МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Луганский государственный университет имени Владимира Даля»
(ФГБОУ ВО «ЛГУ им. В. Даля»)

Юридический институт
Кафедра административного и экологического права

УТВЕРЖДАЮ:
Директор Юридического института
_____проф. Л.И. Лазор
(подпись)
«__» ____04_____ 2023 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ»

По направлению подготовки 40.04.01 Юриспруденция
Магистерская программа: «Уголовно-правовая»

Луганск – 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины «Информационная безопасность в сфере государственного управления» по направлению подготовки 40.04.01 Юриспруденция. – 35 с.

Рабочая программа учебной дисциплины «Информационная безопасность в сфере государственного управления» составлена с учетом Федерального государственного образовательного стандарта высшего образования - магистратура по направлению подготовки 40.04.01 Юриспруденция (утвержденный приказом Министерства науки и высшего образования Российской Федерации от 25 ноября 2020 года № 1451).

СОСТАВИТЕЛЬ:
канд. юр. наук, доцент Афанасьев К.К.

Рабочая программа дисциплины утверждена на заседании кафедры административного и экологического права «24» 03 2023 г., протокол № 8

Заведующийкафедрой
административного и экологического права _____ доц. К.К. Афанасьев

Переутверждена: «___» _____2023 г., протокол № _____

Согласована (для обеспечивающей кафедры):
Директор Юридического института _____ проф. Л.И. Лазор

Переутверждена: «___» _____20____ года, протокол № _____

Рекомендована на заседании учебно-методической комиссии Юридического института «20» 04 2023 г., протокол № 9.

Председатель учебно-методической
комиссии Юридического института _____В.А. Зверяка

Структура и содержание дисциплины

1. Цели и задачи дисциплины, ее место в учебном процессе

Целью изучения дисциплины «Информационная безопасность в сфере государственного управления» являетсяраскрытие:теоретических основ информационной безопасности в сфере государственного управления; содержания правового и организационного регулирования отношений в области защиты информации; понятия видов защищаемой информации по законодательству Российской Федерации; системы защиты государственной тайны и конфиденциальной информации, а также основ государственного контроля в области информационной безопасности и видов правонарушений в информационной сфере.

Задачами дисциплины являются: изучение основ информационного законодательства Российской Федерации, правил нормативного регулирования в сфере информационной безопасности, знаний о правонарушениях в информационной сфере; формирование у студентов высокого уровня правосознания в правовом регулировании информационных общественных отношений информационной сферы и практики эффективного применения механизмов правового регулирования информационных общественных отношений.

В результате изучения дисциплины студент должен

знать: содержание основных понятий по правовому и организационному обеспечению информационной безопасности; правовые и организационные основы защиты государственной тайны и конфиденциальной информации; основы нормативных требований в области защиты информации и особенности организации контроля (надзора) органами государственной власти, регламентирующими обеспечение информационной безопасности в РФ; виды ответственности в области правонарушений в информационной сфере

уметь: использовать правовые знания в различных сферах информационной деятельности; разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем; участвовать в формировании комплекса мер (правила, процедуры, методы) для защиты информации ограниченного доступа

владеть: навыками применения нормативно правовых актов в области информационной безопасности

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность в сфере государственного управления» входит в часть, формируемую участниками образовательных отношений учебного плана подготовки студентовпо направлению подготовки 40.04.01 Юриспруденция.

Необходимыми условиями для освоения дисциплины являются: знания основных положений информационного права, организационно-правовых основ государственного управления; умения анализировать содержание

государственной информационной деятельности, состояние информационной безопасности; навыки использования информационных систем и технологий в профессиональной деятельности юриста. Содержание дисциплины является логическим продолжением содержания дисциплин «Административное право», «Информационное право», «Информационные технологии в юридической деятельности» и служит основой для освоения дисциплин«Противодействие коррупционным нарушениям»,«Судебная экспертиза», а знания материалов данной дисциплины могут использоваться в процессе написания магистерской диссертации и в дальнейшей профессиональной деятельности.

3. Требования к результатам освоения содержания дисциплины

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Выбирает на государственном и иностранном (-ых) языках коммуникативно приемлемые стиль делового общения, вербальные и невербальные средства взаимодействия с партнерами УК-4.2. Использует информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (-ых) языках УК-4.4. Умеет коммуникативно и культурно приемлемо вести устные деловые разговоры на государственном и иностранном (-ых) языках	Знать: современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации Уметь: применять на практике коммуникативные технологии, методы и способы делового общения Владеть: методикой межличностного делового общения на государственном и иностранном языках

ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	ОПК-7.1. Работает с разными источниками информации, поисковыми и правовыми системами с учетом требований информационной безопасности ОПК-7.2. Использует в профессиональной деятельности правовые системы, современные цифровые инструменты, технические средства и программное обеспечение для поиска, обработки правовой информации, оформление юридических документов и проведения статистического анализа информации ОПК-7.3. Внедряет в процессе профессиональной деятельности современные технические средства и информационно-коммуникационные технологии	Знать: назначение, функции, компоненты информационных технологий и ключевые алгоритмы решения задач с их применением в профессиональной деятельности, а также основные источники, включая правовые базы данных, для получения юридически значимой информации, принципы и правила защиты конфиденциальной информации и информационной безопасности в целом Уметь: подбирать технические и программные средства и реализовать решение ключевых задач профессиональной деятельности с помощью информационных технологий, а также использовать справочные правовые системы для составления подборки правовых актов, относящихся к анализируемой ситуации, осуществлять информационные технологии сбора, хранения, поиска и обработки информации в юридической деятельности Владеть: навыками осуществления поиска профессиональной информации, в том числе навыками использования справочных правовых систем для поиска изменений в законодательстве и правоприменительной практике, а также навыками обработки, хранения, представления и передачи данных с помощью информационных технологий
ПК-5. Способен участвовать в организации правового сопровождения деятельности органов публичной власти	ПК-5.1. Представляет интересы органов публичной власти во взаимоотношениях с другими органами власти ПК-5.2. Осуществляет исполнительно-распорядительные и обеспечивающие функции ПК-5.3. Способен осуществлять координацию	Знать: нормативно-правовые основы деятельности органов публичной власти Уметь: давать квалифицированные юридические заключения и консультации по правовому сопровождению деятельности органов публичной власти Владеть: навыками организации правового сопровождения деятельности органов публичной власти

	деятельности должностных лиц органов публичной власти	

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов (зач. ед.)		
	Очная форма	**Очно-заочная форма**	**Заочная форма**
Общая учебная нагрузка (всего)	**180 (5зач. ед)**	**-**	**180 (5зач. ед)**
Обязательная контактная работа (всего) в том числе:	**48**	**-**	**20**
Лекции	12	-	8
Семинарские занятия	36	-	12
Практические занятия	-	-	-
Лабораторные работы	-	-	-
Курсовая работа (курсовой проект)	-	-	-
Другие формы и методы организации образовательного процесса (*расчетно-графические работы,* индивидуальные задания *и т.п.)*	-	-	-
Самостоятельная работа студента (всего)	**132**	**-**	**160**
Форма аттестации	экзамен	-	экзамен

4.2. Содержание разделов дисциплины

Тема 1. Теоретические основы информационной безопасности

Политика государства в области информатизации общества и в отрасли информационных технологий.

Составляющие национальных интересов Российской Федерациив информационной сфере. Понятие, сущность и актуальность защиты информации.Предмет и объект защиты информации. Основные определения и задачи информационной безопасности.Основные принципы и методы защиты информации. Уровни правового обеспечения информационной безопасности. Риски и угрозы информационной безопасности. Принципы построения защищенных систем. Нормативно-правовое обеспечение информационнойбезопасности. Стандарты информационной безопасности

Патриотизм и историческая память как опорные категории российской информационной политики. Переход от информационного противоборства к диалогу культур как практика межгосударственной информационной политики.

Тема 2. Информационная безопасность в сфере государственного управления

Информационная безопасность: понятие, содержание. Принципы государственной информационной безопасности. Задачи обеспечения безопасностив информационной сфере. Информационная функция в системе функций государственного управления, ее системообразующий характер.

Значение информации для основных групп государственно-управленческих функций (функции ориентирования системы, обеспечения системы и оперативного управления системой). Формы и методы управления, используемые исполнительными органами государственной власти в процессе осуществления полномочий в сфере информационной безопасности. Информационная безопасностьв системе видов государственной безопасности.

Угрозы, риски, правонарушения в областиинформационной безопасности. Правовые гарантии обеспечения информационнойбезопасности.

Информационная безопасность личности как приоритетная задача электронной России.

Тема 3. Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации

Категории информации по условиям доступа к ней.

Законодательство в области защиты персональных данных. Классификация информационных систем персональных данных. Базовая и частная модели угроз безопасности персональных данных. Классификация государственных информационных систем и требования к их защищенности

Персональные данные. Коммерческая тайна. Служебная тайна. Профессиональные тайны. Процессуальные тайны.

Отнесение сведений к различным видам конфиденциальной информации. Грифы секретности и реквизиты носителей сведений, составляющих государственную и коммерческую тайну. Порядок засекречивания и рассекречивания сведений, отнесенных к государственной тайне. Порядок и отнесение сведений к коммерческой тайне. Организация допуска и доступа персонала к конфиденциальной информации

Государственная тайна. Государственная система зашиты информации. Правовые основы защиты государственной тайны. Допуск должностных лиц и граждан к государственной тайне.

Тема 4. Организационно-правовые основы государственной деятельности, связанной с обеспечением информационной безопасности

Нормативно-правовая и институциональная база государственных управленческих решений в сфере обеспечения информационной безопасности. Особенности современных угроз в сфере информационной безопасности.

Структура, задачи и основные функции органов государственной власти, ответственных за организацию защиты информации в РФ. Правовые основы лицензирования, сертификации и аттестации в области защиты информации.

Органы государственного управления, обеспечивающие реализацию информационной функции в системе государственного управления. Федеральные и территориальные органы исполнительной власти РФ, обеспечивающие информационную безопасность в государстве.

Исполнительные органы государственной власти РФ, обеспечивающие контроль и надзор в сфере оборота информации.

Информация как объект правовых отношений. Конституция РФ как основной регулятор правоотношений, возникающих в процессе оборота информации. Основные нормативные правовые акты РФ, формирующие правовые основы для государственной деятельности по обеспечению информационной безопасности.

Принципы организационной защиты информации. Основные направления организационной защиты информации. Подходы и требования к организации системы защиты информации. Основные силы и средства, используемые для организации защиты информации.

Организационные методы защиты информации. Разработка организационно-распорядительных документов в области защиты информации.

Тема 5. Методологические основы государственной деятельности, связанной с обеспечением информационной безопасности

Методы и технологии защиты информации.Классификация методов и средств защиты информации. Антивирусная защита. Системы идентификации и аутентификации.Системы разграничения доступа. Стенографические и криптографические методы защиты информации. Технология электронной подписи. Методы обнаружения и блокирования угроз информационнойбезопасности. Методы защиты информации в операционных системах.Сетевые технологии защиты информации.

Тема 6. Юридическая ответственность за правонарушения в сфере связи, информационных технологий и массовых коммуникаций.

Ответственность за нарушение режима информационной безопасности.

Государственный контроль(надзор) за деятельностью по технической защите конфиденциальной информации ФСТЭК. Государственный контроль(надзор) за деятельностью в области защиты информации ФСБ. Государственный контроль(надзор) за соответствием обработки и защиты персональных данных требованиям законодательства РФ.

Нормативно-правовое обеспечение в сфере связи и коммуникации. Государственное регулирование вопросов использования криптографических средств и ЭЦП.

Административные правонарушения в сфере связи, информационных технологий и массовых коммуникаций. Субъекты административной ответственности за правонарушения в сфере связи, информационных технологий и массовых коммуникаций.

Административное правонарушение,посягающее на состояние информационной безопасности, как фактическое основание административной ответственности лица. Отличие административного правонарушения,посягающего на состояние информационной безопасности, от преступления и дисциплинарного проступка. Особенности состава

административного правонарушения, посягающего на состояние информационной безопасности.

4.3. Лекции

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1.	Теоретические основы информационной безопасности	2	-	-
2.	Информационная безопасность в сфере государственного управления	2	-	2
3.	Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации	2	-	2
4.	Организационно-правовые основы государственной деятельности, связанной с обеспечением информационной безопасности	2	-	2
5.	Методологические основы государственной деятельности, связанной с обеспечением информационной безопасности	2	-	
6.	Юридическая ответственность за правонарушения в сфере связи, информационных технологий и массовых коммуникаций	2	-	2
Итого:		**12**	**-**	**8**

4.4. Практические (семинарские) занятия

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1.	Политика РФ в области информатизации общества и в отрасли информационных технологий.	2	-	2
2.	Предмет и объект защиты информации.	2	-	-
3.	Информационная безопасность: понятие, содержание.	2	-	-
4.	Риски и угрозы информационной безопасности РФ.	2	-	
5.	Значение информации для основных групп государственно-управленческих функций (функции ориентирования системы, обеспечения системы и оперативного управления системой).	2	-	2
6.	Правовые гарантии обеспечения информационной безопасности в РФ.	2	-	-
7.	Категории информации по условиям доступа к ней.	2	-	-
8.	Персональные данные. Коммерческая тайна. Служебная тайна. Профессиональные тайны. Процессуальные тайны.	2	-	2

9.	Государственная тайна и ее защита в РФ.	2	-	-
10.	Нормативно-правовая и институциональная база государственных управленческих решений в сфере обеспечения информационной безопасности.	2	-	2
11.	Органы государственного управления РФ, обеспечивающие реализацию информационной функции в системе государственного управления.	2	-	-
12.	Федеральные и территориальные органы исполнительной власти РФ, обеспечивающие информационную безопасность в государстве.	2	-	-
13.	Принципы организационной защиты информации.	2	-	-
14.	Организационные методы защиты информации.	2	-	2
15.	Методы и технологии защиты информации.	2	-	-
16.	Ответственность за нарушение режима информационной безопасности.	2	-	-
17.	Государственный контроль(надзор) за соответствием обработки и защиты персональных данных требованиям законодательства РФ.	2	-	2
18.	Административная ответственность за правонарушения в сфере связи, информационных технологий и массовых коммуникаций.	2	-	-
Итого:		**36**	**-**	**12**

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов		
			Очная форма	Очно-заочная форма	Заочная форма
1.	Политика РФ в области информатизации общества и в отрасли информационных технологий.	Написание творческого задания	5		7
2.	Предмет и объект защиты информации.	Изучение теоретических положений, решение тестов	5		7
3.	Информационная безопасность: понятие, содержание.	Изучение теоретических положений, решение тестов и ситуативных задач	5		7
4.	Риски и угрозы информационной безопасности РФ.	Написание творческого задания Изучение теоретических положений, решение тестов	5		7

5.	Значение информации для основных групп государственно-управленческих функций (функции ориентирования системы, обеспечения системы и оперативного управления системой).	Написание творческого задания	5		7
6.	Правовые гарантии обеспечения информационной безопасности в РФ.	Написание творческого задания	5		7
7.	Категории информации по условиям доступа к ней.	Написание творческого задания	5		7
8.	Персональные данные. Коммерческая тайна. Служебная тайна. Профессиональные тайны. Процессуальные тайны.	Изучение теоретических положений, решение тестов и ситуативных задач	5		7
9.	Государственная тайна и ее защита в РФ.	Написание творческого задания Изучение теоретических положений, решение тестов	5		7
10.	Нормативно-правовая и институциональная база государственных управленческих решений в сфере обеспечения информационной безопасности.	Написание творческого задания	5		7
11.	Органы государственного управления РФ, обеспечивающие реализацию информационной функции в системе государственного управления.	Изучение теоретических положений, решение тестов и ситуативных задач	5		7
12.	Федеральные и территориальные органы исполнительной власти РФ, обеспечивающие информационную безопасность в государстве.	Изучение теоретических положений, решение тестов и ситуативных задач	5		7

13.	Принципы организационной защиты информации.	Написание творческого задания Изучение теоретических положений, решение тестов	6		7
14.	Организационные методы защиты информации.	Написание творческого задания	6		7
15.	Методы и технологии защиты информации.	Написание творческого задания	6		7
16.	Ответственность за нарушение режима информационной безопасности.	Написание творческого задания Изучение теоретических положений, решение тестов	6		7
17.	Государственный контроль(надзор) за соответствием обработки и защиты персональных данных требованиям законодательства РФ.	Изучение теоретических положений, решение тестов и ситуативных задач	6		6
18.	Административная ответственность за правонарушения в сфере связи, информационных технологий и массовых коммуникаций.	Изучение теоретических положений, решение тестов и ситуативных задач	6		6
19.	Экзамен	Подготовка к экзамену	36	-	36
Итого:			**132**		**160**

4.7. Курсовые работы/проекты по дисциплине «Информационная безопасность в сфере государственного управления» не предполагаются учебным планом.

5. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

традиционные объяснительно-иллюстративные технологии, которые обеспечивают доступность учебного материала для большинства студентов, системность, отработанность организационных форм и привычных методов, относительно малые затраты времени;

технологии проблемного обучения, направленные на развитие познавательной активности, творческой самостоятельности студентов и

предполагающие последовательное и целенаправленное выдвижение перед студентом познавательных задач, разрешение которых позволяет студентам активно усваивать знания (используются поисковые методы; постановка познавательных задач);

технологии развивающего обучения, позволяющие ориентировать учебный процесс на потенциальные возможности студентов, их реализацию и развитие;

технологии концентрированного обучения, суть которых состоит в создании максимально близкой к естественным психологическим особенностям человеческого восприятия структуры учебного процесса и которые дают возможность глубокого и системного изучения содержания учебных дисциплин за счет объединения занятий в тематические блоки;

технологии модульного обучения, дающие возможность обеспечения гибкости процесса обучения, адаптации его к индивидуальным потребностям и особенностям обучающихся (применяются, как правило, при самостоятельном обучении студентов по индивидуальному учебному плану);

технологии дифференцированного обучения, обеспечивающие возможность создания оптимальных условий для развития интересов и способностей студентов, в том числе и студентов с особыми образовательными потребностями, что позволяет реализовать в культурно-образовательном пространстве университета идею создания равных возможностей для получения образования

технологии активного (контекстного) обучения, с помощью которых осуществляется моделирование предметного, проблемного и социального содержания будущей профессиональной деятельности студентов (используются активные и интерактивные методы обучения) и т.д.

Максимальная эффективность педагогического процесса достигается путем конструирования оптимального комплекса педагогических технологий и (или) их элементов на личностно-ориентированной, деятельностной, диалогической основе и использования необходимых современных средств обучения.

6. Учебно-методическое и информационное обеспечение дисциплины:

а) основная литература:

1. Груздева, Л. М. Основы информационной безопасности : учеб. пособие в двух частях. — Ч. 1 / Л. М. Груздева. — М. : Юридический институт МИИТа, 2017. - 101 с.

2. Сухостат В.В. Основы информационной безопасности : учебное пособие / В.В. Сухостат, И.Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 103 с.

3. Бачило, И. Л. Информационное право : учебник для магистров / И. Л. Бачило. - 3-е изд., перераб. и доп. - М. : Издательство Юрайт, 2015. - 564 с. — Серия : Магистр.

4. Административное право: Общая часть: учебник / К.К. Афанасьев, В.И. Ткаченко, А.С. Кравцов; ГОУ ВПО ЛНР «ЛНУ им. В. Даля». – Луганск: Изд-во ГОУ ВПО ЛНР «ЛНУ им. В. Даля», 2020. – 515 с.

5. Административное право: Особенная часть: учебник / Авторский коллектив. – Луганск: Изд-во ЛГУ им. В. Даля, 2021. – 564 с.

б) дополнительная литература:

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»// [Электронный ресурс]. – Режим доступа: https://15.rkn.gov.ru/law/p8182/

2. Федеральный закон Российской Федерации от 5 марта 1992 г. № 2446-I «О безопасности» // [Электронный ресурс]. – Режим доступа: https://15.rkn.gov.ru/law/p8182/

3. Федеральный закон от 21 июля 1993 г. № 5495-ФЗ «О государственной тайне» // Режим доступа: http://svr.gov.ru/svr_today/doc05.htm

4. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» // [Электронный ресурс]. – Режим доступа: https://15.rkn.gov.ru/law/p8182/

5. Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности в Российской Федерации»// [Электронный ресурс]. – Режим доступа: http://pravo.levonevsky.org/bazazru/texts24/txt24598.htm

6. Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // [Электронный ресурс]. – Режим доступа: https://15.rkn.gov.ru/law/p8182/

7. Резер, Т. М. Информационная открытость органов государственного и муниципального управления : учеб. пособие / Т. М. Резер ; М-во образования и науки Рос. Федерации, Урал. федер.ун-т. -Екатеринбург : Изд-во Урал. ун-та, 2018. - 160 с.

8. Килин, А.П. Информационно-аналитическая деятельность в органах государственного управления субъектов Российской Федерации / А.П. Килин, Д.В. Колобова, О.В. Чистякова ; Министерство образования и науки Российской Федерации, Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. - Екатеринбург : Издательство Уральского университета, 2014. - 155 с. : табл. - Библиогр.: с. 135-145. - ISBN 978-5-7996-1208-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=275733

9. Гафарова, Е.А. Организационно-правовое обеспечение информационной безопасности : учебное пособие / Е.А. Гафарова. - Челябинск : Издательство ЗАО «Библиотека А. Миллера». - 153 с.

10. Чеботарева, А. А. Информационное право : учеб. пособие / А. А. Чеботарева. — М. : Юридический институт МИИТа, 2014. - 160 с.

11. Кубанков, А. Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект

[Электронный ресурс] : учебное пособие / А. Н. Кубанков, Н. Н. Куняев ; под ред. А. В. Морозов. — Электрон. текстовые данные. — М. : Всероссийский государственный университет юстиции (РПА Минюста России), 2014. - 78 с. - 978-5-89172-850-9. - Режим доступа: http://www.iprbookshop.ru/47262.html

13. Кудряшова Л. В. Основы государственного и муниципального управления : учебное пособие. В 2-х частях / Л. В. Кудряшова. – Томск : ФДО, ТУСУР, 2015. – Ч. I: Основы государственного управления – 137 с.

в) методические рекомендации:

1. Методические указания к семинарским занятиям по дисциплине «Информационная безопасность в сфере государственного управления» (для студентов направления подготовки 40.04.01 Юриспруденция) / Сост.: К.К. Афанасьев, О.А. Прохорова, В.А. Комаров, А.П. Грепан. – Луганск: ЛГУ им. В. Даля, 2023. – 75 с. – Режим доступа: http://biblio.dahluniver.ru/ , http://91.201.108.138/MegaPro/Web/SearchResult/ToPage/1

2. Методические указания об организации самостоятельной работы по дисциплине «Информационная безопасность в сфере государственного управления» (для студентов направления подготовки 40.04.01 «Юриспруденция») / Сост.: К.К. Афанасьев, О.А. Прохорова, В.А. Комаров, А.П. Грепан. – Луганск: ЛГУ им. В. Даля, 2023. – 32 с. – Режим доступа: http://biblio.dahluniver.ru/,http://91.201.108.138/MegaPro/Web/SearchResult/ToPage/1

3. Методические указания к выполнению контрольных работ по дисциплине «Информационная безопасность в сфере государственного управления» (для студентов заочной формы обучения направления подготовки «Юриспруденция») / Авторы: К.К. Афанасьев, О.А. Прохорова, В.А. Комаров, А.П. Грепан. – Луганск: ЛГУ им. В. Даля, 2023. – 44 с. - Режим доступа: http://biblio.dahluniver.ru/, http://91.201.108.138/MegaPro/Web/SearchResult/ToPage/1

г) Интернет-ресурсы:

Официальные сетевые ресурсы Президента России - http://www.kremlin.ru/contacts

Министерство образования и науки Российской Федерации – https://minobrnauki.gov.ru/

Федеральная служба по надзору в сфере образования и науки – https://obrnadzor.gov.ru/

Федеральные государственные образовательные стандарты высшего образования –https://fgos.ru/

Справочная правовая система «Консультант Плюс» – https://www.consultant.ru/sys/

Электронные библиотечные системы и ресурсы

Научно-техническая библиотека ЮРГПУ (НПИ) - https://www.npi-tu.ru/education/ntb/

Образовательная платформа Юрайт - https://urait.ru/?=

Научная электронная библиотека eLibrary -

https://elibrary.ru/defaultx.asp

Информационный ресурс библиотеки образовательной организации

Научная библиотека имени А. Н. Коняева – https://biblio.dahluniver.ru/

7. Материально-техническое и программное обеспечение дисциплины

Освоение дисциплины «Информационная безопасность в сфере государственного управления» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.

Программное обеспечение:

Функциональное назначение	**Бесплатное программное обеспечение**	**Ссылки**
Офисный пакет	Libre Office 6.3.1	https://www.libreoffice.org/ https://ru.wikipedia.org/wiki/LibreOffice
Операционная система	UBUNTU 19.04	https://ubuntu.com/ https://ru.wikipedia.org/wiki/Ubuntu
Браузер	FirefoxMozilla	http://www.mozilla.org/ru/firefox/fx
Браузер	Opera	http://www.opera.com
Почтовый клиент	MozillaThunderbird	http://www.mozilla.org/ru/thunderbird
Файл-менеджер	FarManager	http://www.farmanager.com/download.php
Архиватор	7Zip	http://www.7-zip.org/
Графический редактор	GIMP (GNU Image Manipulation Program)	http://www.gimp.org/ http://gimp.ru/viewpage.php?page_id=8 http://ru.wikipedia.org/wiki/GIMP
Редактор PDF	PDFCreator	http://www.pdfforge.org/pdfcreator
Аудиоплейер	VLC	http://www.videolan.org/vlc/

8. Оценочные средства по дисциплине

Паспорт
оценочных средств по дисциплине
«Информационная безопасность в сфере государственного управления»

Перечень компетенций (элементов компетенций), формируемых в результате освоения учебной дисциплины

№ п/п	Код контролируемой компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Контролируемые темы учебной дисциплины, практики	Этапы формирования (семестр изучения)
1	УК-4.	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Выбирает на государственном и иностранном (-ых) языках коммуникативно приемлемые стиль делового общения, вербальные и невербальные средства взаимодействия с партнерами УК-4.2. Использует информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (-ых) языках УК-4.4. Умеет коммуникативно и культурно приемлемо вести устные деловые разговоры на государственном	Тема 1. Теоретические основы информационной безопасности Тема 2. Информационная безопасность в сфере государственного управления	3
				Тема 3. Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации	3
				Тема 4. Организационно-правовые основы государственной деятельности, связанной с обеспечением информационной безопасности	3

			и иностранном (-ых) языках		
2.	ОПК-7.	Способенприменять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	ОПК-7.1. Работает с разными источниками информации, поисковыми и правовыми системами с учетом требований информационной безопасности ОПК-7.2. Использует в профессиональной деятельности правовые системы, современные цифровые инструменты, технические средства и программное обеспечение для поиска, обработки правовой информации, оформление юридических документов и проведения статистического анализа информации ОПК-7.3. Внедряет в процессе профессиональной деятельности современные технические средства и информационно-коммуникационные технологии	Тема 2. Информационная безопасность в сфере государственного управления	3
				Тема 4. Организационно-правовые основы государственной деятельности, связанной с обеспечением информационной безопасности	3
				Тема 5. Методологические основы государственной деятельности, связанной с обеспечением информационной безопасности	3
3.	ПК-5.	Способен участвовать в организации правового	ПК-5.1. Представляет интересы органов публичной власти	Тема 2.Информационная безопасность в сфере	3

		сопровождения деятельности органов публичной власти	во взаимоотношениях с другими органами власти ПК-5.2. Осуществляет исполнительно-распорядительные и обеспечивающие функции ПК-5.3. Способен осуществлять координацию деятельности должностных лиц органов публичной власти	государственного управления	
				Тема 3. Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации	3
				Тема 4. Организационно-правовые основы государственной деятельности, связанной с обеспечением информационной безопасности Тема 6. Юридическая ответственность за правонарушения в сфере связи, информационных технологий и массовых коммуникаций	3

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код контролируемой компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов	Контролируемые темы учебной дисциплины	Наименование оценочного средства
1.	УК-4	УК-4.1 УК-4.2 УК-4.4	Знать: виды информационно-коммуникационных технологий, используемых в сфере государственного управления Уметь: использовать информационно-коммуникационные технологии при	Тема 1. Тема 2. Тема 3. Тема 4.	Вопросы для обсуждения (в виде сообщений), тесты, контрольные работы, творческие задания

			поиске необходимой информации в процессе решения стандартных коммуникативных задач в сфере государственного управления (в том числе на иностранном (-ых) языках); соблюдать требования информационной безопасности; Владеть: навыками поиска необходимой информации, в том числе конфиденциальной; навыками решения стандартных коммуникативных задач в сфере государственного управления		
2.	ОПК-7	ОПК-7.1 ОПК-7.2 ОПК-7.3	Знать: современные источники информации, поисковые и правовые системы, основные требования относительно информационной безопасности Уметь: использовать в профессиональной деятельности современные технические средства и информационно-коммуникационные технологии для поиска, обработки правовой информации, в том числе с ограниченным	Тема 2. Тема 4. Тема 5.	Вопросы для обсуждения (в виде сообщений), контрольные работы, творческие задания

			доступом или специальным грифом Владеть: навыками внедрения и использования в процессе профессиональной деятельности современных технических средств и информационно-коммуникационных технологий		
3.	ПК-5	ПК-5.1 ПК-5.2 ПК-5.3	Знать: виды и содержание исполнительно-распорядительных и обеспечивающих функций органов публичной власти в сфере государственного управления; Уметь: осуществлять исполнительно-распорядительные и обеспечивающие функции в процессе профессиональной деятельности, в том числе связанной с информацией Владеть: навыками реализации исполнительно-распорядительных и обеспечивающих функций органов публичной власти в процессе профессиональной деятельности, связанной с информацией; навыками соблюдения требований информационной	Тема 2. Тема 3. Тема 4. Тема 6.	Вопросы для обсуждения (в виде сообщений), тесты, контрольные работы, творческие задания

			безопасности		

Вопросы к контрольным работам

1. Предмет и объект защиты информации.
2. Основные принципы и методы защиты информации.
3. Информационная безопасность в сфере государственного управления: общая характеристика
4. Информационная безопасность: понятие, содержание.
5. Задачи обеспечения безопасности в информационной сфере.
6. Информационная функция в системе функций государственного управления, ее системообразующий характер.
7. Информационная безопасность в системе видов государственной безопасности.
8. Угрозы, риски, правонарушения в области информационной безопасности.
9. Правовые гарантии обеспечения информационной безопасности.
10. Информационная безопасность личности как приоритетная задача электронной России.
11. Категории информации по условиям доступа к ней.
12. Законодательство в области защиты персональных данных.
13. Персональные данные.
14. Коммерческая тайна.
15. Служебная тайна.
16. Профессиональные тайны.
17. Порядок засекречивания и рассекречивания сведений, отнесенных к государственной тайне.
18. Порядок и отнесение сведений к коммерческой тайне.
19. Государственная тайна. Правовые основы защиты государственной тайны.
20. Организационно-правовые основы государственной деятельности, связанной с обеспечением информационной безопасности
21. Структура, задачи и основные функции органов государственной власти, ответственных за организацию защиты информации в РФ.
22. Федеральные и территориальные органы исполнительной власти РФ, обеспечивающие информационную безопасность в государстве.
23. Информация как объект правовых отношений.
24. Основные нормативные правовые акты РФ, формирующие правовые основы для государственной деятельности по обеспечению информационной безопасности.
25. Методы и технологии защиты информации.
26. Ответственность за нарушение режима информационной безопасности.
27. Государственный контроль (надзор) за деятельностью по технической защите конфиденциальной информации ФСТЭК.

28. Государственный контроль (надзор) за деятельностью в области защиты информации ФСБ.

29. Государственный контроль (надзор) за соответствием обработки и защиты персональных данных требованиям законодательства РФ.

30. Административные правонарушения в сфере связи, информационных технологий и массовых коммуникаций.

Задачи к контрольным работам

Задача 1.

Гражданин Иванов, служил в качестве члена научно-исследовательской группы института "Прогресс". Иванов дал интервью для журнала «Метрополитен», в котором оценил радиационную обстановку в регионе с целью продемонстрировать суть его технической разработки по определению интенсивности излучения.

Интервью с Ивановым была опубликовано, информация стала общедоступной, известной научному руководству Института "Прогресс".

Администрация института подала заявление на Иванова о возбуждении уголовного дела по признакам преступлений, предусмотренных ст. 147 и ст. 183 Уголовного кодекса.

Защитнику Иванова стало известно, что Иванов воспользовался для разработки своего технического устройства сведениями, составляющими коммерческую тайну.

Будет ли Иванов привлечен к уголовной ответственности? Как ему избежать уголовной ответственности?

Задача 2

Репортер взял интервью у высокопоставленного чиновника Министерства экономического развития. В интервью были указаны сведения о стратегических запасах золота, платины и серебра. В отношении репортера и чиновника было возбуждено уголовное дело за распространение информации, составляющих государственную тайну.

Что нужно предпринять журналисту и чиновнику, чтобы избежать уголовной ответственности по ст. 283 УК РФ?

Задача 3

Инженер Михайлов, который был гражданином Российской Федерации и инженер Скрипко, который был гражданином Украины, провели совместной научно-исследовательской работу, разработали новую технологию по виртуализации доменов. Оба соавтора имели доступ к сведениям, составляющим государственную тайну. При рассмотрении заявки федеральным органом исполнительной власти по интеллектуальной собственности было установлено, что в новой технологии использованы сведения, составляющие государственную тайну. Какой орган имеет право рассматривать заявки на секретные изобретения, если они относится к техническим средствам в области разведывательной деятельности?

Может ли в Российской Федерации быть выдан патент на секретное изобретение?

Задача 4

Химический комбинат г. Дубоссарск осуществил сброс производственных отходов в реку. Городские власти, получив от санэпидемслужбы города соответствующую информацию, не оповестили граждан об опасности. В результате купающиеся в реке получили ожоги.

Имеется ли вина городской администрации? Приведите правовые нормы, обосновывающие вашу позицию.

Задача 5

Российский научно-исследовательский институт «Квант» являлся разработчиком и создателем информационной базы данных об испытаниях авиационно-космической техники. Институт получил разрешение Правительства РФ и соответственно своего министерства о направлении соответствующей информации о характеристиках авиационной аппаратуры в аналогичную научную организацию, находящуюся на территории Белоруссии.

Однако представитель ФАПСИ, через которого предполагалось обеспечить передачу этой информации, обратил внимание дирекции института на конфиденциальный характер передаваемых сведений и, ссылаясь на этот факт, отказал НИИ в выделении каналов и средств для передачи информации. Институт «Квант» обжаловал решение представителя ФАПСИ в Правительство РФ. Оцените ситуацию с точки зрения действующего законодательства.

Задача 6

Общественная организация «За здоровье нации» обратилась к администрации Аргаяшской птицефабрики с заявлением о предоставлении информации о технике безопасности на предприятии: уровне ПДК в воздухе производственных помещений, уровне травматизма на производстве и выплате компенсаций по здоровьесбережению. Руководство предприятия отказалось удовлетворить просьбу общественной организации, мотивируя свое отказное решение тем, что указанные данные являются конфиденциальной информацией.

Дайте разъяснения по существу сложившейся ситуации, приведите правовые нормы в обоснование своих доводов.

Задача 7

Сотрудники частной нотариальной конторы «Дело» на одном из своих совещаний приняли решение - создать собственный тайный архив, в котором собирать наиболее интересную частную информацию о всех своих клиентах и по мере необходимости использовать ее в своей повседневной деятельности.

На следующий день был назначен руководитель архива и два эксперта и они начали собирать через своих коллег нужные сведения и данные о клиентах. Однако о факте создания тайного архива в нотариальной конторе «Дело» стало известно одному из клиентов, и он пожаловался на нотариусов в прокуратуру.

Нарушила ли в этом случае контора законодательство?

Задача 8

Используя электронную сеть «Межсвязь», главный специалист коммерческого банка «Кубыш» Кусочкин в течение двух недель передавал с магнитных носителей информацию в департамент ценных бумаг ЦБ РФ.

При этом он однажды рассказал о содержании направленных в ЦБ сообщений своему другу -юристу Министерства связи Савенко. Савенко, зная, что его товарищи из адвокатской фирмы «Прокруст» готовят иск против «Кубыш», немедленно переправил им полученную информацию. Адвокаты по достоинству оценили полученные сведения, использовали их при подготовке иска и в итоге – выиграли дело у банка. Узнав об этом, председатель правления коммерческого банка «Кубыш» Кубышкин уволил Кусочкина с работы за разглашение коммерческой тайны. Кусочкин не согласился с решением Кубышкина и обжаловал его действия в суде.

Проанализируйте ситуацию с точки зрения норм информационного права и квалифицируйте действия Кусочкина, Савенко и Кубышкина.

Задача 9

Журналисты провели расследование совместно с общественной организацией «Маяк» и выявили повышенный уровень радиоизлучения в деревне Дербишево, находящейся на расстоянии 60 км от химкобината «Маяк». Об этом было рассказано в газете «За правое дело». Имеются ли в действиях журналистов признаки злоупотребления правом?

Оцените эту ситуацию с точки зрения законодательства о средствах массовой информации. Какие меры здесь необходимо принять к нарушителям?

Задача 10

Лех Я.В. обратился в суд с иском к ООО «Гранада» о взыскании компенсации за нарушение исключительного права на произведение, компенсации морального вреда, возложении обязанности по удалению произведения с сайта.

В обоснование иска указал, что общество разместило на своем сайте литературно-художественный публицистический очерк (документальный рассказ), посвященный дню защиты Земли, автором которого он является Лех. Разрешение на публикацию очерка на сайте ответчика он не давал. Путем размещения на сайте указанного очерка было нарушено его авторское неимущественное право. Представитель ответчика факт размещения произведения истца на сайте не отрицала, исковые требования признала в части компенсации за нарушение ответчиком авторского права истца, при этом ссылалась на завышенный размер компенсации, заявленный истцом. В части компенсации морального вреда иск не признала, ссылаясь на то, что неимущественные права истца ответчиком не нарушены.

Отмечает, что «незаконно использованный» ответчиком очерк по количеству строк более чем в два раза превышает написанный им рассказ, авторские права на который были приобретены московским продюсером за

1000 долларов. При этом над очерком он работал около 4 месяцев, а рассказ написан за 1 день. Как разрешитъ этот спор с позиции норм информационного права?

Задача 11

Смирнов П.Б. обратился в суд с иском к Новиковой Е.О. о защите авторских прав. Свои требования истец мотивирует тем, что на странице интернет-сайта ответчика неправомерно использована фотография, автором которой является истец, без его согласия на воспроизведение и доведение до всеобщего сведения, без заключения с истцом авторского лицензионного договора, без указания и ссылок на источник и автора произведения, что является нарушением ст. 1229, 1265, 1270, 1300 Гражданского кодекса Российской Федерации (далее по тексту ГК РФ). Ответчиком допущено искажение фотографии в частности: кадрирование, обрезка изображения, наложение на фотографию надписи изменение цветового фона изображения. Истец просил взыскать с Новиковой Е.О. денежную компенсацию за нарушение авторских исключительных прав на фотографию (произведение), компенсацию морального вреда за использование фотографии без указания авторства, судебные расходы по обеспечению доказательств нотариусом и расходы по оплате услуг представителя.

Ответчик вину в неправомерном размещении в сети Интернет фотографии не признала, пояснила, что фотографию удалила, ее размещение носило некоммерческий характер. Считает заявленные истцом суммы к взысканию завышенными. Оцените ситуацию с позиции правовых норм. Какое решение должен принять суд?

Задача 12

Организация «Новые технологии», занимающаяся формированием информационных ресурсов, начала разработку новой программы для государственных информационных систем. Для обеспечения защиты информационных ресурсов в этой системе был использован криптографический алгоритм «Крипт» компании «Джомолунгма» . Правомерно ли использование этого криптоалгоритма в разрабатываемой программе? Если да, то при каких условиях?

Задача 13

ООО «Холдинг-М» в лице Москвина осуществляло предоставление возмездных Интернет услуг с применением 2-х электронных терминалов «Инфоинтсэйл», на жестких дисках которых установлены и использовались для работы терминала два экземпляра программы для ЭВМ «MicrosoftWindows XP Professional», обладателем авторских и смежных прав на которую является «Корпорация Microsoft».

Вышеуказанные экземпляры ЭВМ являются контрафактными по следующими признакам: отсутствуют документы, подтверждающие приобретение копии программы «MicrosoftWindows XP Professional»; в корпусе системного блока не имеется сертификата подлинности программы (СОА) с наименованием и уникальным буквенно-цифровым ключом

программного продукта; отсутствует соглашение с правообладателем об участии в программе корпоративного лицензирования, тем самым ООО «Холдинг-М» использовало с целью получения прибыли программу для ЭВМ «MicrosoftWindows XP Professional». Представитель ООО «Холдинг-М» Москвин пояснял, что документов, подтверждающих приобретение обществом операционной «Windows XP» у него не имеется.

Оцените ситуацию с точки зрения авторского права.

Задача 14

Оператор ПК Абдуллин, согласно своим должностным обязанностям, при приеме электронных носителей с материалами обязан был проверять их на наличие вирусов. Пытаясь завершить работу как можно скорее, Абдуллин проигнорировал проверку на антивирусном программном обеспечении.

В результате попадания вируса в компьютерную систему был испорчен готовый к печати оригинал-макет выпуска газеты. Редакция понесла убытки, был нанесен репутационный вред изданию.

Оцените действия Абдуллина с точки зрения действующего законодательства.

Задача 15

Разработчик программного обеспечения Стив несколько лет работал в акционерном обществе "Галатея". В трудовом договоре не было указано на явно имущественные права на созданные программы в процессе трудовой деятельности программиста.

Во время работы Стив разработал эффективную систему автоматизации учета товаров на предприятии. Увидев, что его программа дает значительный экономический эффект, Стив потребовал от руководства доплату к ежемесячному окладу. Руководство рассмотрело вопрос по оплате и отказалось осуществлять доплату, вместо этого они приняли на работу еще одного программиста. Стив, в надежде, что он не сможет прийти к соглашению с компаниями, модифицировал свою программу, в результате чего она перестала функционировать.

Оцените сложившуюся ситуацию с точки зрения действующего законодательства. Как квалифицировать действия Стива?

Задача 16

Программисту Иванову было поручено создать базу данных по финансовым и нематериальным активам предприятия. В целях быстрейшего Иванов, стремясь выполнить свою работу как можно быстрее, проигнорировал требования антивирусной защиты. В результате база данных и программная оболочка были повреждены, предприятию пришлось закупать новое программное обеспечение. На программиста было наложено административное взыскание штраф, с чем он не согласился и обжаловал действия администрации

Имеются ли здесь нарушения законодательства об информации, информатизации, защите информации и трудового права?

Задача 17

Адвокат Хорошавин, работая в юридической фирме «Лига А» в качестве помощника генерального директора, получил несанкционированный доступ к программам других людей и постоянно использовал их. Более того, часть информации, полученной в базах данных, адвокат Хорошавин продал заинтересованным людям. В то же время, из-за несанкционированного проникновения помощника генерального директора в вышеупомянутые программы, в них начали появляться сбои, после чего владельцы источников информации, чтобы найти причину сбоя программного обеспечения провели экспертизу и установили причину сбоев. Владельцы программ и баз данных потребовали строгого наказания Хорошавина. Оцените сложившуюся ситуацию с точки зрения действующего законодательства.

Задача 18

Сельский почтальон по просьбе своей дочери подслушивал телефонные разговоры ее мужа. Он постоянно вскрывал письма и рассказывал об их содержании своей дочери, жалея ее, ведь она могла остаться одна и воспитывать двоих детей, если муж уйдет от нее к другой женщине.

Имеются ли нарушения законодательства?

Задача 19

Разработчик программного обеспечения Шариков использовал часть алгоритма своего знакомого Кошечкина, уехавшего некоторое время назад в Европу. Шариков зарегистрировал программу в установленном порядке и получил охранный документ. Кошечкин узнал о коммерческом использовании Шариковым программного продукта и подал на него в суд. Необходимо классифицировать действия Шарикова и Кошечкина. Будет ли удовлетворен иск?

Задача 20

Петровский получил на телефон сообщение, в котором был прислан единоразовый пароль для входа в личный кабинет банковских транзакций его подруги Ивановской. Однажды Ивановская просила его телефон для проведения транзакций и, по-видимому, «привязала» номер к личному профилю интернет-банка. Петровский помнил номер карты Ивановской и, воспользовавшись единоразовым паролем, перевел часть денежных средств с банковской карты Ивановской на свой расчетный счет. Оцените действия Петровского и Ивановской с точки зрения информационной безопасности и норм права.

Критерии и шкала оценивания по оценочному средству «контрольная работа»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Контрольная работа выполнена на высоком уровне (правильные

	ответы даны на 90-100% вопросов/задач)
4	Контрольная работа выполнена на среднем уровне (правильные ответы даны на 75-89% вопросов/задач)
3	Контрольная работа выполнена на низком уровне (правильные ответы даны на 50-74% вопросов/задач)
2	Контрольная работа выполнена на неудовлетворительном уровне (правильные ответы даны менее чем на 50%)

Творческие задания

1. Раскройте содержание базовых понятий, видов и источников информации, подлежащей защите.
2. Определите систему, задачи, принципы институтов информационного права.
3. Дайте характеристику элементам системы информационного законодательства РФ.
4. Раскройте содержание информационно-правовых норм Конституции России.
5. Дайте характеристику отраслям законодательства РФ, содержащим нормативные Законодательные акты регулирующие общественные отношения в информационной сфере.
6. Раскройте содержание основных нормативных правовых актов информационного законодательства РФ
7. Осуществите классификацию и приведите характеристики правонарушений режима защиты конфиденциальной информации.
8. Сформулируйте и аргументируйте систему основных признаков информации как объекта правоотношений.
9. Проанализируйте и раскройте содержание понятия информационной безопасности субъекта.
10. Осуществите классификацию видов угроз информационной безопасности личности, общества, государства.
11. Подготовьте видеопрезентацию о месте информационной безопасности в системе национальной безопасности России.
12. Раскройте содержание функции организационного и правового регулирования информационной безопасности и ее значение для системы комплексной защиты информации.
13. Приведите факторы, обосновывающие необходимость развития правовой системы информационного общества.
14. Определите проблемы формирования и развития направлений государственной политики Российской Федерации в сфере информационной безопасности.

15. Раскройте содержание Концепции правовой информатизации субъектов Российской Федерации как основы информационной безопасности личности, общества, государства.

16. Назовите основания и систему классификации нормативных правовых актов РФ по информационной безопасности.

17. Систематизируйте основные нормы Конституции РФ и Гражданского кодекса о правах и обязанностях граждан России в сфере информационной безопасности.

18. Раскройте содержание элементов системы лицензирования РФ в области защиты конфиденциальной информации.

19. Покажите и обоснуйте алгоритм проведения административного расследования по фактам нарушения установленного порядка обеспечения информационной безопасности

20. Перечислите и раскройте содержание государственных мер по предупреждению правонарушений в информационной среде

Критерии и шкала оценивания по оценочному средству «творческое задание»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Творческое задание представлено на высоком уровне (студент в полном объеме осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений и т.п.). Оформлено в соответствии с требованиями предъявляемыми к данному виду работ.
4	Творческое задание представлено на среднем уровне (студент в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений и т.п.). В оформлении допущены некоторые неточности в соответствии с требованиями, предъявляемыми к данному виду работ.
3	Творческое задание представлено на низком уровне (студент допустил существенные неточности, изложил материал с ошибками и т.п.). В оформлении допущены ошибки в соответствии с требованиями, предъявляемыми к данному виду работ.
2	Творческое задание представлено на неудовлетворительном уровне или не представлен (студент не готов, не выполнил задание и т.п.)

Тесты

1. Что не входит в перечень сведений, составляющих гос.тайну?

а) Сведения в военной области

b) Сведения о науке и технике

c) Сведения о разведке, контрразведке

d) Сведения о ЧП, катастрофах

e) Сведения о зарплате высших должностных лиц

2. Укажите регуляторов в области защиты персональных данных?

a) Роскомнадзор

b) ФСТЭК

c) ФСБ

d) ГТК

3. Сколько грифов секретности обычно присваивают конфиденциальной информации?

a) 2

b) 1

c) 3

d) 4

4. Кто наделен полномочиями изменения перечня сведений, относящихся к гостайне, в учреждениях и организациях?

a) ФСБ

b) ФСТЭК

c) Межведомственная комиссия

d) руководители организаций/учреждений

5. Какие сведения не относится к коммерческой тайне?

a) Сведения о структуре и масштабах производства

b) О внутренних и зарубежных заказчиках

c) О методах защиты товарных знаков

d) О графике работы

6. Через сколько лет требуется переоформление допуска к гос.тайне по 1-й и 2-й форме соответственно при переходе граждан на другое место работы?

a) 3 и 5

b) 5 и 10

c) 10 и 15

d) 15 и 20

7. Сколько уровней правового обеспечения можно выделить?

a) Первый, второй, третий, четвертый

b) Первый, второй, третий

c) Секретные, совершенно секретные, конфиденциальные

d) Общедоступные, секретные

8. Регуляторами в области защиты персональных данных являются:

a) Роскомнадзор

b) ФСБ

c) ФСТЭК

d) Межведомственная комиссия

9. Методы защиты информации:

a) Правовые

b) Организационные

c) Программно-технические

d) Все ответы верны

10. По каким критериям(согласно стандартам) оценивается надежность систем?

a) Политика безопасности

b) Безопасность повторного использования

c) Подотчетность

d) Гарантированность

11. В соответствии с законом о гос.тайне срок засекречивания не должен превышать (кроме отдельных случаев)?

a) 50 лет

b) 20 лет

c) 30 лет

d) 10 лет

12. Какая из льгот не относится к льготам допущенных к гос.тайне?

a) Льгота на предоставление медицинского обслуживания

b) Надбавка к зарплате

c) Процентная надбавка за стаж

13. Какие понятия включает в себя информационная безопасность?

a) Целостность, достоверность, конфиденциальность

b) Целостность, доступность, ,конфиденциальность

c) Целостность, достоверность, комплексность

d) Целостность, доступность, комплексность

14. С чем связано появление стандартов ИБ?

a) Создание первой ЭВМ

b) Учреждение АНБ США

c) Внедрения информационных технологий в промышленность

d) Появление интернета

e) Теракт 11 сентября 2001г.

15. Что нельзя отнести к коммерческой тайне?

a) Зарплаты сотрудников коммерческой организации

b) Используемые технологии промышленного производства

c) Влияние деятельности организации на окружающую среду

d) Используемые в организации ТСО (технические средства охраны)

16. Документы, требующие при поездке в командировку и доступе к гос.тайне:

a) Документ, удостоверяющий личность

b) Справка о допуске

c) Пропуск на производство

d) Предписание

17. Ответственное лицо за организацию доступа к гос.тайне персонала:

a) Руководитель

b) Отдел кадров

c) Первый отдел

d) Секретарь

18. Имея определенный уровень доступа, лицо может получать непосредственный доступ к информации и/или ее носителем. Или нужен приказ руководителя?

a) Да

b) Нет

c) Необязательно, но может и быть

19. К методам защиты от несанкционированного доступа относятся:

a) Разграничение доступа

b) Увеличение доступа

c) Минимизация привилегий

d) Аутентификация и идентификация

20. Назовите гриф секретности, который не используется в режиме гос.тайны:

a) Секретно

b) Совершенно секретно

c) Для служебного пользования

d) Особой важности

21. Какие ограничения накладываются на гражданина, допущенного к гос. тайне

a) В праве на выезд за границу

b) В праве на вступление в брак с гражданином иностранного государства

c) В праве на переписку с гражданами иностранных государств

d) В праве на неприкосновенность частной жизни

22. Перечень должностей, при назначении на которые граждане, обязаны получить допуск к гос. тайне, определяется:

a) Руководителем предприятия

b) Межведомственной комиссией

c) Номенклатурой должностей

d) ФСБ

23. Номенклатура должностей, для которых требуется оформление допуска к гос. тайне :

a) Разрабатывается предприятием, согласовывается с ФСБ

b) Разрабатывается предприятием, утверждается руководителем

c) Разрабатывается предприятием, утверждается межведомственной комиссией

d) Разрабатывается предприятием, утверждается Правительством РФ

24. Для гос. тайны существует три формы допуска. Какая из форм является наивысшей?

a) первая;

b) вторая;

c) третья.

25. Каково полное название федерального закона ФЗ №149 от 2006г.?

a) "Об информации";

b) "Об информации, информационных технологиях и защите информации";

c) "О новых направлениях в защите информации"

d) "Современные технологии защиты информационных технологий"

Критерии и шкала оценивания по оценочному средству «тесты»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Тесты выполнены на высоком уровне (правильные ответы даны на 90-100% тестов)
4	Тесты выполнены на среднем уровне (правильные ответы даны на 75-89% тестов)
3	Тесты выполнены на низком уровне (правильные ответы даны на 50-74% тестов)
2	Тесты выполнены на неудовлетворительном уровне (правильные ответы даны менее чем на 50% тестов)

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)