МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
имени И.Т. ТРУБИЛИНА»

Юридический факультет
Криминалистики

КубГАУ Кубанский государственный аграрный университет
Документ подписан простой электронной подписью
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 2a0000098add596f008935c40900020000098a
Владелец: Куемжиева Светлана Александровна
Действителен от 23-05-2021 до 22-05-2026

УТВЕРЖДЕНО
Декан
Куемжиева С.А.
Протокол от 19.05.2025 № 8

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ»

Уровень высшего образования: магистратура

Направление подготовки: 40.04.01 Юриспруденция

Направленность (профиль)подготовки: Юридическая деятельность в сфере земельно-имущественных отношений и агробизнеса

Квалификация (степень) выпускника: магистр

Формы обучения: очная, очно-заочная

Год набора (приема на обучение): 2025

Срок получения образования: Очная форма обучения – 2 года
Очно-заочная форма обучения – 3 года

Объем: в зачетных единицах: 2 з.е.
в академических часах: 72 ак.ч.

2025

Разработчики:
Доцент, кафедра криминалистики Агеев Н.В.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлени ю подготовки 40.04.01 Юриспруденция, утвержденного приказом Минобрнауки от 25.11.2020 № 1451, с учетом трудовых функций профессиональных стандартов: "Специалист в сфере предупреждения коррупционных правонарушений", утвержден приказом Минтруда России от 08.08.2022 № 472н; "Специалист по конкурентному праву", утвержден приказом Минтруда России от 16.09.2021 № 637н; "Специалист по определению кадастровой стоимости", утвержден приказом Минтруда России от 02.09.2020 № 562н; "Следователь-криминалист", утвержден приказом Минтруда России от 23.03.2015 № 183н; "Эксперт в сфере закупок", утвержден приказом Минтруда России от 10.09.2015 № 626н; "Специалист в сфере управления проектами государственно-частного партнерства", утвержден приказом Минтруда России от 20.07.2020 № 431н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Юридический факультет	Председатель методической комиссии/совета	Сапфирова А.А.	Согласовано	19.05.2025, № 8
2		Руководитель образовательной программы	Глушко О.А.	Согласовано	19.05.2025, № 8

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - является формирование комплекса знаний, умений и навыков, необходимых для осуществления юридической деятельности с учетом использования информационно-коммуникационных технологий и требований информационной безопасности.

Задачи изучения дисциплины:

- - формирование способности применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ОПК-7 Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности

ОПК-7.1 Применяет информационные технологии для решения задач профессиональной деятельности

Знать:

ОПК-7.1/Зн1 Применяет информационные технологии для решения задач профессиональной деятельности

ОПК-7.2 Использует правовые базы данных для решения задач профессиональной деятельности

Знать:

ОПК-7.2/Зн1 Использует правовые базы данных для решения задач профессиональной деятельности

ОПК-7.3 Учитывает требования информационной безопасности при применении информационных технологий и использовании правовых баз данных

Знать:

ОПК-7.3/Зн1 Учитывает требования информационной безопасности при применении информационных технологий и использовании правовых баз данных

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности» относится к обязательной части образовательной программы и изучается в семестре(ах): Очная форма обучения - 2, Очно-заочная форма обучения - 2.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Очная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Внеаудиторная контактная работа (часы)	Зачет (часы)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Второй семестр	72	2	19	1		4	14	53	Зачет
Всего	72	2	19	1		4	14	53	

Очно-заочная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Внеаудиторная контактная работа (часы)	Зачет (часы)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Второй семестр	72	2	15	1	4	4	6	57	Зачет (4) Контрольная работа
Всего	72	2	15	1	4	4	6	57	

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Очная форма обучения

Наименование раздела, темы	Всего	Внеаудиторная контактная работа	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Правовые базы данных и цифровые технологии в юридической практике	**43**		**2**	**10**	**31**	ОПК-7.1 ОПК-7.2 ОПК-7.3
Тема 1.1. Информационное общество и информатизация.	12			4	8	

Тема 1.2. Информационно-коммуникационные технологии.	18		2	4	12	
Тема 1.3. Компьютерные системы обмена информацией в профессиональной деятельности.	13			2	11	
Раздел 2. Информационная безопасность и защита данных в работе юриста	**28**		**2**	**4**	**22**	ОПК-7.1 ОПК-7.2 ОПК-7.3
Тема 2.1. Правовые вопросы обеспечение информационной безопасности.	13			2	11	
Тема 2.2. Защита и обслуживание информации в компьютерных системах.	15		2	2	11	
Раздел 3. Вид контроля	**1**	**1**				ОПК-7.1 ОПК-7.2 ОПК-7.3
Тема 3.1. Зачет	1	1				
Итого	**72**	**1**	**4**	**14**	**53**	

Очно-заочная форма обучения

Наименование раздела, темы	Всего	Внеаудиторная контактная работа	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Правовые базы данных и цифровые технологии в юридической практике	**41**		**3**	**5**	**33**	ОПК-7.1 ОПК-7.2 ОПК-7.3
Тема 1.1. Информационное общество и информатизация.	18		1	2	15	
Тема 1.2. Информационно-коммуникационные технологии.	6		1	2	3	
Тема 1.3. Компьютерные системы обмена информацией в профессиональной деятельности.	17		1	1	15	
Раздел 2. Информационная безопасность и защита данных в работе юриста	**26**		**1**	**1**	**24**	ОПК-7.1 ОПК-7.2 ОПК-7.3
Тема 2.1. Правовые вопросы обеспечение информационной безопасности.	17		1	1	15	

Тема 2.2. Защита и обслуживание информации в компьютерных системах.	9				9	
Раздел 3. Вид контроля	**1**	**1**				ОПК-7.1 ОПК-7.2 ОПК-7.3
Тема 3.1. Зачет	1	1				
Итого	**68**	**1**	**4**	**6**	**57**	

5.2. Содержание разделов, тем дисциплин

Раздел 1. Правовые базы данных и цифровые технологии в юридической практике (Заочная: Лекционные занятия - 2ч.; Практические занятия - 4ч.; Самостоятельная работа - 36ч.; Очная: Лекционные занятия - 2ч.; Практические занятия - 10ч.; Самостоятельная работа - 31ч.; Очно-заочная: Лекционные занятия - 3ч.; Практические занятия - 5ч.; Самостоятельная работа - 33ч.)

Тема 1.1. Информационное общество и информатизация.

(Заочная: Лекционные занятия - 1ч.; Практические занятия - 2ч.; Самостоятельная работа - 12ч.; Очно-заочная: Лекционные занятия - 1ч.; Практические занятия - 2ч.; Самостоятельная работа - 15ч.; Очная: Практические занятия - 4ч.; Самостоятельная работа - 8ч.)

Информация и данные. Виды информации. Обработка информации. Компьютер как универсальная система сбора, хранения и обработки многих видов информации (числовой, текстовой, символьной и др.). Понятие информационного общества и его особенности. Системы связи и обмена информацией. Право и информационные технологии. Государственная политика в сфере использования информационных технологий в органах государственной власти.

Тема 1.2. Информационно-коммуникационные технологии.
(Заочная: Лекционные занятия - 1ч.; Практические занятия - 1ч.; Самостоятельная работа - 12ч.; Очная: Лекционные занятия - 2ч.; Практические занятия - 4ч.; Самостоятельная работа - 12ч.; Очно-заочная: Лекционные занятия - 1ч.; Практические занятия - 2ч.; Самостоятельная работа - 3ч.)

История развития правовой информатики в России и за рубежом.
Системы связи и обмена информацией.
Развитие информационных и коммуникационных технологий как фактор развития общества.
Информационные системы в области правоохранительной деятельности, государственного управления и информационной безопасности.
Информационно-правовые системы: структура и классификация.
Государственная система распространения правовой информации.
Государственные информационные системы.
Система электронного опубликования нормативных актов и их проектов.

Тема 1.3. Компьютерные системы обмена информацией в профессиональной деятельности.
(Очно-заочная: Лекционные занятия - 1ч.; Практические занятия - 1ч.; Самостоятельная работа - 15ч.; Заочная: Практические занятия - 1ч.; Самостоятельная работа - 12ч.; Очная: Практические занятия - 2ч.; Самостоятельная работа - 11ч.)

Типы компьютерных сетей, их топология.
Физическая и логическая топология компьютерных сетей.
Базовые топологии компьютерных сетей.
Локальные сети и их типы.
Сеть Интернет как глобальный информационный ресурс.
Средства и устройства сетевого обмена цифровой информацией: телефонная сеть и модем, удаленный и мобильный доступ, провайдер Интернета.
Понятия «протокол», «интерфейс», «стек протоколов».
Протоколы передачи информации в сети.
Службы Интернет: Веб, почта, FTP и др.
Адреса информации в Интернете (числовой адрес компьютера, доменное имя компьютера, URL-адрес документа).
Веб-технологии в Интернете и локальной сети.
Веб-страница. Гипертекст, гиперссылки абсолютные и относительные.
Язык и формат HTML.
Возможности использования информационных и телекоммуникационных технологий в профессиональной деятельности.

Раздел 2. Информационная безопасность и защита данных в работе юриста
(Очная: Лекционные занятия - 2ч.; Практические занятия - 4ч.; Самостоятельная работа - 22ч.; Очно-заочная: Лекционные занятия - 1ч.; Практические занятия - 1ч.; Самостоятельная работа - 24ч.; Заочная: Практические занятия - 2ч.; Самостоятельная работа - 23ч.)

Тема 2.1. Правовые вопросы обеспечение информационной безопасности.

(Очно-заочная: Лекционные занятия - 1ч.; Практические занятия - 1ч.; Самостоятельная работа - 15ч.; Заочная: Практические занятия - 1ч.; Самостоятельная работа - 12ч.; Очная: Практические занятия - 2ч.; Самостоятельная работа - 11ч.)
Общие вопросы информационных прав и свобод человека и гражданина.
Сущность конституционного права на информацию и его гарантии.
Особенности обеспечения информационной безопасности в различных сферах жизни общества.
Правонарушение в информационной сфере, состав правонарушения.
Гражданская, административная, уголовная, дисциплинарная и иные виды ответственности.

Тема 2.2. Защита и обслуживание информации в компьютерных системах.
(Очная: Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 11ч.; Заочная: Практические занятия - 1ч.; Самостоятельная работа - 11ч.; Очно-заочная: Самостоятельная работа - 9ч.)
Принципы защиты информации.
Категории защищаемой информации.
Угрозы, риски и пути утечки компьютерной информации.
Основы защиты информации и сведений, составляющих государственную тайну.
Классификация мер защиты.
Приемы защиты информации.
Разграничение доступа, преобразование информации к нечитаемому виду (архивация, кодирование, шифрование).
Парольная защита.
Электронная подпись.

Раздел 3. Вид контроля
(Заочная: Внеаудиторная контактная работа - 1ч.; Очная: Внеаудиторная контактная работа - 1ч.; Очно-заочная: Внеаудиторная контактная работа - 1ч.)

Тема 3.1. Зачет
(Заочная: Внеаудиторная контактная работа - 1ч.; Очная: Внеаудиторная контактная работа - 1ч.; Очно-заочная: Внеаудиторная контактная работа - 1ч.)
Зачет

6. Оценочные материалы текущего контроля

Раздел 1. Правовые базы данных и цифровые технологии в юридической практике

Форма контроля/оценочное средство: Задача

Вопросы/Задания:

1. Установите соответствие между правовой базой данных и ее характеристикой:

База данных
1. КонсультантПлюс
2. Гарант
3. СПС "Кодекс"
4. Правовая Россия

Характеристика
А. Государственная система правовой информации
Б. Коммерческая система с аналитическими блоками
В. Включает судебную практику и экспертные материалы
Г. Официальный портал государственных нормативных актов

2. Какой из перечисленных методов защиты информации относится к организационным мерам?

А) Шифрование данных
Б) Установка антивирусного ПО
В) Разработка политики информационной безопасности
Г) Использование VPN

3. Установите правильную последовательность действий при работе с правовой базой данных:

1. Формулировка запроса
2. Выбор базы данных
3. Анализ полученных документов
4. Ввод поисковых критериев
5. Сохранение или экспорт результатов

4. Какие из перечисленных мер обеспечивают защиту персональных данных в соответствии с ФЗ-152? (Выберите 3 варианта)

А) Регулярное обновление паролей
Б) Назначение ответственного за обработку ПДн
В) Использование только бумажных носителей
Г) Ведение журнала учета обращений к данным

5. Опишите, какие угрозы информационной безопасности могут возникнуть при использовании облачных сервисов в юридической деятельности и как их минимизировать.

Угрозы: утечка данных из-за слабой защиты облачного провайдера, несанкционированный доступ, риски потери данных при аварии сервера.
Меры: выбор сертифицированных облаков (например, с ГОСТ Р 57580), шифрование данных перед загрузкой, двухфакторная аутентификация, регулярное резервное копирование.

Подходит ли вышесказанное к заданному вопросу? Если нет, то запишите свой вариант ответа. Если да, то запишите "Да, подходит"

6. Установите соответствие между стандартом информационной безопасности и его описанием:

Стандарт

1. ISO 27001
2. ФЗ-152
3. ГОСТ Р 57580
4. ФСТЭК России

Описание
А. Российский стандарт защиты персональных данных
Б. Международный стандарт управления ИБ
В. Требования к средствам криптозащиты
Г. Регулирует защиту критической информационной инфраструктуры

7. Проанализируйте, какие правовые базы данных наиболее эффективны для поиска судебной практики по арбитражным спорам. Обоснуйте выбор.

Наиболее эффективны:
- КонсультантПлюс (раздел "Судебная практика" с фильтрами по категориям дел).
- ГАС "Правосудие" (официальные решения судов).
- Картотека арбитражных дел (онлайн-доступ к делам).

Подходит ли вышесказанное к заданному вопросу? Если нет, то запишите свой вариант ответа. Если да, то запишите "Да, подходит"

8. Какие элементы должны включаться в политику информационной безопасности юридической фирмы? (Выберите 3 варианта)

А) Правила использования электронной почты
Б) График уборки офиса
В) Порядок доступа к конфиденциальным документам
Г) Регламент резервного копирования
Д) Список сотрудников с их зарплатами

9. Какой федеральный закон регулирует защиту персональных данных в России?

А) ФЗ-149 "Об информации, информационных технологиях и о защите информации"
Б) ФЗ-152 "О персональных данных"
В) ФЗ-99 "О лицензировании отдельных видов деятельности"
Г) ФЗ-63 "Об электронной подписке"

10. Установите соответствие между термином и его определением:

Термин
1. Конфиденциальность
2. Целостность
3. Доступность

Определение
А. Гарантия того, что информация доступна только авторизованным пользователям
Б. Защита от несанкционированного изменения данных
В. Обеспечение доступа к информации в нужное время

11. Какие из перечисленных мер относятся к криптографической защите информации? (Выберите 3 варианта)

А) Использование электронной подписи
Б) Установка антивируса
В) Шифрование файлов
Г) Настройка брандмауэра
Д) Применение VPN

12. Установите правильную последовательность обработки персональных данных в организации:

1. Получение согласия субъекта ПДн
2. Определение целей обработки
3. Внедрение мер защиты данных

4. Назначение ответственного за обработку ПДн
5. Регистрация в Роскомнадзоре (если требуется)

13. Опишите, какие технические и организационные меры должны быть применены в юридической фирме для защиты клиентских данных при использовании облачных хранилищ.

Технические меры:
- Шифрование данных перед загрузкой в облако (AES-256).
- Использование сертифицированных облачных провайдеров (например, с соответствием ГОСТ Р 57580).
- Двухфакторная аутентификация для доступа.

Организационные меры:
- Заключение NDA с сотрудниками и облачным провайдером.
- Регулярный аудит доступа к данным.
- Инструктаж сотрудников по работе с облачными сервисами.

Подходит ли вышесказанное к заданному вопросу? Если нет, то запишите свой вариант ответа. Если да, то запишите "Да, подходит"

14. Установите соответствие между правовым актом и его сферой регулирования:

Акт
1. ФЗ-149
2. ФЗ-152
3. ФЗ-187
4. Приказ ФСТЭК №17

Сфера регулирования
А. Защита персональных данных
Б. Информационная безопасность КИИ
В. Общие принципы работы с информацией
Г. Требования к СЗИ от угроз утечки

15. Какой стандарт информационной безопасности обязателен для государственных информационных систем в РФ?

А) ISO 27001
Б) PCI DSS
В) ГОСТ Р 57580
Г) GDPR

16. Какие риски возникают при использовании публичного Wi-Fi для доступа к правовым базам данных? Предложите меры защиты.

Риски:
- Перехват данных (логины, пароли).
- Фишинг-атаки через поддельные точки доступа.

Меры:
- Использование VPN.
- Отключение автоматического подключения к сетям.
- Проверка HTTPS-соединения.

Подходит ли вышесказанное к заданному вопросу? Если нет, то запишите свой вариант ответа. Если да, то запишите "Да, подходит"

17. Установите порядок действий при утечке персональных данных:

1. Блокировка доступа к данным
2. Уведомление Роскомнадзора
3. Расследование инцидента
4. Информирование субъектов ПДн

18. Какие элементы включает электронная подпись? (Выберите 2 варианта)

А) ФИО подписанта

Б) Криптографический ключ
В) IP-адрес компьютера
Г) Сертификат проверки подлинности

19. Установите соответствие между этапами расследования киберинцидента и действиями юриста:

Этап
1. Идентификация
2. Сдерживание
3. Восстановление
4. Анализ

Действие
А. Фиксация доказательств (логи, дампы памяти)
Б. Определение вектора атаки и уязвимости
В. Изоляция зараженных систем от сети
Г. Восстановление данных из backup

20. Какие ключевые меры информационной безопасности необходимы при внедрении СЭД в юридической фирме для защиты клиентских данных?

1. Использование только простой электронной подписи для всех документов
2. Внедрение системы разграничения доступа на основе ролей (RBAC)
3. Обязательное шифрование всех передаваемых документов
4. Хранение архивов документов на персональных компьютерах сотрудников
5. Регулярное проведение аудита действий пользователей в системе
6. Использование облачного хранилища без дополнительных мер защиты

Раздел 2. Информационная безопасность и защита данных в работе юриста

Форма контроля/оценочное средство: Компетентностно-ориентированное задание

Вопросы/Задания:

1. При проведении e-discovery в рамках арбитражного спора обнаружены противоречия в метаданных файлов. Какие технические методы позволят доказать фальсификацию? (Выберите 3 варианта)

А) Анализ MAC-времени (изменение/создание файлов)
Б) Проверка хэш-сумм оригиналов и копий
В) Экспертиза стилистики текста
Г) Сопоставление логов доступа к файловому серверу

2. Определите порядок изъятия электронных доказательств:

1. Фиксация состояния устройства (фото/видео)
2. Извлечение памяти с помощью write-blocker
3. Составление протокола с участием понятых
4. Копирование данных на сертифицированный носитель
5. Проверка целостности копии через хэширование

3. Сравните требования к уведомлению о нарушениях ПДн по GDPR и ФЗ-152. В каких случаях российская компания, работающая с данными граждан ЕС, должна выполнять оба регламента?

- GDPR: Уведомление в течение 72 часов, если нарушение создает риск для прав субъектов (ст. 33).
- ФЗ-152: Уведомление Роскомнадзора в течение 24 часов при наличии угрозы (ст. 22).
- Двойной compliance: Требуется при обработке данных граждан ЕС на территории РФ (например, интернет-магазин с европейскими клиентами).

Подходит ли вышесказанное к заданному вопросу? Если нет, то запишите свой вариант ответа. Если да, то запишите "Да, подходит"

4. При проверке ИБ выявлено, что сотрудник хранит клиентские договоры в личном облаке Mail.ru. Какая статья КоАП РФ будет применена?

А) Ст. 13.11 (нарушение требований к защите ПДн)
Б) Ст. 13.12 (несоблюдение правил использования СКЗИ)
В) Ст. 19.5 (невыполнение предписаний регулятора)
Г) Ст. 28.3 (злоупотребление должностными полномочиями)

5. Вам как юристу компании поступил запрос от ИБ-отдела о согласовании политики BYOD (Bring Your Own Device). Какие 3 ключевых пункта должны быть включены в политику для соблюдения ФЗ-152?

1. Обязательное шифрование устройств с доступом к ПДн.
2. Удаленный wipe данных при утере/увольнении.
3. Запрет на хранение ПДн в личных облачных сервисах.

Подходит ли вышесказанное к заданному вопросу? Если нет, то запишите свой вариант ответа. Если да, то запишите "Да, подходит"

6. Проанализируйте скриншот интерфейса СПС "КонсультантПлюс". Какие ошибки в работе с базой данных допустил юрист (на примере поиска судебной практики по ст. 178 ГК РФ)?

- Использование только ключевых слов без операторов поиска ("обман" вместо "обман + ст. 178 ГК РФ").
- Отсутствие фильтрации по дате (актуальность данных).
- Не сохранены результаты поиска в личный кабинет для аудита.

Подходит ли вышесказанное к заданному вопросу? Если нет, то запишите свой вариант ответа. Если да, то запишите "Да, подходит"

7. Какой вид электронной подписи является наиболее защищенным и приравнивается к собственноручной подписи с печатью?

А) Простая электронная подпись
Б) Неквалифицированная электронная подпись
В) Квалифицированная электронная подпись
Г) Усиленная неквалифицированная подпись

8. Установите правильный порядок действий при проверке контрагента через правовые базы данных:

1. Поиск реквизитов компании в ЕГРЮЛ
2. Проверка наличия судебных дел в картотеке арбитражных судов
3. Анализ финансовой отчетности в СПАРК или SCAN
4. Поиск упоминаний в реестре недобросовестных поставщиков
5. Формирование отчета о благонадежности

9. В организации произошла утечка данных клиентов из-за взлома почтового ящика юриста. Опишите:

Опишите:

1. Какие нормативные акты были нарушены (укажите статьи)
2. Порядок действий по расследованию
3. Меры для предотвращения подобных инцидентов

1. Нарушены:
- Ст. 19 ФЗ-152 (необеспечение безопасности ПДн)
- Ст. 13.11 КоАП РФ (влечет штраф до 200 тыс. руб.)
2. Действия:
- Фиксация времени взлома через логи почтового сервиса
- Уведомление Роскомнадзора в течение 72 часов
- Аудит систем защиты email (отсутствие 2FA)
3. Меры:
- Внедрение обязательной двухфакторной аутентификации
- Регулярные тренинги по фишинговой безопасности

Подходит ли вышесказанное к заданному вопросу? Если нет, то запишите свой вариант ответа. Если да, то запишите "Да, подходит"

10. Установите соответствие между государственной информационной системой и ее функционалом:

Система
1. ГАС "Правосудие"
2. ФИС ФРДО
3. ЕГРН
4. Портал госуслуг

Функционал
А. Доступ к текстам судебных решений
Б. Проверка дипломов об образовании
В. Получение данных о недвижимости
Г. Подача искового заявления онлайн

Раздел 3. Вид контроля

Форма контроля/оценочное средство:

Вопросы/Задания:

.

7. Оценочные материалы промежуточной аттестации

Очная форма обучения, Второй семестр, Зачет
Контролируемые ИДК: ОПК-7.1 ОПК-7.2 ОПК-7.3
Вопросы/Задания:

1. Информация и данные.

2. Виды информации. Обработка информации.

3. Компьютер как универсальная система сбора, хранения и обработки многих видов информации (числовой, текстовой, символьной и др.).

4. Понятие информационного общества и его особенности.

5. Развитие информационных и коммуникационных технологий как фактор развития общества.

6. Общие вопросы информационных прав и свобод человека и гражданина.

7. Сущность конституционного права на информацию и его гарантии.

8. Системы связи и обмена информацией.

9. Компьютерные сети.

10. Типы компьютерных сетей, их топология.

11. Физическая и логическая топология компьютерных сетей.

12. Базовые топологии компьютерных сетей.

13. Локальные сети и их типы.

14. Сеть Интернет как глобальный информационный ресурс.

15. Средства и устройства сетевого обмена цифровой информацией: телефонная сеть и модем, удаленный и мобильный доступ, провайдер Интернета.

16. Понятия «протокол», «интерфейс», «стек протоколов».

17. Протоколы передачи информации в сети.

18. Службы Интернет: Веб, почта, FTP и др.

19. Адреса информации в Интернете (числовой адрес компьютера, доменное имя компьютера, URL-адрес документа).

20. Веб-технологии в Интернете и локальной сети.

21. Веб-страница.

22. Гипертекст, гиперссылки абсолютные и относительные.

23. Язык и формат HTML.

24. Право и информационные технологии.

25. Государственная политика в сфере использования информационных технологий в органах государственной власти.

26. Информационные технологии в сфере правовых отношений: этапы развития.

27. История развития правовой информатики в России и за рубежом.

28. Информационные системы в области правоохранительной деятельности, государственного управления и информационной безопасности.

29. Информационные системы: структура и классификация.

30. Государственная система распространения правовой информации.

31. Государственные информационные системы. Система электронного опубликования нормативных актов и их проектов.

32. Использование компьютерных сетей в организациях и правоохранительной сфере.

33. Особенности обеспечения информационной безопасности в различных сферах жизни общества.

34. Правонарушение в информационной сфере, состав правонарушения.

35. Гражданская, административная, уголовная, дисциплинарная и иные виды ответственности за правонарушения в информационной сфере.

36. Информационная безопасность.

37. Понятие защиты информации.

38. Принципы защиты информации.

39. Категории защищаемой информации.

40. Угрозы, риски и пути утечки компьютерной информации.

41. Основы защиты информации и сведений, составляющих государственную тайну. Классификация мер защиты.

42. Приемы защиты информации.

43. Разграничение доступа, преобразование информации к нечитаемому виду (архивация, кодирование, шифрование).

44. Возможности использования информационных и телекоммуникационных технологий в профессиональной деятельности.

45. Перспективы развития информационных технологий в правовой сфере

46. Электронное правительство и цифровизация государственных услуг

47. Роль искусственного интеллекта в правоохранительной деятельности

48. Киберпреступность и методы борьбы с ней

49. Цифровая трансформация судебной системы

50. Правовое регулирование персональных данных в цифровую эпоху

Очно-заочная форма обучения, Второй семестр, Зачет
Контролируемые ИДК: ОПК-7.1 ОПК-7.2 ОПК-7.3
Вопросы/Задания:

1. Информация и данные.

2. Виды информации. Обработка информации.

3. Компьютер как универсальная система сбора, хранения и обработки многих видов информации (числовой, текстовой, символьной и др.).

4. Понятие информационного общества и его особенности.

5. Развитие информационных и коммуникационных технологий как фактор развития общества.

6. Общие вопросы информационных прав и свобод человека и гражданина.

7. Сущность конституционного права на информацию и его гарантии.

8. Системы связи и обмена информацией.

9. Компьютерные сети.

10. Типы компьютерных сетей, их топология.

11. Физическая и логическая топология компьютерных сетей.

12. Базовые топологии компьютерных сетей.

13. Локальные сети и их типы.

14. Сеть Интернет как глобальный информационный ресурс.

15. Средства и устройства сетевого обмена цифровой информацией: телефонная сеть и модем, удаленный и мобильный доступ, провайдер Интернета.

16. Понятия «протокол», «интерфейс», «стек протоколов».

17. Протоколы передачи информации в сети.

18. Службы Интернет: Веб, почта, FTP и др.

19. Адреса информации в Интернете (числовой адрес компьютера, доменное имя компьютера, URL-адрес документа).

20. Веб-технологии в Интернете и локальной сети.

21. Веб-страница.

22. Гипертекст, гиперссылки абсолютные и относительные.

23. Язык и формат HTML.

24. Право и информационные технологии.

25. Государственная политика в сфере использования информационных технологий в органах государственной власти.

26. Информационные технологии в сфере правовых отношений: этапы развития.

27. История развития правовой информатики в России и за рубежом.

28. Информационные системы в области правоохранительной деятельности, государственного управления и информационной безопасности.

29. Информационные системы: структура и классификация.

30. Государственная система распространения правовой информации.

31. Государственные информационные системы. Система электронного опубликования нормативных актов и их проектов.

32. Использование компьютерных сетей в организациях и правоохранительной сфере.

33. Особенности обеспечения информационной безопасности в различных сферах жизни общества.

34. Правонарушение в информационной сфере, состав правонарушения.

35. Гражданская, административная, уголовная, дисциплинарная и иные виды ответственности за правонарушения в информационной сфере.

36. Информационная безопасность.

37. Понятие защиты информации.

38. Принципы защиты информации.

39. Категории защищаемой информации.

40. Угрозы, риски и пути утечки компьютерной информации.

41. Основы защиты информации и сведений, составляющих государственную тайну. Классификация мер защиты.

42. Приемы защиты информации.

43. Разграничение доступа, преобразование информации к нечитаемому виду (архивация, кодирование, шифрование).

44. Возможности использования информационных и телекоммуникационных технологий в профессиональной деятельности.

45. Перспективы развития информационных технологий в правовой сфере

46. Электронное правительство и цифровизация государственных услуг

47. Роль искусственного интеллекта в правоохранительной деятельности

48. Киберпреступность и методы борьбы с ней

49. Цифровая трансформация судебной системы

50. Правовое регулирование персональных данных в цифровую эпоху

Очно-заочная форма обучения, Второй семестр, Контрольная работа
Контролируемые ИДК: ОПК-7.1 ОПК-7.2 ОПК-7.3
Вопросы/Задания:

1. Дайте определение понятиям «информационное общество» и «цифровая экономика». Как эти явления влияют на современную правовую систему?

2. Опишите структуру государственных информационных систем в сфере правоохранительной деятельности. Приведите примеры таких систем в РФ.

3. Какие виды угроз информационной безопасности наиболее актуальны для юридических организаций? Раскройте методы противодействия им.

4. Объясните принципы работы технологии блокчейн. Как она может быть использована в нотариальной деятельности или ведении реестров прав?

5. В чем заключаются особенности регулирования персональных данных по 152-ФЗ и GDPR? Сравните эти законы по критериям: объем данных, права субъектов, штрафные санкции.

6. Ситуационная задача:
В юридической фирме произошла утечка конфиденциальных данных клиентов через фишинговое письмо. Опишите алгоритм действий для:
- минимизации последствий,
- расследования инцидента,
- предотвращения подобных случаев в будущем.

7. Составьте схему
«Протоколы передачи данных в компьютерных сетях» с пояснениями, где:
- Укажите уровни модели OSI,
- Приведите примеры протоколов (HTTP, FTP, TLS) и их назначение.

8. Задание на знание веб-технологий:
Дайте определение следующим терминам:
- URL-адрес,
- HTML-тег,
- гиперссылка.
Приведите пример использования каждого в юридическом сайте (например, размещение нормативного акта).

9. Кейс по информационной безопасности:
Сотрудник правоохранительного органа использовал незашифрованный USB-накопитель для передачи служебных данных. Какие нормы закона он нарушил? Какие технические и организационные меры защиты должны были быть применены?

10. Тестовое задание (выберите правильные ответы):
1. Криптография используется для:
a) Сжатия файлов,
b) Защиты данных от несанкционированного доступа,
c) Ускорения работы сети.

2. Локальная сеть (LAN) — это:

a) Сеть в пределах одного здания,
b) Глобальная сеть типа Интернет,
c) Система спутниковой связи.

3. Какой закон регулирует защиту государственной тайны в РФ?
a) 149-ФЗ,
b) 5485-1-ФЗ,
c) 152-ФЗ.

11. Дайте определение понятию "правовая информатика". Каковы её основные задачи в юридической деятельности?

12. Опишите этапы развития информационных технологий в правовой сфере. Как менялось их применение с 1990-х годов по настоящее время?

13. Какие виды информации по степени доступа существуют в соответствии с российским законодательством? Дайте характеристику каждому виду.

14. Раскройте содержание принципа "электронного правительства". Приведите примеры его реализации в России.

15. Что такое "информационная безопасность" в контексте юридической деятельности? Назовите 3 основных составляющих ИБ.

16. Объясните назначение и функции Государственной автоматизированной системы "Правосудие" (ГАС "Правосудие").

17. Дайте сравнительную характеристику Федеральных законов № 149-ФЗ и № 152-ФЗ по следующим критериям:
- Сфера регулирования
- Субъекты отношений
- Ответственность за нарушения

18. Каковы правовые основы использования электронной подписи в юридической деятельности? Виды ЭП и их различия.

19. Опишите структуру и назначение системы "КонсультантПлюс" как примера справочной правовой системы.

20. Какие международные стандарты в области информационной безопасности применяются в российской практике?

21. Составьте сравнительную таблицу "Типы компьютерных сетей" по критериям:
- Масштаб (LAN, WAN и др.)
- Способ организации
- Использование в юридической деятельности

22. Решите задачу:
В адвокатское бюро поступил вирус через электронную почту, что привело к утечке данных клиентов. Какие действия должен предпринять IT-специалист в соответствии с 152-ФЗ? Составьте пошаговый алгоритм.

23. Составьте схему "Способы защиты информации в юридической фирме" с выделением:
- Технических мер

- Организационных мер
- Правовых мер

24. Проанализируйте ситуацию:

Сотрудник прокуратуры использовал мессенджер для передачи служебной информации. Оцените правомерность действий с точки зрения ФЗ "О персональных данных" и ведомственных регламентов.

25. Составьте инструкцию "Правила работы с конфиденциальными документами в электронном виде" (не менее 5 пунктов).

26. Определите виды ответственности за следующие правонарушения в ИТ-сфере:

a) Несанкционированный доступ к информации
b) Разглашение коммерческой тайны
c) Нарушение правил эксплуатации средств защиты информации

27. Разработайте памятку "Безопасное использование облачных сервисов в юридической практике" (не менее 5 рекомендаций).

28. Решите кейс:

При проведении электронного аукциона возник спор о подлинности электронной подписи. Какие экспертизы могут быть назначены и какие нормативные акты регулируют этот вопрос?

29. Составьте глоссарий из 10 ключевых терминов по курсу с их определениями.

Пример: "Криптография" - наука о методах обеспечения конфиденциальности...

30. Решите ситуацию:

Ситуация:
В юридической фирме произошёл инцидент: злоумышленники получили доступ к конфиденциальным данным клиентов через уязвимость в системе электронного документооборота. В результате были похищены персональные данные 500 клиентов, включая их паспортные данные и финансовую информацию.

Задание:
- Определите виды нарушенных требований законодательства РФ (укажите конкретные статьи 152-ФЗ, 149-ФЗ, УК РФ).
- Разработайте план мероприятий по ликвидации последствий инцидента (не менее 5 шагов).
- Предложите меры профилактики подобных инцидентов в будущем (технические, организационные, правовые).
- Опишите порядок уведомления регуляторов и пострадавших клиентов в соответствии с 152-ФЗ.

Заочная форма обучения, Второй семестр, Зачет
Контролируемые ИДК: ОПК-7.1 ОПК-7.2 ОПК-7.3

Вопросы/Задания:

1. Информация и данные.

2. Виды информации. Обработка информации.

3. Компьютер как универсальная система сбора, хранения и обработки многих видов информации (числовой, текстовой, символьной и др.).

4. Понятие информационного общества и его особенности.

5. Развитие информационных и коммуникационных технологий как фактор развития общества.

6. Общие вопросы информационных прав и свобод человека и гражданина.

7. Сущность конституционного права на информацию и его гарантии.

8. Системы связи и обмена информацией.

9. Компьютерные сети.

10. Типы компьютерных сетей, их топология.

11. Физическая и логическая топология компьютерных сетей.

12. Базовые топологии компьютерных сетей.

13. Локальные сети и их типы.

14. Сеть Интернет как глобальный информационный ресурс.

15. Средства и устройства сетевого обмена цифровой информацией: телефонная сеть и модем, удаленный и мобильный доступ, провайдер Интернета.

16. Понятия «протокол», «интерфейс», «стек протоколов».

17. Протоколы передачи информации в сети.

18. Службы Интернет: Веб, почта, FTP и др.

19. Адреса информации в Интернете (числовой адрес компьютера, доменное имя компьютера, URL-адрес документа).

20. Веб-технологии в Интернете и локальной сети.

21. Веб-страница.

22. Гипертекст, гиперссылки абсолютные и относительные.

23. Язык и формат HTML.

24. Право и информационные технологии.

25. Государственная политика в сфере использования информационных технологий в органах государственной власти.

26. Информационные технологии в сфере правовых отношений: этапы развития.

27. История развития правовой информатики в России и за рубежом.

28. Информационные системы в области правоохранительной деятельности, государственного управления и информационной безопасности.

29. Информационные системы: структура и классификация.

30. Государственная система распространения правовой информации.

31. Государственные информационные системы. Система электронного опубликования нормативных актов и их проектов.

32. Использование компьютерных сетей в организациях и правоохранительной сфере.

33. Особенности обеспечения информационной безопасности в различных сферах жизни общества.

34. Правонарушение в информационной сфере, состав правонарушения.

35. Гражданская, административная, уголовная, дисциплинарная и иные виды ответственности за правонарушения в информационной сфере.

36. Информационная безопасность.

37. Понятие защиты информации.

38. Принципы защиты информации.

39. Категории защищаемой информации.

40. Угрозы, риски и пути утечки компьютерной информации.

41. Основы защиты информации и сведений, составляющих государственную тайну. Классификация мер защиты.

42. Приемы защиты информации.

43. Разграничение доступа, преобразование информации к нечитаемому виду (архивация, кодирование, шифрование).

44. Возможности использования информационных и телекоммуникационных технологий в профессиональной деятельности.

45. Перспективы развития информационных технологий в правовой сфере

46. Электронное правительство и цифровизация государственных услуг

47. Роль искусственного интеллекта в правоохранительной деятельности

48. Киберпреступность и методы борьбы с ней

49. Цифровая трансформация судебной системы

50. Правовое регулирование персональных данных в цифровую эпоху

Заочная форма обучения, Второй семестр, Контрольная работа
Контролируемые ИДК: ОПК-7.1 ОПК-7.2 ОПК-7.3
Вопросы/Задания:

1. Дайте определение понятиям «информационное общество» и «цифровая экономика». Как эти явления влияют на современную правовую систему?

2. Опишите структуру государственных информационных систем в сфере правоохранительной деятельности. Приведите примеры таких систем в РФ.

3. Какие виды угроз информационной безопасности наиболее актуальны для юридических организаций? Раскройте методы противодействия им.

4. Объясните принципы работы технологии блокчейн. Как она может быть использована в нотариальной деятельности или ведении реестров прав?

5. В чем заключаются особенности регулирования персональных данных по 152-ФЗ и GDPR? Сравните эти законы по критериям: объем данных, права субъектов, штрафные санкции.

6. Ситуационная задача:

В юридической фирме произошла утечка конфиденциальных данных клиентов через фишинговое письмо. Опишите алгоритм действий для:
- минимизации последствий,
- расследования инцидента,
- предотвращения подобных случаев в будущем.

7. Составьте схему

«Протоколы передачи данных в компьютерных сетях» с пояснениями, где:
- Укажите уровни модели OSI,
- Приведите примеры протоколов (HTTP, FTP, TLS) и их назначение.

8. Задание на знание веб-технологий:

Дайте определение следующим терминам:
- URL-адрес,
- HTML-тег,
- гиперссылка.

Приведите пример использования каждого в юридическом сайте (например, размещение нормативного акта).

9. Кейс по информационной безопасности:

Сотрудник правоохранительного органа использовал незашифрованный USB-накопитель для передачи служебных данных. Какие нормы закона он нарушил? Какие технические и организационные меры защиты должны были быть применены?

10. Тестовое задание (выберите правильные ответы):

1. Криптография используется для:
a) Сжатия файлов,
b) Защиты данных от несанкционированного доступа,
c) Ускорения работы сети.

2. Локальная сеть (LAN) — это:
a) Сеть в пределах одного здания,
b) Глобальная сеть типа Интернет,
c) Система спутниковой связи.

3. Какой закон регулирует защиту государственной тайны в РФ?
a) 149-ФЗ,
b) 5485-1-ФЗ,
c) 152-ФЗ.

11. Дайте определение понятию "правовая информатика". Каковы её основные задачи в юридической деятельности?

12. Опишите этапы развития информационных технологий в правовой сфере. Как менялось их применение с 1990-х годов по настоящее время?

13. Какие виды информации по степени доступа существуют в соответствии с российским законодательством? Дайте характеристику каждому виду.

14. Раскройте содержание принципа "электронного правительства". Приведите примеры его реализации в России.

15. Что такое "информационная безопасность" в контексте юридической деятельности? Назовите 3 основных составляющих ИБ.

16. Объясните назначение и функции Государственной автоматизированной системы "Правосудие" (ГАС "Правосудие").

17. Дайте сравнительную характеристику Федеральных законов № 149-ФЗ и № 152-ФЗ по следующим критериям:
- Сфера регулирования
- Субъекты отношений
- Ответственность за нарушения

18. Каковы правовые основы использования электронной подписи в юридической деятельности? Виды ЭП и их различия.

19. Опишите структуру и назначение системы "КонсультантПлюс" как примера справочной правовой системы.

20. Какие международные стандарты в области информационной безопасности применяются в российской практике?

21. Составьте сравнительную таблицу "Типы компьютерных сетей" по критериям:
- Масштаб (LAN, WAN и др.)
- Способ организации
- Использование в юридической деятельности

22. Решите задачу:
В адвокатское бюро поступил вирус через электронную почту, что привело к утечке данных клиентов. Какие действия должен предпринять IT-специалист в соответствии с 152-ФЗ? Составьте пошаговый алгоритм.

23. Составьте схему "Способы защиты информации в юридической фирме" с выделением:
- Технических мер
- Организационных мер
- Правовых мер

24. Проанализируйте ситуацию:

Сотрудник прокуратуры использовал мессенджер для передачи служебной информации. Оцените правомерность действий с точки зрения ФЗ "О персональных данных" и ведомственных регламентов.

25. Составьте инструкцию "Правила работы с конфиденциальными документами в электронном виде" (не менее 5 пунктов).

26. Определите виды ответственности за следующие правонарушения в ИТ-сфере:

a) Несанкционированный доступ к информации

b) Разглашение коммерческой тайны

c) Нарушение правил эксплуатации средств защиты информации

27. Разработайте памятку "Безопасное использование облачных сервисов в юридической практике" (не менее 5 рекомендаций).

28. Решите кейс:

При проведении электронного аукциона возник спор о подлинности электронной подписи. Какие экспертизы могут быть назначены и какие нормативные акты регулируют этот вопрос?

29. Составьте глоссарий из 10 ключевых терминов по курсу с их определениями.

Пример: "Криптография" - наука о методах обеспечения конфиденциальности...

30. Решите ситуацию:

Ситуация:

В юридической фирме произошёл инцидент: злоумышленники получили доступ к конфиденциальным данным клиентов через уязвимость в системе электронного документооборота. В результате были похищены персональные данные 500 клиентов, включая их паспортные данные и финансовую информацию.

Задание:

- Определите виды нарушенных требований законодательства РФ (укажите конкретные статьи 152-ФЗ, 149-ФЗ, УК РФ).
- Разработайте план мероприятий по ликвидации последствий инцидента (не менее 5 шагов).
- Предложите меры профилактики подобных инцидентов в будущем (технические, организационные, правовые).
- Опишите порядок уведомления регуляторов и пострадавших клиентов в соответствии с 152-ФЗ.

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. ГРИЦАЕВ С. И. Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности: метод. указания / ГРИЦАЕВ С. И.. - Краснодар: КубГАУ, 2025. - 25 с. - Текст: непосредственный.

2. ПОМАЗАНОВ В. В. Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности: учеб. пособие / ПОМАЗАНОВ В. В.. - Краснодар: КубГАУ, 2021. - 102 с. - 978-5-907474-90-1. - Текст: электронный. // : [сайт]. - URL: https://edu.kubsau.ru/mod/resource/view.php?id=10358 (дата обращения: 08.09.2025). - Режим доступа: по подписке

Дополнительная литература

1. ГРИЦАЕВ С. И. Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности: метод. указания / ГРИЦАЕВ С. И.. - Краснодар: КубГАУ, 2024. - 19 с. - Текст: непосредственный.

2. ПОМАЗАНОВ В.В. Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности: учеб. пособие / ПОМАЗАНОВ В.В.. - Краснодар: КубГАУ, 2021. - 101 с. - 978-5-907474-90-1. - Текст: непосредственный.

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. https://sudact.ru/ - Судебные и нормативные акты РФ
2. https://www.consultant.ru/ - КонсультантПлюс

Ресурсы «Интернет»

1. https://www.rsl.ru/ - ФГБУ «Российская государственная библиотека»
2. https://www.kublse.ru - Официальный сайт ФБУ «Краснодарская лаборатория судебной экспертизы Министерства юстиции Российской Федерации»
3. www.sledcom.ru - Официальный сайт Следственного комитета Российской Федерации
4. http://www.pravo.gov.ru/ips/ - Официальный интернет-портал правовой информации
5. www.мвд.рф - Официальный сайт МВД России

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине позволяют:
– обеспечить взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет»;
– фиксировать ход образовательного процесса, результатов промежуточной аттестации по дисциплине и результатов освоения образовательной программы;
– организовать процесс образования путем визуализации изучаемой информации посредством использования презентаций, учебных фильмов;
– контролировать результаты обучения на основе компьютерного тестирования.
Перечень лицензионного программного обеспечения:
1 Microsoft Windows - операционная система.
2 Microsoft Office (включает Word, Excel, Power Point) - пакет офисных приложений.
Перечень профессиональных баз данных и информационных справочных систем:
1 Гарант - правовая, https://www.garant.ru/
2 Консультант - правовая, https://www.consultant.ru/
3 Научная электронная библиотека eLibrary - универсальная, https://elibrary.ru/
Доступ к сети Интернет, доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Не используется.

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Университет располагает на праве собственности или ином законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации программы бакалавриата, специлитета, магистратуры по Блоку 1 "Дисциплины (модули)" и Блоку 3 "Государственная итоговая аттестация" в соответствии с учебным планом.
Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне его. Условия для функционирования электронной информационно-образовательной среды могут быть созданы с использованием ресурсов иных организаций.

Лекционный зал
3гд
Облучатель-рециркулятор воздуха 600 - 0 шт.

Учебная аудитория
436гл
доска ДК11Э2010.. - 1 шт.
жалюзи.. - 1 шт.
парты.. - 15 шт.
Сплит-система настенная QuattroClima QV/QN-ES18WA - 1 шт.
437гл
сплит-система BEKO - 0 шт.
014зоо
Парта - 16 шт.
телевизор Samsung LCD- LE-46 - 0 шт.
020зоо
Парта - 16 шт.
025зоо
стол компьютерный - 16 шт.
телевизор ,,Филипс,, - 0 шт.
026а зоо
Парта - 16 шт.
телевизор SONY - 0 шт.

Лаборатория
510гл
Аквадистиллятор АЭ-5 - 1 шт.
баня ТЖ-ТБ-01/26 термостатирующая, Термобаня жидкостная ТЖ-ТБ-01 (26ц) - 1 шт.
Весы лабораторные МЛ 0,6-II ВЖА (0,01; D=116) "Ньютон-1" (d=0.01) с поверкой - 1 шт.
Весы МЛ 3-VII ВЖА "Ньютон-1" 3 кг с поверкой - 1 шт.
Магнитная мешалка с нагревом UED-20 - 1 шт.
Плита нагревательная лабораторная ПЛ-1818 - 1 шт.
Прибор для перегонки спирта - 1 шт.
Рефрактометр ИРФ-454 Б2М - 1 шт.
Спектрофотометр ПЭ-5400УФ/Россия с компьютером и принтером - 1 шт.
Телевизор LED 75*(190см) DEXP U75H8000K {4K UltraHD, 3840x2160, Smart TV, Яндекс.ТВ} - 1 шт.
Холодильник бытовой двухкамерный Позис RK-101, белый, 250 л, 3 полки, стекло, Россия - 1 шт.
Шейкер US-1350L - 1 шт.
Электроплитка "Кварц" 2 модель ЭПП-1-1,2/220 (6,5) - 1 шт.

Компьютерный класс
025а зоо
Компьютер персональный Lenovo ThinkCentre 4GbDDR4 128 GB SSD+монитор Dell - 0 шт.
стол компьютерный - 10 шт.

9. Методические указания по освоению дисциплины (модуля)

Учебная работа по направлению подготовки осуществляется в форме контактной работы с преподавателем, самостоятельной работы обучающегося, текущей и промежуточной аттестаций, иных формах, предлагаемых университетом. Учебный материал дисциплины структурирован и его изучение производится в тематической последовательности. Содержание методических указаний должно соответствовать требованиям Федерального государственного образовательного стандарта и учебных программ по дисциплине. Самостоятельная работа студентов может быть выполнена с помощью материалов, размещенных на портале поддержки Moodl.

Методические указания по формам работы

Лекционные занятия

Передача значительного объема систематизированной информации в устной форме достаточно большой аудитории. Дает возможность экономно и систематично излагать учебный материал. Обучающиеся изучают лекционный материал, размещенный на портале поддержки обучения Moodl.

Практические занятия

Форма организации обучения, проводимая под руководством преподавателя и служащая для детализации, анализа, расширения, углубления, закрепления, применения (или выполнения разнообразных практических работ, упражнений) и контроля усвоения полученной на лекциях учебной информации. Практические занятия проводятся с использованием учебно-методических изданий, размещенных на образовательном портале университета.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

Для инвалидов и лиц с ОВЗ может изменяться объём дисциплины (модуля) в часах, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося (при этом не увеличивается количество зачётных единиц, выделенных на освоение дисциплины).

Фонды оценочных средств адаптируются к ограничениям здоровья и восприятия информации обучающимися.

Основные формы представления оценочных средств – в печатной форме или в форме электронного документа.

Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением зрения:

– устная проверка: дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.;

– с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, дистанционные формы, если позволяет острота зрения - графические работы и др.;

– при возможности письменная проверка с использованием рельефно-точечной системы Брайля, увеличенного шрифта, использование специальных технических средств (тифлотехнических средств): контрольные, графические работы, тестирование, домашние задания, эссе, отчеты и др.

Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением слуха:

– письменная проверка: контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.;
– с использованием компьютера: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы и др.;
– при возможности устная проверка с использованием специальных технических средств (аудиосредств, средств коммуникации, звукоусиливающей аппаратуры и др.): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.
Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением опорно-двигательного аппарата:
– письменная проверка с использованием специальных технических средств (альтернативных средств ввода, управления компьютером и др.): контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.;
– устная проверка, с использованием специальных технических средств (средств коммуникаций): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.;
– с использованием компьютера и специального ПО (альтернативных средств ввода и управления компьютером и др.): работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы предпочтительнее обучающимся, ограниченным в передвижении и др.
Адаптация процедуры проведения промежуточной аттестации для инвалидов и лиц с ОВЗ.
В ходе проведения промежуточной аттестации предусмотрено:
– предъявление обучающимся печатных и (или) электронных материалов в формах, адаптированных к ограничениям их здоровья;
– возможность пользоваться индивидуальными устройствами и средствами, позволяющими адаптировать материалы, осуществлять приём и передачу информации с учетом их индивидуальных особенностей;
– увеличение продолжительности проведения аттестации;
– возможность присутствия ассистента и оказания им необходимой помощи (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с преподавателем).
Формы промежуточной аттестации для инвалидов и лиц с ОВЗ должны учитывать индивидуальные и психофизические особенности обучающегося/обучающихся по АОПОП ВО (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями зрения:
– предоставление образовательного контента в текстовом электронном формате, позволяющем переводить плоскопечатную информацию в аудиальную или тактильную форму;
– возможность использовать индивидуальные устройства и средства, позволяющие адаптировать материалы, осуществлять приём и передачу информации с учетом индивидуальных особенностей и состояния здоровья студента;
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;
– использование чёткого и увеличенного по размеру шрифта и графических объектов в мультимедийных презентациях;
– использование инструментов «лупа», «прожектор» при работе с интерактивной доской;
– озвучивание визуальной информации, представленной обучающимся в ходе занятий;
– обеспечение раздаточным материалом, дублирующим информацию, выводимую на экран;
– наличие подписей и описания у всех используемых в процессе обучения рисунков и иных графических объектов, что даёт возможность перевести письменный текст в аудиальный;
– обеспечение особого речевого режима преподавания: лекции читаются громко, разборчиво, отчётливо, с паузами между смысловыми блоками информации, обеспечивается интонирование, повторение, акцентирование, профилактика рассеивания внимания;
– минимизация внешнего шума и обеспечение спокойной аудиальной обстановки;
– возможность вести запись учебной информации студентами в удобной для них форме

(аудиально, аудиовизуально, на ноутбуке, в виде пометок в заранее подготовленном тексте);
– увеличение доли методов социальной стимуляции (обращение внимания, апелляция к ограничениям по времени, контактные виды работ, групповые задания и др.) на практических и лабораторных занятиях;
– минимизирование заданий, требующих активного использования зрительной памяти и зрительного внимания;
– применение поэтапной системы контроля, более частый контроль выполнения заданий для самостоятельной работы.
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями опорно-двигательного аппарата (маломобильные студенты, студенты, имеющие трудности передвижения и патологию верхних конечностей):
– возможность использовать специальное программное обеспечение и специальное оборудование и позволяющее компенсировать двигательное нарушение (коляски, ходунки, трости и др.);
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;
– применение дополнительных средств активизации процессов запоминания и повторения;
– опора на определенные и точные понятия;
– использование для иллюстрации конкретных примеров;
– применение вопросов для мониторинга понимания;
– разделение изучаемого материала на небольшие логические блоки;
– увеличение доли конкретного материала и соблюдение принципа от простого к сложному при объяснении материала;
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;
– увеличение доли методов социальной стимуляции (обращение внимания, аппеляция к ограничениям по времени, контактные виды работ, групповые задания др.);
– обеспечение беспрепятственного доступа в помещения, а также пребывания них;
– наличие возможности использовать индивидуальные устройства и средства, позволяющие обеспечить реализацию эргономических принципов и комфортное пребывание на месте в течение всего периода учёбы (подставки, специальные подушки и др.).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями слуха (глухие, слабослышащие, позднооглохшие):
– предоставление образовательного контента в текстовом электронном формате, позволяющем переводить аудиальную форму лекции в плоскопечатную информацию;
– наличие возможности использовать индивидуальные звукоусиливающие устройства и сурдотехнические средства, позволяющие осуществлять приём и передачу информации; осуществлять взаимообратный перевод текстовых и аудиофайлов (блокнот для речевого ввода), а также запись и воспроизведение зрительной информации;
– наличие системы заданий, обеспечивающих систематизацию вербального материала, его схематизацию, перевод в таблицы, схемы, опорные тексты, глоссарий;
– наличие наглядного сопровождения изучаемого материала (структурно-логические схемы, таблицы, графики, концентрирующие и обобщающие информацию, опорные конспекты, раздаточный материал);
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;
– обеспечение практики опережающего чтения, когда студенты заранее знакомятся с материалом и выделяют незнакомые и непонятные слова и фрагменты;
– особый речевой режим работы (отказ от длинных фраз и сложных предложений, хорошая артикуляция; четкость изложения, отсутствие лишних слов; повторение фраз без изменения слов и порядка их следования; обеспечение зрительного контакта во время говорения и чуть более медленного темпа речи, использование естественных жестов и мимики);
– чёткое соблюдение алгоритма занятия и заданий для самостоятельной работы (называние темы, постановка цели, сообщение и запись плана, выделение основных понятий и методов

их изучения, указание видов деятельности студентов и способов проверки усвоения материала, словарная работа);
– соблюдение требований к предъявляемым учебным текстам (разбивка текста на час¬ти; выделение опорных смысловых пунктов; использование наглядных средств);
– минимизация внешних шумов;
– предоставление возможности соотносить вербальный и графический материал; комплексное использование письменных и устных средств коммуникации при работе в группе;
– сочетание на занятиях всех видов речевой деятельности (говорения, слушания, чтения, письма, зрительного восприятия с лица говорящего).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с прочими видами нарушений (ДЦП с нарушениями речи, заболевания эндокринной, центральной нервной и сердечно-сосудистой систем, онкологические заболевания):
– наличие возможности использовать индивидуальные устройства и средства, позволяющие осуществлять приём и передачу информации;
– наличие системы заданий, обеспечивающих систематизацию вербального материала, его схематизацию, перевод в таблицы, схемы, опорные тексты, глоссарий;
– наличие наглядного сопровождения изучаемого материала;
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;
– обеспечение практики опережающего чтения, когда студенты заранее знакомятся с материалом и выделяют незнакомые и непонятные слова и фрагменты;
– предоставление возможности соотносить вербальный и графический материал; комплексное использование письменных и устных средств коммуникации при работе в группе;
– сочетание на занятиях всех видов речевой деятельности (говорения, слушания, чтения, письма, зрительного восприятия с лица говорящего);
– предоставление образовательного контента в текстовом электронном формате;
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;
– возможность вести запись учебной информации студентами в удобной для них форме (аудиально, аудиовизуально, в виде пометок в заранее подготовленном тексте);
– применение поэтапной системы контроля, более частый контроль выполнения заданий для самостоятельной работы;
– стимулирование выработки у студентов навыков самоорганизации и самоконтроля;
– наличие пауз для отдыха и смены видов деятельности по ходу занятия.

10. Методические рекомендации по освоению дисциплины (модуля)

Дисциплина "Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности" ведется в соответствии с учебным планом и расписанием занятий по неделям. Темы проведения занятий определяются тематическим планом рабочей программы дисциплины.