МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Институт Гражданской защиты
Кафедра Прокурорско-следственной деятельности

УТВЕРЖДАЮ:
Директор _____ Малкин В.Ю.
(подпись)
«30» 04 2023 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (модуля)

По дисциплине Правовое обеспечение информационной безопасности
(название дисциплины по учебному плану)

По специальности 40.05.01 Правовое обеспечение национальной безопасности

Специализация Государственно-правовая

Луганск 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины "Правовое обеспечение информационной безопасности", по специальности 40.05.01 "Правовое обеспечение национальной безопасности", специализация "Государственно-правовая", программа "Правовое обеспечение информационной безопасности" - 34 с.

Рабочая программа учебной дисциплины "Правовое обеспечение информационной безопасности" разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 40.05.01 Правовое обеспечение национальной безопасности (утвержденный приказом Министерства образования и науки Российской Федерации от 31 августа 2020 г. № 1138.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

к.ю.н., доцент, кафедры прокурорско-следственной деятельности Машуков Р.А.

(ученая степень, ученое звание, должность фамилия, инициалы)

Рабочая программа дисциплины утверждена на заседании кафедры Прокурорско-следственной деятельности «6» апреля 2023 г., протокол № 10

(название кафедры)

Заведующий кафедрой _____Машуков Р.А.

СОГЛАСОВАНО *(для потоковых дисциплин):*

Директор_____Малкин В.Ю.

Рекомендована на заседании учебно-методической комиссии института «20» апреля 2023 г., протокол № 8

Председатель учебно-методической комиссии института _____ Михайлов Д. В.

1. Цели и задачи дисциплины освоения дисциплины (модуля)

Цель изучения дисциплины – освоения учебной дисциплины «Правовое обеспечение информационной безопасности» является формирование у студентов знаний по основам правового обеспечения информационной безопасности государства и личности, основами организации информационной безопасности в органах прокуратуры Российской Федерации и работы со сведениями, отнесенными к государственной и иной охраняемой законом тайне.

Задачи:

–ознакомление с важнейшими принципами правового регулирования, определяющими содержание норм антикоррупционного законодательства;

–характеристика и анализ основных правовых мер системы борьбы с коррупционными проявлениями;

–понимание основных форм социально-политического насилия;

–знание содержания основных документов и нормативно-правовых актов противодействия терроризму в Российской Федерации, а также приоритетных задач государства в борьбе с терроризмом;

–создание представления о процессе ведения «информационных» войн и влиянии этого процесса на дестабилизацию социально-политической и экономической обстановки в регионах Российской Федерации;

–воспитание уважительного отношения к различным этнокультурам и религиям;

–знание основных рисков и угроз национальной безопасности России.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина «Правовое обеспечение информационной безопасности» входит часть, формируемую участниками образовательных отношений дисциплин учебного плана.

Необходимыми условиями для освоения дисциплины являются: знания, полученные в ходе изучения обеспечения информационной безопасности, а также изучение этой дисциплины. Знать: содержание основных понятий по правовому обеспечению информационной безопасности; понятие и виды защищаемой информации; правовые способы защиты информации ограниченного доступа и интеллектуальной собственности; уметь: находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью справочно-правовых систем; применять действующую законодательную базу в области информационной безопасности; владеть: навыками находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью справочно-правовых систем; навыками применять действующую законодательную базу в области информационной безопасности.

Содержание дисциплины является логическим продолжением содержания дисциплин, следующего уровня образования-магистратура: национальные банковские системы и обеспечение безопасности банковской деятельности.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
ОПК-9. Способен принимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ОПК-9.1 Способен оперировать основными общеправовыми понятиями и категориями, анализировать и толковать нормы права, давать юридическую оценку фактам и обстоятельствам.	**знать:** основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; **уметь:** применять действующую законодательную базу в области обеспечения информационной безопасности; **владеть:** навыками работы с нормативными правовыми актами.

4. Структура и содержание дисциплины (модуля)

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)	**144 (4 зач. ед)**	-	**144 (4 зач. ед)**
Обязательная контактная работа (всего) в том числе:	**48**	**-**	**8**
Лекции	24	-	4
Семинарские занятия	24	-	4
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)	**90**	**-**	**132**
Форма аттестации	зачет		зачет

4.2. Содержание разделов дисциплины

В разделе приводится полный перечень дидактических единиц, подлежащих усвоению при изучении данной дисциплины, структурированный по разделам дисциплины. Рекомендуется нумеровать каждую дидактическую единицу.

Семестр 8

Тема 1. Теоретические основы информационной безопасности

Понятие, предмет и назначение учебной дисциплины «Правовые основы информационной безопасности»

Информация как объект правового регулирования.

Нормативно-правовые акты, регулирующие общественные отношения в сфере информационной безопасности.

Понятие информационной безопасности.

Национальные интересы в информационной сфере.

Виды угроз информационной безопасности Российской Федерации.

Стратегические цели и основные направления обеспечения информационной безопасности

Тема 2. Правовое регулирование общественных отношений в сфере информации, информационных технологий и защиты информации

Понятие, структура и виды общественных отношений в информационной сфере.

Законодательство Российской Федерации об информации, информационных технологиях и о защите информации

Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Конституционные права граждан в сфере информации.

Право на доступ к информации

Общедоступная информация, информация ограниченного доступа. Государственная тайна. Персональные данные.

Правовой статус государственных информационных систем

Информационные ресурсы

Тема 3. Противодействие информационным угрозам

Понятие, признаки и исторические аспекты информационных войн.

Информационная безопасность личности.

Основы информационной гигиены личности.

Проверка информации на достоверность (фактчекинг).

Основы государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей

Субъекты и объекты правоотношений в области защиты от информации.

Виды информации, распространение которой запрещено или ограничено.

Стратегия противодействия экстремизму в Российской Федерации до 2025 года

Защита информации.

Полномочия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Федеральный государственный контроль (надзор) за соблюдением требований в связи с распространением информации в информационно-телекоммуникационных сетях, в том числе сети "Интернет".

Информация, причиняющая вред здоровью и (или) развитию детей.

Информационная продукция для детей разного возраста (не достигших возраста шести лет; достигших возраста шести, двенадцати и шестнадцати лет).

Контроль за деятельностью лиц, находящихся под иностранным влиянием

Тема 4. Государственная политика Российской Федерации в области международной информационной безопасности

Государственная политика Российской Федерации в области международной информационной безопасности.

Сущность международной информационной безопасности и основные угрозы международной информационной безопасности

Цель и задачи государственной политики Российской Федерации в области международной информационной безопасности

Основные направления реализации государственной политики в области международной информационной безопасности

Механизмы реализации государственной политики в области международной информационной безопасности

Международное законодательство в сфере информационной безопасности.

Законодательство зарубежных стран, регулирующее правоотношения в сфере информационной безопасности.

Тема 5. Полномочия прокурора в сфере ограничения доступа к информации, распространяемой с нарушением закона и основные принципы организации информационной безопасности в органах прокуратуры.

Порядок ограничения доступа к информации, распространяемой с нарушением закона.

Полномочия органов прокуратуры Российской Федерации в сфере ограничения доступа к информации, распространяемой с нарушением закона.

Полномочия органов прокуратуры Российской Федерации по противодействию экстремизму в информационной сфере.

Информационная безопасность как один из базовых принципов цифровой трансформации органов прокуратуры Российской Федерации.

Основные принципы организации информационной безопасности в органах прокуратуры Российской Федерации.

Тема 6. Защита интеллектуальных прав и ответственность за правонарушения в сфере информации

Законодательство Российской Федерации об интеллектуальной собственности. Объекты и субъекты авторского права. Исключительные авторские права. Смежные права.

Ответственность за правонарушения в информационной сфере.

Общая характеристика и виды ответственности за правонарушения в информационной сфере.

Уголовная ответственность в информационной сфере.

Административная ответственность в информационной сфере.

Дисциплинарная ответственность в информационной сфере.

Материальная ответственность в информационной сфере.

Тема 7. Информационные системы и применение компьютерной техники в профессиональной деятельности

Основные понятия и определения. Классификация информационных систем. Классификация персональных компьютеров

Тема 8. Технические средства информационных технологий

Тема 9. Организация ремонтного обслуживания аппаратуры и средств защиты

Изъятие компьютерной техники и носителей информации. Инструкция изъятия компьютерной техники. Исследование компьютерной техники и носителей информации. Оформление результатов исследования.

Тема 10. Организация пропускного и внутри объектового режимов

Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима. Основные положения инструкции об организации пропускного

режима и работе бюро пропусков. Понятие пропуска. Понятие внутри объектового режима. Общие требования внутри объектового режима.
Тема 11. Допуск лиц и сотрудников к сведениям, составляющим государственную тайну и конфиденциальную информацию
Тема 12. Сертификация и аттестация по требованиям безопасности информации
Аттестация объектов информатизации по требованиям безопасности информации. Основные понятия в области аттестации по требованиям безопасности информации и их определения. Системы сертификации средств защиты информации по требованиям безопасности информации

4.3. Лекции

№ п/п	**Название темы**	**Объем часов**		
		Очная форма	**Очно-заочная форма**	**Заочная форма**
1.	Теоретические основы информационной безопасности	**2**	-	**2**
2.	Правовое регулирование общественных отношений в сфере информации, информационных технологий и защиты информации	**2**	-	**2**
3.	Противодействие информационным угрозам	2	-	-
4.	Государственная политика Российской Федерации в области международной информационной безопасности	**2**	-	-
5.	Полномочия прокурора в сфере ограничения доступа к информации, распространяемой с нарушением закона и основные принципы организации информационной безопасности в органах прокуратуры.	**2**	-	-
6.	Защита интеллектуальных прав и ответственность за правонарушения в сфере информации	**2**	-	-
7.	Информационные системы и применение компьютерной техники в профессиональной деятельности	**2**	-	-
8.	Технические средства информационных технологий	**2**	-	-
9.	Организация ремонтного обслуживания аппаратуры и средств защиты	**2**	-	-
10.	Организация пропускного и внутри объектового режимов	**2**	-	-
11.	Допуск лиц и сотрудников к сведениям, составляющим государственную тайну и конфиденциальную информацию	**2**	-	-
12.	Сертификация и аттестация по требованиям безопасности информации	**2**	-	
Итого:		**24**	**0**	**4**

4.4. Практические (семинарские) занятия

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1.	Теоретические основы информационной безопасности	**2**	-	**2**
2.	Правовое регулирование общественных отношений в сфере информации, информационных технологий и защиты информации	**2**	-	-
3.	Противодействие информационным угрозам	2	-	**2**
4.	Государственная политика Российской Федерации в области международной информационной безопасности	**2**	-	-
5.	Полномочия прокурора в сфере ограничения доступа к информации, распространяемой с нарушением закона и основные принципы организации информационной безопасности в органах прокуратуры.	**2**	-	-
6.	Защита интеллектуальных прав и ответственность за правонарушения в сфере информации	**2**	-	-
7.	Информационные системы и применение компьютерной техники в профессиональной деятельности	**2**	-	-
8.	Технические средства информационных технологий	**2**	-	-
9.	Организация ремонтного обслуживания аппаратуры и средств защиты	**2**	-	-
10.	Организация пропускного и внутри объектового режимов	**2**	-	-
11.	Допуск лиц и сотрудников к сведениям, составляющим государственную тайну и конфиденциальную информацию	**2**	-	-
12.	Сертификация и аттестация по требованиям безопасности информации	**2**	-	-
Итого:		**24**	-	**4**

4.5 Лабораторные работы

Не предусмотрено.

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Форма/вид СРС	Объем часов		
			Очная форма	Очно-заочная	Заочная форма

				форма	
1.	Теоретические основы информационной безопасности	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	8	-	20
2.	Правовое регулирование общественных отношений в сфере информации, информационных технологий и защиты информации	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	8	-	12
3.	Противодействие информационным угрозам	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	8	-	10
4.	Государственная политика Российской Федерации в области международной информационной безопасности	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	8	-	10
5.	Полномочия прокурора в сфере ограничения доступа к информации, распространяемой с нарушением закона и основные принципы организации информационной безопасности в органах прокуратуры.	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	8	-	10
6.	Защита интеллектуальных прав и ответственность за правонарушения в сфере информации	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	8	-	10
7.	Информационные системы и применение компьютерной техники в профессиональной деятельности	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	8		10

8.	Технические средства информационных технологий	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	8		10
9.	Организация ремонтного обслуживания аппаратуры и средств защиты	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	8		10
10.	Организация пропускного и внутри объектового режимов	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	8		10
11.	Допуск лиц и сотрудников к сведениям, составляющим государственную тайну и конфиденциальную информацию	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	8		10
12.	Сертификация и аттестация по требованиям безопасности информации	Изучение учебной литературы, подготовка глоссария по теме, реферата, доклада	2		10
13.	Курсовая работа		-	-	-
Итого:			**90**	**-**	**132**

4.7. Курсовые работы/проекты по дисциплине *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. Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления / А. Ю. Пучков, А. М. Соколов, С. С. Широков, Н. Н. Прокимнов // Прикладная информатика. - 2023. - Т. 18, № 2. - С. 85-102.
2. Баринова А. Как HR-у самостоятельно провести обучение по информационной безопасности: готовый конспект лекций по главным угрозам / А. Баринова // Директор по персоналу. - 2022. - № 5. - С. 40-45.
3. Белов А. С. Модернизация системы информационной безопасности = Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. - 2022. - № 4. - С. 76-80.
4. Белов А. С. Модернизация системы информационной безопасности = Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. - 2022. - № 4. - С. 76-80.
5. Белов А. С. Модернизация системы информационной безопасности = Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. - 2022. - № 4. - С. 76-80.
6. Белов А. С. Модернизация системы информационной безопасности = Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. - 2022. - № 4. - С. 76-80.

б) дополнительная литература

1. Голубев Г. Д. Обзор безопасности маломощных глобальных сетей: угрозы, проблемы и потенциальные решения / Г. Д. Голубев // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 5-11.

2. Горбунов Д. Д. Криптовалюта и блокчейн: перспективы развития с точки зрения информационной безопасности / Д. Д. Горбунов // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 11-17.

3. Догучаева С. М. Анализ современных проблем информационной безопасности в российских компаниях / С. М. Догучаева // Риск: ресурсы, информация, снабжение, конкуренция. - 2022. - № 2. - С. 65-68.

4. Долганов К. А. Технология блокчейн с точки зрения информационной безопасности / К. А. Долганов // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 14-17.

5. Ефремов Н. А. Процессы информатизации экономики и информационная безопасность / Н. А. Ефремов, Т. В. Мужжавлева // Экономика и предпринимательство. - 2023. - № 3. - С. 287-294.

6. Иванов А. А. Ключевые понятия системного подхода к адаптивному мониторингу информационной безопасности киберфизических систем / А. А. Иванов // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 17-20.

в) интернет ресурсы

1. Ивличева Н. А. Влияние отраслевых опросов на приоритеты в обеспечении безопасности информационных систем предприятий / П. С. Ивличев, Н. А. Ивличева // Экономика и предпринимательство. - 2022. - № 3. - С. 1029-1032.

2. Информационная безопасность современного предприятия = Information Security of Advanced Company: Password Protection: парольная защита / М. Ю. Иванов, М. В. Сыготина, М. Ю. Вахрушева, В. В. Надршин // Защита информации. Инсайд. - 2022. - № 6. - С. 62-66.

3. Камалов Б. Р. Программное обеспечение обнаружения "скрытых майнеров" в браузерной среде / Б. Р. Камалов, М. В. Тумбинская // Прикладная информатика. - 2023. - Т. 18, № 1. - С. 96-110.

4. Комплексная методика проведения расследования инцидента информационной безопасности = ComprehensiveMethodologyforConductinganInformationSecurityIncidentInvestigation / С. И. Смирнов, А. Н. Киселев, В. Д. Азерский [и др.] // Защита информации. Инсайд. - 2023. - № 2. - С. 14-26.

5. Коноплева Л. А. Гуманитарные аспекты информационной безопасности : учеб. пособие / Л. А. Коноплева ; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. - Екатеринбург : Изд-во Урал. гос. экон. ун-та, 2022. -162 с.

6. Красинский В. В. Кибертерроризм: криминологическая характеристика и квалификация = Cyberterrorism: criminological characteristics and qualification / В. В. Красинский, В. В. Машко // Государство и право. - 2023. - № 1. - С. 79-91.

д) методические указания для обучающихся по основанию дисциплины

1. Кузьмина О. В. Информационно-технологическая безопасность обучающихся / О. В. Кузьмина // BI-технологии и корпоративные информационные системы в оптимизации

бизнес-процессов цифровой экономики : материалы IX Междунар. науч. - практ. конф. (Екатеринбург, 2 дек. 2021 г.). - Екатеринбург, 2021. - С.134-136.

2. Курило А. Куда идти? Три первых шага / А. Курило // Bis journal. - 2022. - № 1. - С. 9-15.

3. Мансуров Г. З. Право цифровой безопасности : учебник / Г. З. Мансуров. – Москва : Директ-Медиа, 2022. – 148 с.

4. Марков А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей / А. С. Марков // Вопросы кибербезопасности. - 2022. - № 1. - С. 2-9.

5. Муратова М. Н. Информационная безопасность в области оценки недвижимости / М. Н. Муратова // Экономика и предпринимательство. - 2023. - № 1. - С. 1236-1239.

6. Назаров Д. М. Основы обеспечения безопасности персональных данных в организации : учеб. пособие / Д. М. Назаров, К. М. Саматов ; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. - Екатеринбург : Изд-во Урал. гос. экон. ун-та, 2019. -118 с.

7. Материально-техническое и программное обеспечение дисциплины (модуля)

Используется: специально оборудованные кабинеты и аудитории: компьютерные классы, аудитории, оборудованные мультимедийными средствами обучения, которые используются при изучении данной дисциплины. Вуз располагает материально-технической базой, обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, практической и научно-исследовательской работы обучающихся, которые предусмотрены учебным планом вуза и соответствующей действующим санитарным и противопожарным нормам и правилам.

При изучении дисциплины используются: а) учебный зал судебных заседаний; б) компьютерный класс для проведения тестирования. Вуз обеспечен необходимым комплектом лицензионного программного обеспечения. Самостоятельная работа обучающихся осуществляется в помещениях, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно - образовательную среду университета.

8. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации по дисциплине (модулю)

Паспорт
оценочных средств по учебной дисциплине
«Правовое обеспечение информационной безопасности»

Описание уровней сформированности и критериев оценивания компетенций на этапах их формирования в ходе изучения дисциплины

Этап	Код компетенции	Уровни сформированности компетенции	Критерии оценивания компетенции

Начальный	ОПК-9. Владеть основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информации.	**Пороговый**	**знать:** - в целом верно воспроизводит полученные знания, испытывает затруднения в комментировании. **уметь:** - способен при обсуждении предложенной проблемы соотнести ее с положениями изучаемых наук. Комментирует проблему, используя предложенные преподавателем понятия и термины **владеть:** - может с помощью педагога поставить задачу поиска информации; отобрать источники. Испытывает трудности в оценке источников. Может корректно использовать информацию.
Основной		**Базовый**	**знать:** - в целом верно воспроизводит полученные знания, верно комментирует их. **уметь:** - Способен обсуждать предложенную проблему, соотнести ее с положения ми изучаемых наук и прокомментировать, используя понятийно-терминологический аппарат науки **владеть:** - Может поставить задачу поиска информации; отобрать источники; с помощью педагога оценить их актуальность и достоверность, полноту и глубину рассмотрения вопроса, корректно использовать информацию.
Заключительный		**Высокий**	**знать:** -термины и понятия изучаемых дисциплин, ориентируется в основных методах, способах и средствах получения, хранения, переработки информации в соответствии с минимумом, определенным в рабочей программе дисциплины **уметь:** - соотносить актуальные вопросы профессиональной деятельности, проблемы профильных наук с положениями изучаемых дисциплин и комментировать эти проблемы, опираясь на понятийно-терминологический аппарат ИКТ. **владеть:** - навыком поиска, оценивания и использования информации по вопросам изучаемых дисциплин .

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

№ п/п	Код компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по дисциплине)	Темы учебной дисциплины	Этапы формирования (семестр изучения)
1	ОПК-9	Владеть основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информации.	ОПК-9.2. Владеет основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией ОПК-9.3. Владеет основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией	Тема 1. Тема 2. Тема 3. Тема 4. Тема 5. Тема 6. Тема 7. Тема 8. Тема 9. Тема 10. Тема 11. Тема 12.	Начальный Тема 1 Тема 2 Основной Тема 3 Тема 4 Заключительный Тема 5 Тема 6

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код компетенции	Индикаторы достижений компетенции	Планируемые результаты обучения по дисциплине	Контролируемые темы учебной дисциплины	Наименование оценочного средства
1.	ОПК-9. Владеть основными методами, способами и средствами получения,	ОПК-9.2. Владеет основными методами, способами и средствами	**знать: –** информацию об устройстве и назначении компьютера, о названиях,	Тема 1. Тема 2. Тема 3. Тема 4. Тема 5. Тема 6.	Доклад, задачи, тестовые задания,реферат

	хранения, переработки информации, навыками работы с компьютером как средством управления информации.	получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией	функциях и принципах работы его частей, устройств и приспособлений, о правилах информационной безопасности при работе в электронных средах. **уметь:** - пользоваться компьютером как средством управления информацией, выполнять необходимые действия по использованию компьютерной и демонстрационной техники, по обеспечению сохранности оборудования. **владеть:** навыком ИКТ на общепользовательс ком уровне.	Тема 7. Тема 8. Тема 9. Тема 10. Тема 11. Тема 12.	

(примерный перечень оценочных средств)

1. Тестовые задания

(пороговый уровень)

1. Наиболее важным при реализации защитных мер политики безопасности является:
А) Аудит, анализ затрат на проведение защитных мер
Б) Аудит, анализ безопасности
В) Аудит, анализ уязвимостей, риск-ситуаций

2. Политика безопасности в системе (сети) – это комплекс:
А) Руководств, требований обеспечения необходимого уровня безопасности
Б) Инструкций, алгоритмов поведения пользователя в сети
В) Нормы информационного права, соблюдаемые в сети

3. Окончательно, ответственность за защищенность данных в компьютерной сети несет:
А) Владелец сети
Б) Администратор сети

В) Пользователь сети

4. Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
А) Программные, технические, организационные, технологические
Б) Серверные, клиентские, спутниковые, наземные
В) Личные, корпоративные, социальные, национальные

5. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
А) Регламентированной
Б) Правовой
В) Защищаемой

6. Угроза информационной системе (компьютерной сети) – это:
А) Вероятное событие
Б) Детерминированное (всегда определенное) событие
В) Событие, происходящее периодически

7. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
А) Целостность
Б) Доступность
В) Актуальность

8. Утечкой информации в системе называется ситуация, характеризуемая:
А) Потерей данных в системе
Б) Изменением формы информации
В) Изменением содержания информации

9. Наиболее распространены средства воздействия на сеть офиса:
А) Слабый трафик, информационный обман, вирусы в интернет
Б) Вирусы в сети, логические мины (закладки), информационный перехват
В) Компьютерные сбои, изменение администрирования, топологии

10. Наиболее распространены угрозы информационной безопасности сети:
А) Распределенный доступ клиент, отказ оборудования
Б) Моральный износ сети, инсайдерство
В) Сбой (отказ) оборудования, нелегальное копирование данных

11. Наиболее распространены угрозы информационной безопасности корпоративной системы:
А) Покупка нелицензионного ПО
Б) Ошибки эксплуатации и неумышленного изменения режима работы системы
В) Сознательного внедрения сетевых вирусов

12. ЭЦП – это:
А) Электронно-цифровой преобразователь

Б) Электронно-цифровая подпись
В) Электронно-цифровой процессор

13. Принцип Кирхгофа:
А) Секретность ключа определена секретностью открытого сообщения
Б) Секретность информации определена скоростью передачи данных
В) Секретность закрытого сообщения определяется секретностью ключа

14. Когда получен спам по e-mail с приложенным файлом, следует:
А) Прочитать приложение, если оно не содержит ничего ценного – удалить
Б) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
В) Удалить письмо с приложением, не раскрывая (не читая) его

15. К основным типам средств воздействия на компьютерную сеть относится:
А) Компьютерный сбой
Б) Логические закладки («мины»)
В) Аварийное отключение питания

16. Принципом политики информационной безопасности является принцип:
А) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Б) Одноуровневой защиты сети, системы
В) Совместимых, однотипных программно-технических средств сети, системы

17. Принципом политики информационной безопасности является принцип:
А) Усиления защищенности самого незащищенного звена сети (системы)
Б) Перехода в безопасное состояние работы сети, системы
В) Полного доступа пользователей ко всем ресурсам сети, системы

18. Принципом политики информационной безопасности является принцип:
А) Невозможности миновать защитные средства сети (системы)
Б) Усиления основного звена сети, системы
В) Полного блокирования доступа при риск-ситуациях

19. Принципом информационной безопасности является принцип недопущения:
А) Неоправданных ограничений при работе в сети (системе)
Б) Рисков безопасности сети, системы
В) Презумпции секретности

20. К основным функциям системы безопасности можно отнести все перечисленное:
А) Установление регламента, аудит системы, выявление рисков
Б) Установка новых офисных приложений, смена хостинг-компании
В) Внедрение аутентификации, проверки контактных данных пользователей

Методические рекомендации:

при использовании формы текущего контроля «Тестирование» студентам могут предлагаться задания на бумажном носителе.

Критерии и шкала оценивания по оценочному средству «тестирование»

Шкала оценивания	Критерий оценивания

(интервал баллов)	
5	85 – 100% правильных ответов
4	71 – 85% правильных ответов
3	61 – 70% правильных ответов
2	60% правильных ответов и ниже

2. Вопросы для обсуждения (в виде докладов и сообщений)

(пороговый уровень)

1. Какие положения, связанные с вопросами обработки информации, закреплены в Конституции Российской Федерации?
2. Понятие, предмет и назначение учебной дисциплины «Правовые основы информационной безопасности»?
3. Информация как объект правового регулирования?
4. Нормативно-правовые акты, регулирующие общественные отношения в сфере информационной безопасности?
5. Понятие информационной безопасности?
6. Национальные интересы в информационной сфере?
7. Виды угроз информационной безопасности Российской Федерации?
8. Стратегические цели и основные направления обеспечения информационной безопасности?
9. Понятие и структура информационной безопасности в Российской Федерации?
10. Критическая инфраструктура Российской Федерации?
11. Понятие, структура и виды общественных отношений в информационной сфере?
12. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации?
13. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации?
14. Конституционные права граждан в сфере информации?
15. Право на доступ к информации?
16. Общедоступная информация, информация ограниченного доступа. Государственная тайна. Персональные данные?
17. Правовой статус государственных информационных систем?
18. Информационные ресурсы?
19. Понятие, признаки и исторические аспекты информационных войн?
20. Информационная безопасность личности?

Критерии и шкала оценивания по оценочному средству

«доклад, сообщение»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Доклад (сообщение) представлен(о) на высоком уровне (студент в полном объеме осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, владеет профильным понятийным (категориальным) аппаратом и т.п.)
4	Доклад (сообщение) представлен(о) на среднем уровне (студент в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности и т.п.)
3	Доклад (сообщение) представлен(о) на низком уровне (студент допустил существенные неточности, изложил материал с

	ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.)
2	Доклад (сообщение) представлен(о) на неудовлетворительном уровне или не представлен (студент не готов, не выполнил задание и т.п.)

3. Реферат

(базовый уровень)

1. Национальные интересы в информационной сфере
2. Виды угроз информационной безопасности Российской Федерации.
3. Стратегические цели и основные направления обеспечения информационной безопасности
4. Понятие и структура информационной безопасности в Российской Федерации.
5. Критическая инфраструктура Российской Федерации.
6. Конституционные права граждан в сфере информации.
7. Основы информационной гигиены личности.
8. Проверка информации на достоверность (фактчекинг).
9. Основы государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей
10. Федеральный государственный контроль (надзор) за соблюдением требований в связи с распространением информации в информационно-телекоммуникационных сетях, в том числе сети "Интернет".
11. Контроль за деятельностью лиц, находящихся под иностранным влиянием
12. Государственная политика Российской Федерации в области международной информационной безопасности.
13. Законодательство зарубежных стран, регулирующее правоотношения в сфере информационной безопасности.
14. Полномочия органов прокуратуры Российской Федерации в сфере ограничения доступа к информации, распространяемой с нарушением закона
15. Полномочия органов прокуратуры Российской Федерации по противодействию экстремизму в информационной сфере.
16. Информационная безопасность как один из базовых принципов цифровой трансформации органов прокуратуры Российской Федерации.
17. Ответственность за правонарушения в информационной сфере.

Ограничение прав субъектов, связанное с государственной тайной.

18. Перечень сведений, составляющих государственную тайну. Сведения, которые не могут относиться к государственной тайне.
19. Контроль и надзор за обеспечением защиты государственной тайны.
20. Правовое регулирование информационных отношений в области коммерческой тайны.
21. Защита прав на коммерческую тайну.
22. Особенности информационных правоотношений, возникающих при производстве, передаче и распространении персональных данных.
23. Правовые основания работы с персональными данными.
24. Персональные данные как особый институт охраны прав на неприкосновенность частной жизни.
25. Объекты и субъекты права на неприкосновенность частной жизни.
26. Ограничения информационной сферы налогового контроля.

27. Обеспечение права на информацию налогоплательщика.
28. Понятие налоговой тайны и ее правовое регулирование.
29. Виды юридической ответственности за нарушение информационно-правовых норм в сфере налогового контроля.
30. Информационно-правовые основы организации и методики современного налогового контроля.
31. Применение информационных технологий при проведении налоговых проверок.
32. Правонарушения в сфере информации при проведения мероприятий налогового контроля.

Критерии и шкала оценивания по оценочному средству «реферат»

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

4. Задачи

(высокий уровень)

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 опубликована и стала общедоступной, и научным руководством 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?
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 23 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?

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?

Критерии и шкала оценивания по оценочному средству
«задачи»

Шкала оценивания (интервал баллов)	Критерии оценивания
5	Обучающийся полностью и правильно выполнил задание. Показал отличные знания, умения и владения навыками, применения их при решении задач в рамках усвоенного учебного материала. Работа оформлена аккуратно в соответствии с предъявляемыми требованиями
4	Обучающийся выполнил задание с небольшими неточностями. Показал хорошие знания, умения и владения навыками, применения их при решении задач в рамках освоенного учебного материала. Есть недостатки в оформлении работы
3	Обучающийся выполнил задание с существенными неточностями. Показал удовлетворительные знания, умения и владения навыками, применения их при решении задач
2	Обучающийся выполнил задание неправильно. При выполнении обучающийся продемонстрировал недостаточный уровень знаний, умений и владения ими при решении задач в рамках усвоенного учебного материала

5. Разноуровневые задачи и задания

(пороговый уровень)

Задание №1. Информация- это…

1) Сведения, поступающие от СМИ

2) Только документированные сведения о лицах, предметах, фактах, событиях

3) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

4) Только сведения, содержащиеся в электронных базах данных

Ответ: 3

Задание №2. Соотнесите в верной последовательности

А)Информация, зафиксированная, позволяющая ее идентифицировать	1)С ограниченным доступом

Б)Доступность информации классифицируется	2)Защита
В)Документы содержащие конфиденциальность	3)Документированной
Г)Комплекс мероприятий, направленные на обеспечение информационной безопасности	4)Государственная тайна

Ответ: А3, Б1, В4, Б2

Задание №3. По доступности информация классифицируется на

А) Открытую информацию и государственную тайну

Б) Конфиденциальную информацию и информацию свободного доступа

В) Информацию с ограниченным доступом и общедоступную информацию

Г) Виды информации, указанные в остальных пунктах

Ответ: В

Задание №4. Сопоставьте

1. Закон «О коммерческой тайне»
2. Конфиденциальность
3. Источник угрозы
4. Побочное влияние

А) Потенциальный злоумышленник

Б) Негативное воздействие на систему в целом или отдельные элементы

В) Зашита от несанкционированного доступа к информации

Г) Акт содержащий сведения по защите коммерческой тайны

Ответ: 1Г, 2В, 3А, 4Б

Задание №5. Доступность- это…

А) Возможность за приемлемое время получить требуемую информационную услугу

Б) Логическая независимость

В) Нет правильного ответа

Ответ: А

Задание №6. Сопоставьте

1. Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу
2. Как принято классифицировать информацию в зависимости от категории доступа согласно российскому законодательству
3. Возможность получения информации и ее использования
4. Контрольные мероприятия без взаимодействия с контролируемым лицом

А) Ограниченного доступа и общедоступная

Б) Доступ информации

В) Выездное обследование

Г) Персональные данные

Ответ: 1Г, 2А, 3Б, 4В

7. Обеспечение информационной безопасности есть обеспечение…

А) Независимости информации

Б) Изменения информации

В) Копирования информации

Г) Сохранности информации
Д) Преобразования информации

8. Федеральный закон "Об информации, информации и защите информации" дает определение информации:
А) Текст книги или письма
Б) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
В) Сведения о явлениях и процессах
Г) Факты и идеи в формализованном виде
Д) Шифрованный текст, текст на неизвестном языке

9. Для защиты от злоумышленников необходимо использовать:
А) Системное программное обеспечение
Б) Прикладное программное обеспечение
В) Антивирусные программы
Г) Компьютерные игры
Д) Музыку, видеофильмы

10. Электронные Замки «СОБОЛЬ» предназначены для …
А) Обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах
Б) Сканирования отпечатков пальцев
В) Проверки скорости и загрузки файлов
Г) Общего контроля
Д) Идентификации пользователя

11. Аппаратные модули доверенной загрузки «АККОРД - АМДЗ» представляют собой…
А) Аппаратный контролер
Б) Электронный замок
В) Система контроля
Г) Сетевой адаптер
Д) Копировальный аппарат

12. Доступ пользователя к информационным ресурсам компьютера и локальной вычислительной сети предприятия должен разрешаться только после:
А) Включения компьютера
Б) Идентификации по логину и паролю
В) Запроса паспортных данных
Г) Запроса доменного имени
Д) Запроса ФИО

13. Доступ к информации – это:
А) Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

Б) Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
В) Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
Г) Информация, переданная или полученная пользователем информационно-телекоммуникационной сети
Д) Возможность получения информации и ее использования

14. Персональными данными владеют:
А) Государство
Б) Различные учреждения
В) Государственная Дума
Г) Жители Российской Федерации
Д) Медико-социальные организации

15. Информацией, составляющей коммерческую тайну, владеют:
А) Государство
Б) Различные учреждения
В) Государственная Дума
Г) Граждане Российской Федерации
Д) Медико-социальные организации

16. Информацией, составляющей государственную тайну, владеют:
А) Государство
Б) Только образовательные учреждения
В) Только президиум Верховного Совета РФ
Г) Граждане Российской Федерации
Д) Только министерство здравоохранения

Критерии и шкала оценивания по оценочному средству
«разноуровневые задания и задачи»

Шкала оценивания (интервал баллов)	Критерии оценивания
5	Обучающийся полностью и правильно выполнил задание. Показал отличные знания, умения и владения навыками, применения их при решении задач в рамках усвоенного учебного материала. Работа оформлена аккуратно в соответствии с предъявляемыми требованиями
4	Обучающийся выполнил задание с небольшими неточностями. Показал хорошие знания, умения и владения навыками, применения их при решении задач в рамках освоенного учебного материала. Есть недостатки в оформлении работы
3	Обучающийся выполнил задание с существенными неточностями. Показал удовлетворительные знания, умения и владения навыками, применения их при решении задач
2	Обучающийся выполнил задание неправильно. При выполнении обучающийся продемонстрировал недостаточный уровень знаний, умений и владения ими при решении задач в рамках усвоенного учебного материала

6. Практическое (прикладное) задание

(высокий уровень)

Задание № 1. Владелец информационных ресурсов не обязан …

А) бесплатно опубликовывать библиографическую информацию

Б) хранить производственные документы

В) использовать информацию по своему усмотрению

Г) включать библиографическую информацию в международные автоматизированные банки данных

Ответ: В

Задание № 2. Дети до 6 лет не вправе…

А) с согласия законных представителей пользоваться телефонными услугами

Б) с разрешения законных представителей выходить в Интернет

В) с согласия законных представителей совершать сделки с компьютерной техникой

Ответ: В

Задание № 3. Основное средство антивирусной защиты

А) резервное копирование ценных данных

Б) регулярное сканирование жестких дисков

В) подготовка квалифицированных кадров в сфере информационной безопасности

Ответ: А

Задание № 4. Федеральный закон «О персональных данных» от 27 июля 2006 г. не регулирует отношения, возникающие при…

А) обработке персональных данных физическими лицами исключительно для личных и семейных нужд

Б) хранении, комплектовании, учете и использовании архивных документов

В) включении в Единый государственный реестр индивидуальных предпринимателей

Г) обработке персональных данных, отнесенных к государственной тайне

Д) обработке персональных данных, отнесенных к служебной тайне

Ответ: Д

Задание № 5. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений…

А) о размере и составе имущества некоммерческих организаций

Б) об оплате труда работников некоммерческих организаций

В) об использовании безвозмездного труда граждан в деятельности некоммерческой организации

Г) об использовании новых технологий, позволяющих получить коммерческую выгоду

Ответ: Г

Задание № 6. Признак, не относящийся к охраноспособной информации – это …:

А) охране подлежит только документированная информация

Б) доступ к охраноспособной информации ограничен только законом

В) доступ к охраноспособной информации ограничен владельцем информационных ресурсов

Г) защита охраноспособной информации устанавливается Законом

Ответ: В

Критерии и шкала оценивания по оценочному средству

«практическое задание»

Шкала оценивания	Критерий оценивания

(интервал баллов)	
5	Практические задания выполнены на высоком уровне (правильные ответы даны на 90 – 100% вопросов/задач)
4	Практические задания выполнены на среднем уровне (правильные ответы даны на 75 – 89% вопросов/задач)
3	Практические задания выполнены на низком уровне (правильные ответы даны на 50 – 74% вопросов/задач)
2	Практические задания выполнены на неудовлетворительном уровне (правильные ответы даны менее чем на 50%)

7. Комплект заданий для контрольной работы

1. Владельцем информации третьей категории является…
А) Люди
Б) Государство
В) Муниципальное учреждение
Г) Учреждение
Д) Некоммерческая организация

2. Владельцем информации второй категории является…
А) Простые люди
Б) Государство
В) Коммерческая организация
Г) Муниципальное учреждение
Д) Некоммерческая организация

3. Владельцем информации первой категории является…
А) Государство
Б) Коммерческая организация
В) Муниципальное учреждение
Г) Любой гражданин
Д) Группа лиц, имеющих общее дело

4. Хищение информации – это…
А) Несанкционированное копирование информации
Б) Утрата информации
В) Блокирование информации
Г) Искажение информации
Д) Продажа информаци

5. Федеральный Закон «Об информации, информатизации и защите информации» направлен на:
А) Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ
Б) Регулирование взаимоотношений в гражданском обществе РФ
В) Регулирование требований к работникам служб, работающих с информаций
Г) Формирование необходимых норм и правил работы с информацией

Д) Формирование необходимых норм и правил, связанных с защитой детей от информации

6. Информация об Уголовной ответственности за преступление в сфере компьютерной информации описана в:
А) 1 главе Уголовного кодекса
Б) 5 главе Уголовного кодекса
В) 28 главе Уголовного кодекса
Г) 100 главе Уголовного кодекса
Д) 1000 главе Уголовного кодекса

7. Документированной информацией, доступ к которой ограничен в соответствии с законодательством РФ, называется
А) Конфиденциальная
Б) Персональная
В) Документированная
Г) Информация, составляющая государственную тайну
Д) Информация, составляющая коммерческую тайну

8. Информационная безопасность обеспечивает…
А) Блокирование информации
Б) Искажение информации
В) Сохранность информации
Г) Утрату информации
Д) Подделку информации

9. Для того чтобы снизить вероятность утраты информации необходимо:
А) Регулярно производить антивирусную проверку компьютера
Б) Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
В) Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)
Г) Защитить вход на компьютер к данным паролем
Д) Проводить периодическое обслуживание ПК

10. Документированная информация, доступ к которой ограничивает в соответствии с законодательством РФ:
А) Информация, составляющая государственную тайну
Б) Информация, составляющая коммерческую тайну
В) Персональная
Г) Конфиденциальная информация
Д) Документированная информация

11. Наиболее опасным источником угроз информационной безопасности предприятия являются:
А) Другие предприятия (конкуренты)
Б) Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
В) Рядовые сотрудники предприятия

Г) Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
Д) Хакеры

12. Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу это:
А) Идентификация
Б) Аутентификация
В) Стратификация
Г) Регистрация
Д) Авторизация

13. В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности:
А) Выход в Интернет без разрешения администратора
Б) При установке компьютерных игр
В) В случаях установки нелицензионного ПО
Г) В случае не выхода из информационной системы
Д) В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственност

14. «ПЕРСОНАЛЬНЫЕ ДАННЫЕ» это:
А) Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
Б) Фамилия, имя, отчество физического лица
В) Год, месяц, дата и место рождения, адрес физического лица
Г) Адрес проживания физического лица
Д) Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

15. Несанкционированный доступ к информации это:
А) Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
Б) Работа на чужом компьютере без разрешения его владельца
В) Вход на компьютер с использованием данных другого пользователя
Г) Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
Д) Доступ к СУБД под запрещенным именем пользователя

16. За правонарушение в сфере информации, информационных технологий и защиты информации данный вид наказания на сегодняшний день не предусмотрен:
А) Дисциплинарные взыскания
Б) Административный штраф
В) Уголовная ответственность
Г) Лишение свободы
Д) Смертная казнь

17. Для безопасной передачи данных по каналам интернет используется технология:
1. WWW

2. DICOM
3. VPN
4. FTP
5. XML

18. Основное средство, обеспечивающие конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:
А) Идентификация
Б) Аутентификация
В) Авторизация
Г) Экспертиза
Д) Шифрование

19. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название:
А) Токен
Б) Password
В) Пароль
Г) Login
Д) Смарт-карта

20. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на:
А) Многопользовательские
Б) Однопользовательские
В) Без разграничения прав доступа
Г) С разграничением прав доступа
Д) Системы, не имеющие подключений

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%)

8. Оценочные средства для промежуточной аттестации (зачет)

Задания для оценки порогового уровня:
1. Понятие субъекта информационной безопасности и объекты защиты.
2. Виды субъектов информационной безопасности.
3. Российская Федерация как субъект информационной безопасности.

4. Субъекты РФ и муниципальные образования как субъекты информационной безопасности.
5. Граждане и другие физические лица как субъекты информационной безопасности.
6. Несовершеннолетние как субъекты информационной безопасности.
7. Правовой статус общественных объединений и коммерческих организаций как субъектов информационной безопасности.
8. Система и полномочия органов государственной власти, обеспечивающих право доступа к информации.
9. Система и компетенция органов, обеспечивающих охрану государственной тайны.
10. Компетенция органов государственной власти по обеспечению правового режима конфиденциальной информации.
11. Понятие и виды конфиденциальной информации.
12. Режимы защиты информации.
13. Государственная тайна как предмет, изъятый из гражданского оборота.
14. Служебная и профессиональная тайна
15. Коммерческая и банковская тайны
16. Понятие и структура персональных данных
17. Понятие и виды информационных технологий.
18. Порядок создания информационных технологий.
19. Нарушения порядка применения информационных технологий: информационные войны, несанкционированный мониторинг за активностью потребителя информации.
20. Прокурорско-следственная деятельность по обеспечению информационной безопасности
21. Прокурорско-следственная деятельность по обеспечению информационной безопасности личности.
22. Соблюдение конституционных прав и свобод человека и гражданина в области информационных правоотношений.
23. Ограничения использования информации о частной жизни.
24. Гарантии информационных прав граждан. Право на судебную защиту.
25. Правовые и этические пределы вмешательства в личную жизнь при использовании интерактивных методов работы с аудиторией.
26. Понятие безопасности в глобальном информационном пространстве.
27. Информационное обеспечение государственной политики Российской Федерации.
28. Прокурорско-следственная деятельность по обеспечению информационной безопасности общества.
29. Прокурорско-следственная деятельность по обеспечению информационной безопасности государства.
30. Обеспечение защиты информационных ресурсов от несанкционированного доступа.
31. Прокурорско-следственная деятельность по обеспечению информационной безопасности информационных и телекоммуникационных систем.
32. Общая характеристика и виды ответственности за правонарушения в сфере информационной безопасности.
33. Дисциплинарная ответственность в сфере информационной безопасности.
34. Административная ответственность в сфере информационной безопасности.
35. Уголовная ответственность в сфере информационной безопасности.
36. Материальная ответственность в сфере информационной безопасности.

Критерии и шкала оценивания к промежуточной аттестации
«зачет»

Характеристика знания предмета и ответов	Зачеты
Студент глубоко и в полном объѐме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач	зачтено
Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач	
Студент знает только основной программный материал, допускает неточности, недостаточно чѐткие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах	
Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы	не зачтено

9. Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости рабочая программа учебной дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе с применением электронного обучения и дистанционных образовательных технологий.

Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК). В случае необходимости обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося), а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей:

– создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

– создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

– создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников, например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения – аудиально;

– применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной (модулем), за счѐт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

– применение электронного обучения, дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

– применение электронного обучения, дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

– увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

– продолжительность сдачи зачѐта или экзамена, проводимого в письменной форме, – не более чем на 90 минут;

– продолжительность подготовки обучающегося к ответу на зачѐте или экзамене, проводимом в устной форме, – не более чем на 20 минут;

– продолжительность выступления обучающегося при защите курсовой работы – не более чем на 15 минут.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений с указанием страниц	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)
1.			
2.			
3.			
4.			

Приложение 2

Лист дополнений к рабочей программе

УТВЕРЖДАЮ
Зав. кафедрой _____
_____И.О. Фамилия
«_____»_____202__г.

Список литературы к рабочей программе дисциплины
_____направление подготовки/специальность
_____по состоянию на «_____»_____20____г.

Основная литература:

1.
2.
3.

Дополнительная литература:

1.
2.
3.

Преподаватель _____
(подпись) (И.О.Ф.)