
2. Виды деятельности, подлежащие лицензированию.
3. Основные принципы и правила системы лицензирования:
   - Общие принципы и правила лицензирования;
   - Лицензирование средств криптографической защиты информации
4. Сертификация средств защиты информации

Раздел 2. Организационное обеспечение информационной безопасности

Тема 5. Методы обеспечения физической безопасности. Особенности защиты компьютерной информации (семинар).

1. Методы и средства технической охраны объектов информатизации.
2. Системы сигнализации. Противостояние взлому: двери, замки, запоры, ограждения.
3. Методы и средства инженерной защиты объектов информатизации.
4. Пропускной режим предприятия.
5. Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах.

Тема 6. Организация режима секретности. Допуск к государственной тайне (семинар).

1. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.

2. Порядок допуска и доступа к государственной тайне.

3. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.

Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры

Тема 7. Основы обеспечения безопасности объектов критической информационной инфраструктуры (семинар).

1. Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации.
2. Угрозы безопасности информации, обрабатываемой на объекте КИИ.
3. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации.

Тема 8. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры

1. Категорирование объектов КИИ.
2. Требования по обеспечению безопасности значимых объектов КИИ.
3. Стадии (этапы) работ по созданию систем безопасности.
4. Выявление управленческих, технологических производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.

Тема 9. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры

1. Основные документы по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ.
2. Контроль сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры).
3. Анализ защищенности значимого объекта КИИ на соответствие требованиям по обеспечению безопасности.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Лабораторные работы не предусмотрены учебным планом дисциплины.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

8.2 Примерная тематика рефератов:

1. Законодательство РФ об информационной безопасности.
2. Требования Федерального закона РФ «Об информации, информационных технологиях и о защите информации».
3. Требования Федерального закона РФ «О государственной тайне».
4. Требования Федерального закона РФ «О коммерческой тайне».
5. Законодательство РФ в области защиты персональных данных.
6. Проблемы защиты персональных данных.
7. Государственная система лицензирования в области защиты информации.
8. Государственная система сертификации в области защиты информации.
9. Юридическая ответственность за нарушение авторских прав.
10. Методы обеспечения физической безопасности объектов информатизации.
11. Основные каналы утечки информации при обработке на компьютерах.
12. Программные и аппаратные средства защиты информации от несанкционированного доступа.
13. Допуск к государственной тайне. Мероприятия и документы.

14. Требования Федерального закона РФ "О безопасности критической информационной инфраструктуры Российской Федерации".

15. Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации.

16. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации.

17. Категорирование объектов КИИ.

18. Анализ защищенности значимого объекта КИИ на соответствие требованиям по обеспечению безопасности.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЁТУ

1. Информация как объект правоотношений. Законодательство РФ в области информационной безопасности

2. Виды и содержание тайн. Законодательная база охраны государственной тайны.

3. Виды и содержание тайн. Законодательная база охраны коммерческой тайны.

4. Виды и содержание тайн. Законодательная база охраны служебной тайны.

5. Организационные, правовые и технические меры для введения на предприятии режима коммерческой тайны.

6. Виды и содержание тайн. Законодательная база охраны персональных данных.

7. Виды и содержание тайн. Правовые основы защиты профессиональных тайн.

8. Порядок предоставления государственным органам сведений, отнесённой к коммерческой тайне предприятия.

9. Порядок отнесения сведений к государственной тайне.

10. Система защиты сведений, составляющих государственную тайну.

11. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных.

12. Первоочередные мероприятия по созданию системы защиты персональных данных на предприятии.

13. Основные руководящие документы, определяющие порядок лицензирования и сертификации в области защиты информации.

14. Виды деятельности, подлежащие лицензированию. Порядок получения лицензии в области защиты информации.

15. Сертификация средств защиты информации.

16. Общие положения в области охраны результатов интеллектуальной деятельности. Авторское право и смежные права.

17. Общие положения в области охраны результатов интеллектуальной деятельности. Патентное право. Право на секрет производства (ноу-хау).

18. Юридическая ответственность за нарушение авторских прав.

19. Методы и средства технической охраны объектов информатизации.

20. Системы сигнализации. Противостояние взлому: двери, замки, запоры, ограждения.

21. Концепция инженерной защиты и технической охраны объекта.

22. Методы и средства инженерной защиты объектов информатизации.

23. Пропускной режим предприятия.

24. Порядок допуска и доступа к государственной тайне.

25. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.

26. Основные каналы утечки информации при обработке на компьютерах.

27. Виброакустический канал утечки информации. Методы и средства защиты.

28. Визуальный канал утечки информации. Методы и средства защиты.

29. Программные и аппаратные средства защиты от несанкционированного доступа.

30. Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации.

31. Угрозы безопасности информации, обрабатываемой на объекте КИИ.

32. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации.

33. Категорирование объектов КИИ. Требования по обеспечению безопасности значимых объектов КИИ.

34. Система безопасности значимого объекта КИИ. Стадии (этапы) работ по созданию систем безопасности.

35. Основные документы по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ.

7. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Правовое обеспечение информационной безопасности Тема 1. Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 1. Тема 2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 1. Тема 3. Законодательство Российской Федерации по вопросам защиты персональных данных	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 1. Тема 4. Государственная система лицензирования и сертификации в области защиты информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 2. Организационное обеспечение ИБ. Тема 5. Методы обеспечения физической безопасности. Особенности	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт

защиты компьютерной информации			
Раздел 2. Тема 6. Организация режима секретности. Допуск к государственной тайне	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры Тема 7. Основы обеспечения безопасности объектов критической информационной инфраструктуры	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 3. Тема 8. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 3. Тема 9. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Новиков В.К., Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: Учебное пособие. / В.К. Новиков - М.: Горячая линия - Телеком, 2015. - 176 с. - ISBN 978-5-9912-0525-2 - Режим доступа: 1.

2. Судариков С.А., Право интеллектуальной собственности: учебник [Электронный ресурс] / С.А. Судариков. - М.: Проспект, 2014. - 368 с. - ISBN 978-5-392-16752-4 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785392167524.html

дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":

1.1 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")

Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

1.2 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации")

Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

1.3 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

1.4. Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации"
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

1.5 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

1.6 Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

1.7 Постановление Правительства РФ от 06.02.2010 N 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_97474/

1.8 Часть четвертая Гражданского кодекса Российской Федерации (231-ФЗ от 18.12.2006) Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_64629/

1.9 Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_220885/

2. ГОСТ Р ИСО/МЭК 27002-2021 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

3. Котенко Е.С., Авторские права на мультимедийный продукт [Электронный ресурс]: монография / Е.С. Котенко. - М.: Проспект, 2014. - 128 с. - ISBN 978-5-392-11705-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785392117055.html.

учебно-методическая

1. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск: УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). URL: http://edu.ulsu.ru/cources/750/interface/.

2. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Организационное и правовое обеспечение информационной безопасности» для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. **Иванцов**; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2020. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл: 329 КБ). - Текст: электронный.
http://lib.ulsu.ru/MegaPro/Download/MObject/4264

Согласовано:

Гл.библ-рь КБ УлГУ	Попина И.Ю		04.05.2021
должность сотрудника научной библиотеки	ФИО	подпись	дата

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2021]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2021]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2021]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача : электронно-библиотечная система : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2021]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2021]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2021]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2021]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102 . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. Русский язык как иностранный : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2021]. – URL: https://ros-edu.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2021].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2021]. – URL: https://dlib.eastview.com/browse/udb/12. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2021]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2021]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Национальная электронная библиотека : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2021]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase // EBSCOhost : [портал]. – URL: https://ebsco.smartimagebase.com/?TOKEN=EBSCO-

1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://window.edu.ru/ . – Текст : электронный.

6.2. Российское образование : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://www.edu.ru. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ : модуль АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст: электронный.

Согласовано:

Зам.нач. УИТиТ	/ Клочкова А.В.	/	04.05.2021
должность сотрудника УИТиТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

- мультимедийные средства: компьютер и проектор;
- мультимедийные технологии. MS Office, Internet Explorer;
- система защиты конфиденциальной информации и персональных данных «Secret Disk. Базовый комплект с USB-ключом – 4 комплекта;
- электронный замок "Соболь" – 3 комплекта;
- персональные средства аутентификации и защищённого хранения данных - USB-ключи и смарт-карты eToken – 3 комплекта;
- система защиты от НСД «Dallas Lock». 4 комплекта;
- программно-аппаратный комплекс средств защиты информации от НСД “Аккорд–АМДЗ” – 1 комплект.

Аудитория для проведения занятий - 2/24б.

Аудитория 2/24б укомплектована специализированной мебелью, учебной доской, имеются мульт мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающимся) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических возможностей:

– для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик: _____ доцент кафедры Иванцов Андрей Михайлович
подпись должность ФИО

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/выпускающей кафедрой	Подпись	Дата
1.	Провести актуализацию рабочей программы по включению вопросов обеспечения безопасности объектов критической информационной инфраструктуры (КИИ). Основание: Решение Совета УМЦ по защите информации ПФО и регионального отделения УМО ИБ ПФО от 01.03.2022 (г. Киров) с оформлением приложения № 1-7	Андреев А.С.		11.05.2022 Протокол заседания кафедры № 13
2.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 8	Андреев А.С.		11.05.2022 Протокол заседания кафедры № 13
3.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 9	Андреев А.С.		12.04.2023 Протокол заседания кафедры № 12

Приложение 1

4.3. Содержание дисциплины (модуля.) Распределение часов по темам и видам учебной работы:

Форма обучения _____очная_____

Название и разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практические занятия, семинары	Лабораторные работы			
Раздел 1. Правовое обеспечение информационной безопасности							
1. Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности. Правовая охрана результатов интеллектуальной деятельности.	12	2	4			6	Тесты Т1, реф. 1, 2, 9
2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной инф.	12	2	4		4	6	Тесты Т2, реф. 4
3. Законодательство РФ по вопросам защиты персональных данных.	12	2	4		4	6	Тесты Т3, реф 5, 6
4. Государственная система лицензирования и сертификации в области защиты информации.	12	2	4			6	Тесты Т4, реф 7,8
Раздел 2. Организационное обеспечение информационной безопасности							
5. Методы обеспечения физической безопасности. Особенности защиты компьютерной информации.	12	2	4		4	6	Тесты Т5, реф. 10, 11, 12
6. Организация режима секретности. Допуск к государственной тайне.	12	2	4			6	Тесты Т6, реф. 3, 13
Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры							
7. Основы обеспечения безопасности объектов критической информационной инфраструктуры	12	2	4			6	Тесты Т7, реф. 14, 15, 16

8. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры	12	2	4		2	6	Тесты Т8, реф. 17
9. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры	12	2	4		2	6	Тесты Т98, реф. 18
Итого:	108	18	36		18	54	

Приложение 2

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Правовое обеспечение информационной безопасности

Тема 1. Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности.

Структура информационной сферы и характеристика ее элементов. Субъекты и объекты правоотношений в области информационной безопасности. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения. Информация ограниченного доступа. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации Понятие и виды защищаемой информации по законодательству РФ. Правовая охрана результатов интеллектуальной деятельности

Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав. Объекты и субъекты авторского права. Авторские права (личные неимущественные права и исключительное право). Правовая охрана баз данных, топологий интегральных микросхем и единых технологий. Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.

Тема 2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации.

Понятие коммерческой, профессиональной тайн и служебной информации по российскому законодательству. Коммерческая, профессиональная тайны. Служебная тайна. Правовые режимы тайн. Юридическая ответственность за нарушения правовых режимов информации ограниченного доступа (дисциплинарная, гражданско-правовая, административная, уголовная).

Тема 3. Законодательство Российской Федерации по вопросам защиты персональных данных.

Основные мероприятия по вопросам защиты информации и документы, разрабатываемые на предприятии в соответствии с Федеральным законом РФ «О персональных данных».

Тема 4. Государственная система лицензирования и сертификации в области защиты информации.

В данной теме рассмотрены основные руководящие документы, определяющие порядок лицензирования и сертификации в области защиты информации, виды деятельности, подлежащие лицензированию, основные принципы и правила системы лицензирования; сертификация средств защиты информации.

Раздел 2. Организационное обеспечение информационной безопасности

Тема 5. Методы обеспечения физической безопасности. Особенности защиты компьютерной информации.

Объекты обеспечения физической безопасности: сооружения, предметы, люди. Методы и средства технической охраны объектов информатизации. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения. Безопасность при транспортировке носителей информации. Инженерная защита. Пропускной режим. Особенности защиты компьютерной информации. Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах. Аппаратные закладки. Виброакустический канал утечки информации. Визуальный канал утечки информации. Программные и аппаратные средства защиты от несанкционированного доступа. Парольная система доступа. Защита на различных уровнях: операционная система, прикладные программы. Программные закладки. Разграничение доступа. Регистрация. Остаточная информация. Защита от копирования.

Тема 6. Организация режима секретности. Допуск к государственной тайне

Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.

Виды представления информации. Пути прохождения информации. Учет получения, перемещения, преобразования, хранения и уничтожения информации. Первые отделы. Категорирование объектов. Подбор и расстановка кадров. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование. Процедура оформления и переоформления допусков и ее документирование, подлежащие согласованию с органами государственной безопасности. Особенности инструктажа и документальное оформление контракта об оформлении допуска к государственной тайне. Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны.

Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры

Тема 7. Основы обеспечения безопасности объектов критической информационной инфраструктуры

Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации. Угрозы безопасности информации, обрабатываемой на объекте КИИ. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации.

Тема 8. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры

Категорирование объектов КИИ. Требования по обеспечению безопасности значимых объектов КИИ. Система безопасности значимого объекта КИИ. Стадии (этапы) работ по созданию систем безопасности. Выявление управленческих, технологических производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.

Тема 9. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры

Разработка документов по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий:

Раздел 1. Правовое обеспечение информационной безопасности

Тема 1. Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности (семинар). Правовая охрана результатов интеллектуальной деятельности.

1. Информация как объект правоотношений.
2. Виды и содержание тайн.
3. Законодательная база охраны государственной тайны.
4. Законодательная база охраны коммерческой тайны.
5. Законодательная база охраны служебной тайны.
6. Правовая охрана результатов интеллектуальной деятельности.

Тема 2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации (семинар).

1. Законодательство о коммерческой тайне.
2. Правовые основы защиты служебной тайны.
3. Правовые основы защиты профессиональных тайн.

Тема 3. Законодательство Российской Федерации по вопросам защиты персональных данных (семинар).

1. Требования законодательства России по вопросам защиты персональных данных.
2. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных.

Тема 4. Государственная система лицензирования и сертификации в области защиты информации (семинар).

1. Основные руководящие документы, определяющие порядок лицензирования и сертификации в области защиты информации.
2. Виды деятельности, подлежащие лицензированию.
3. Основные принципы и правила системы лицензирования:
   - Общие принципы и правила лицензирования;
   - Лицензирование средств криптографической защиты информации
4. Сертификация средств защиты информации

Раздел 2. Организационное обеспечение информационной безопасности

Тема 5. Методы обеспечения физической безопасности. Особенности защиты компьютерной информации (семинар).

1. Методы и средства технической охраны объектов информатизации.
2. Системы сигнализации. Противостояние взлому: двери, замки, запоры, ограждения.
3. Методы и средства инженерной защиты объектов информатизации.
4. Пропускной режим предприятия.
5. Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах.

Тема 6. Организация режима секретности. Допуск к государственной тайне (семинар).

1. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.
2. Порядок допуска и доступа к государственной тайне.
3. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.

Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры

Тема 7. Основы обеспечения безопасности объектов критической информационной инфраструктуры (семинар).

1. Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации.

2. Угрозы безопасности информации, обрабатываемой на объекте КИИ.

3. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации.

Тема 8. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры

1. Категорирование объектов КИИ.

2. Требования по обеспечению безопасности значимых объектов КИИ.

3. Стадии (этапы) работ по созданию систем безопасности.

4. Выявление управленческих, технологических производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.

Тема 9. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры

1. Основные документы по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ.

2. Контроль сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры).

3. Анализ защищенности значимого объекта КИИ на соответствие требованиям по обеспечению безопасности.

Приложение 4

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

8.2 Примерная тематика рефератов:

1. Законодательство РФ об информационной безопасности.
2. Требования Федерального закона РФ «Об информации, информационных технологиях и о защите информации».
3. Требования Федерального закона РФ «О государственной тайне».
4. Требования Федерального закона РФ «О коммерческой тайне».
5. Законодательство РФ в области защиты персональных данных.
6. Проблемы защиты персональных данных.
7. Государственная система лицензирования в области защиты информации.
8. Государственная система сертификации в области защиты информации.
9. Юридическая ответственность за нарушение авторских прав.
10. Методы обеспечения физической безопасности объектов информатизации.
11. Основные каналы утечки информации при обработке на компьютерах.
12. Программные и аппаратные средства защиты информации от несанкционированного доступа.
13. Допуск к государственной тайне. Мероприятия и документы.
14. Требования Федерального закона РФ "О безопасности критической информационной инфраструктуры Российской Федерации".
15. Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации.
16. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации.
17. Категорирование объектов КИИ.
18. Анализ защищенности значимого объекта КИИ на соответствие требованиям по обеспечению безопасности.

Приложение 5

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЁТУ

1. Информация как объект правоотношений. Законодательство РФ в области информационной безопасности

2. Виды и содержание тайн. Законодательная база охраны государственной тайны.

3. Виды и содержание тайн. Законодательная база охраны коммерческой тайны.

4. Виды и содержание тайн. Законодательная база охраны служебной тайны.

5. Организационные, правовые и технические меры для введения на предприятии режима коммерческой тайны.

6. Виды и содержание тайн. Законодательная база охраны персональных данных.

7. Виды и содержание тайн. Правовые основы защиты профессиональных тайн.

8. Порядок предоставления государственным органам сведений, отнесённой к коммерческой тайне предприятия.

9. Порядок отнесения сведений к государственной тайне.

10. Система защиты сведений, составляющих государственную тайну.

11. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных.

12. Первоочередные мероприятия по созданию системы защиты персональных данных на предприятии.

13. Основные руководящие документы, определяющие порядок лицензирования и сертификации в области защиты информации.

14. Виды деятельности, подлежащие лицензированию. Порядок получения лицензии в области защиты информации.

15. Сертификация средств защиты информации.

16. Общие положения в области охраны результатов интеллектуальной деятельности. Авторское право и смежные права.

17. Общие положения в области охраны результатов интеллектуальной деятельности. Патентное право. Право на секрет производства (ноу-хау).

18. Юридическая ответственность за нарушение авторских прав.

19. Методы и средства технической охраны объектов информатизации.

20. Системы сигнализации. Противостояние взлому: двери, замки, запоры, ограждения.

21. Концепция инженерной защиты и технической охраны объекта.

22. Методы и средства инженерной защиты объектов информатизации.

23. Пропускной режим предприятия.

24. Порядок допуска и доступа к государственной тайне.

25. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.

26. Основные каналы утечки информации при обработке на компьютерах.

27. Виброаккустический канал утечки информации. Методы и средства защиты.

28. Визуальный канал утечки информации. Методы и средства защиты.

29. Программные и аппаратные средства защиты от несанкционированного доступа.

30. Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации.

31. Угрозы безопасности информации, обрабатываемой на объекте КИИ.

32. Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности

информации.

33. Категорирование объектов КИИ. Требования по обеспечению безопасности значимых объектов КИИ.

34. Система безопасности значимого объекта КИИ. Стадии (этапы) работ по созданию систем безопасности.

35. Основные документы по результатам внутреннего контроля за обеспечением безопасности значимого объекта КИИ.

Приложение 6

7. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Правовое обеспечение информационной безопасности Тема 1. Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 1. Тема 2. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 1. Тема 3. Законодательство Российской Федерации по вопросам защиты персональных данных	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 1. Тема 4. Государственная система лицензирования и сертификации в области защиты информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 2. Организационное обеспечение ИБ. Тема 5. Методы обеспечения физической безопасности. Особенности защиты компьютерной информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 2. Тема 6. Организация режима секретности. Допуск к государственной тайне	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры Тема 7. Основы обеспечения безопасности объектов критической информационной	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт

инфраструктуры			
Раздел 3. Тема 8. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 3. Тема 9. Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт

Приложение 7

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Новиков В.К., Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: Учебное пособие. / В.К. Новиков - М.: Горячая линия - Телеком, 2015. - 176 с. - ISBN 978-5-9912-0525-2 - Режим доступа: 1.

2. Судариков С.А., Право интеллектуальной собственности: учебник [Электронный ресурс] / С.А. Судариков. - М.: Проспект, 2014. - 368 с. - ISBN 978-5-392-16752-4 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785392167524.html

дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":

1.1 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

1.2 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

1.3 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

1.4. Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации"
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

1.5 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

1.6 Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

1.7 Постановление Правительства РФ от 06.02.2010 N 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_97474/

1.8 Часть четвертая Гражданского кодекса Российской Федерации (231-ФЗ от 18.12.2006) Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_64629/

1.9 Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_220885/

2. ГОСТ Р ИСО/МЭК 27002-2021 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

3. Котенко Е.С., Авторские права на мультимедийный продукт [Электронный ресурс]: монография / Е.С. Котенко. - М.: Проспект, 2014. - 128 с. - ISBN 978-5-392-11705-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785392117055.html.

учебно-методическая

1. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск: УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). URL: http://edu.ulsu.ru/cources/750/interface/.

2. Иванцов А. М. Методические указания для самостоятельной работы студентов

по дисциплине «Организационное и правовое обеспечение информационной безопасности» для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. **Иванцов**; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2020. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл: 329 КБ). - Текст: электронный.
http://lib.ulsu.ru/MegaPro/Download/MObject/4264

Приложение 8

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2022]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2022]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2022]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2022]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2022]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2022]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2022]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : научно-информационная база данных EBSCO // EBSCOhost : [портал]. – URL: http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102 . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. База данных «Русский как иностранный» : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2022]. – URL: https://ros-edu.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2022].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий EastView : электронные журналы / ООО ИВИС. - Москва, [2022]. – URL: https://dlib.eastview.com/browse/udb/12. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2022]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД Гребенников. – Москва, [2022]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2022]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase : научно-информационная база данных EBSCO // EBSCOhost

: [портал]. – URL: https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал . – URL: http://window.edu.ru/ . – Текст : электронный.

6.2. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Зам.нач. УИТиТ	/ Клочкова А.В.	/	/
должность сотрудника УИТиТ	ФИО	подпись	дата

Приложение 9

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО «Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг». – Москва, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС «Лань». – Санкт-Петербург, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com :** электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.